Avis du Contrôleur européen de la protection des données

sur le paquet de mesures pour une réforme de la protection des données

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

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

vu 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 la demande d'avis formulée conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 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],

A ADOPTÉ L'AVIS SUIVANT:

CHAPITRE I - INTRODUCTION ET REMARQUES GÉNÉRALES

I.1. Introduction

I.1.a. Paquet de mesures pour une réforme de la protection des données et consultation du CEPD

1. Le 25 janvier 2012, la Commission a adopté un paquet de mesures visant à réformer le cadre européen de protection des données. Le paquet inclut:
   - une communication intitulée «Protection de la vie privée dans un monde en réseau: Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle» («la communication»)[3];
   - une proposition de 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 («la proposition de règlement»)[4];
   - 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

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2012)9 final.
[4] COM(2012)11 final.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
E-mail : edps@edps.europa.eu – Site internet: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax : 02-283 19 50

poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données («la proposition de directive»)[5].

2. La proposition de règlement est supposée remplacer la directive 95/46/CE et modifie la directive 2002/58/CE. La proposition de directive est destinée à remplacer la décision-cadre 2008/977/JAI.

3. Par lettre du 25 janvier 2012, le CEPD a été invité par la Commission à formuler un avis sur le paquet. Durant le processus d'élaboration du paquet de mesures pour une réforme, le CEPD a eu l'opportunité de soumettre des observations sur une version antérieure des textes proposés. Plusieurs de ces observations ont donné lieu à des modifications du texte de la proposition finale. Le CEPD apprécie d'avoir eu cette possibilité.

4. Le paquet de réformes du 25 janvier 2012 est la concrétisation des plans présentés par la Commission dans la communication «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», publiée le 4 novembre 2010. Le 14 janvier 2011, en réponse à cette communication, le CEPD a publié un avis exposant sa vision du nouveau cadre relatif à la protection des données[6]. Le présent avis se fonde sur les conclusions présentées dans cet avis. Il se fonde également sur les contributions du groupe de travail «Article 29» auquel le CEPD participe en tant que membre, notamment son avis du 1er décembre 2009 sur l'avenir de la protection de la vie privée[7].

5. Le groupe de travail «Article 29» a également l'intention de publier un avis sur le paquet de réformes. Le présent avis du CEPD et le prochain avis du groupe de travail doivent être considérés comme étant la contribution des autorités de contrôle au processus législatif au sein du Parlement européen et du Conseil.

I.1.b. Contexte et évaluation générale

i) Les motifs pour une réforme du cadre juridique de l'UE relatif à la protection des données

6. La nécessité d'une protection des données s'est accrue dans le monde actuel. L'importance de disposer de bonnes règles pour la protection des données a été confirmée par le traité de Lisbonne. Ce dernier a donné valeur de traité à la Charte des droits fondamentaux de l'Union européenne («la Charte») et, partant, à la protection des données en tant que droit fondamental contraignant. Il a consacré le droit à la protection des données en tant que droit pour chaque individu, à l'article 16 du traité sur le fonctionnement de l'Union européenne («TFUE»).

7. En outre, le traité de Lisbonne a inséré une nouvelle base juridique unique pour les règles sur la protection des données à l'article 16 TFUE. Cette base juridique unique constitue l'élan juridique pour reconsidérer les règles de l'UE sur la protection des données. Toutefois et plus important encore: il existe plusieurs raisons substantielles qui justifient et nécessitent une réforme du cadre de l'UE relatif à la protection des données.

[5] COM(2012)10 final.
[6] Avis du CEPD sur la communication «Une approche globale de la protection des données dans l'Union européenne» du 14 janvier 2011, JO L 181, 22.6.2011, p. 1 («avis du CEPD du 14 janvier 2011»).
[7] Voir l'avis du groupe de travail «Article 29» du 1er décembre 2009 sur l'avenir de la protection de la vie privée (WP168).

8. Premièrement, l'évolution technologique: bien que la directive 95/46/CE ait démontré sa valeur au cours des dix-sept dernières années et n'ait jamais perdu de sa pertinence, les règles nécessitent une mise à jour à la lumière du développement rapide des mutations technologiques depuis son adoption en 1995. Cette mise à jour est également fondamentale dans l'optique de créer un environnement durable pour la poursuite de l'innovation dans les années à venir.

9. Deuxièmement, la sécurité juridique: les citoyens ainsi que les acteurs économiques et les organismes publics peuvent tirer un immense profit de règles modernisées sur la protection des données, créant une sécurité juridique et réglementant la protection des données d'une façon qui garantisse un niveau élevé de protection et qui soit à la fois efficace et productive. Cela signifie également mettre davantage l'accent sur les principes de fond et les résultats souhaitables que sur les formalités et les obligations administratives.

10. Troisièmement, l'harmonisation dans le marché intérieur: la pratique a démontré que dans le cadre de l'actuel directive 95/46/CE, il existe encore entre les législations des États membres de nombreuses différences qui entravent le marché unique de l'UE. Une plus grande harmonisation est manifestement nécessaire.

11. Quatrièmement, la nécessité d'un changement dans le domaine de la coopération policière et judiciaire, à l'heure où le cadre juridique de l'UE relatif à la protection des données dans ce domaine constitue une mosaïque d'instruments spécifiques de l'UE pour la protection des données. En outre, il existe des différences au niveau de la protection des données avec les règles générales sur la protection des données, actuellement contenues dans la directive 95/46/CE. Avec l'article 16 TFUE en place, ces règles peuvent à présent être intégrées dans un cadre juridique complet couvrant tous les domaines de la politique de l'UE.

12. Cinquièmement, la dimension mondiale: le traitement transfrontalier des données et les transferts internationaux ont énormément augmenté ces dernières années. La dimension internationale des règles actuelles de l'UE a besoin d'être affinée afin d'éviter des obstacles inutiles tels que ceux rencontrés aujourd'hui. Les règles de l'UE sur le transfert international des données doivent garantir l'existence d'une protection adéquate des données à caractère personnel sans restreindre inutilement le commerce et la coopération au niveau international.

13. La réforme des règles de l'UE s'inscrit parallèlement à la modernisation des règles relatives à la protection des données, adoptées dans d'autres organismes internationaux. Actuellement, parallèlement à l'UE, le Conseil de l'Europe évalue la façon dont la convention relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel («convention 108») pourrait être modifiée afin de faire face aux défis actuels[8]. Le même exercice a lieu en ce qui concerne les lignes directrices de l'OCDE sur la protection de la vie privée[9].

[8] Voir les propositions pour la modernisation de la Convention 108, T-PD-BUR(2012)01EN, disponibles à l'adresse http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01_EN.pdf.

[9] Voir le rapport de l'OCDE sur le paysage changeant de la protection de la vie privée: 30 ans après les lignes directrices de l'OCDE sur la protection de la vie privée, 6 avril 2011, disponible à l'adresse http://www.oecd.org/dataoecd/22/25/47683378.pdf; voir également la déclaration de Séoul sur le futur de l'économie internet, 18 juin 2008, disponible à l'adresse http://www.oecd.org/dataoecd/49/28/40839436.pdf.

14. Cela signifie que la réforme des règles de l'UE intervient à un moment crucial et ouvre une fenêtre de grandes possibilités. Si celles-ci sont bien utilisées, cela renforcera les cadres juridiques dans l'UE tout en assurant une protection de la vie privée plus globale.

15. Compte tenu de tous ces éléments, le CEPD a invité à plusieurs reprises la Commission à proposer un système robuste et complet qui serait ambitieux et renforcerait l'efficacité et la cohérence de la protection des données dans l'UE, afin de garantir un environnement solide pour un nouveau développement dans les années à venir[10].

ii) Évaluation générale du paquet de réformes

16. Le paquet de réformes adopté le 25 janvier 2012 répond à bon nombre des attentes exposées ci-dessus. Ainsi que le CEPD l'a déjà déclaré dans sa réaction, le jour de la publication du paquet, le règlement proposé constitue un grand pas en avant pour le droit à la protection des données en Europe[11].

17. Les règles proposées dans le règlement renforceront les droits des individus et responsabiliseront davantage les responsables de traitement quant à la manière de traiter les données personnelles. En outre, le rôle et les pouvoirs des autorités nationales de contrôle (séparément et conjointement) se verront réellement renforcés. Bien que le CEPD formule dans le présent avis des observations sur plusieurs dispositions de la proposition de règlement, il souhaite souligner qu'en général, le niveau de l'ambition et l'approche globale de la proposition sont très positifs.

18. Le CEPD est particulièrement heureux de voir que la Commission a proposé l'instrument d'un *règlement* pour les règles générales sur la protection des données. Le CEPD est convaincu qu'un règlement constitue l'instrument adéquat pour parvenir à une protection plus efficace et cohérente des données dans l'UE, ce qui contribuera à la poursuite de la mise en place du marché intérieur de l'UE[12]. La proposition de règlement serait directement applicable dans les États membres et mettrait fin à de nombreuses complexités et incohérences découlant des différentes mesures d'exécution des États membres actuellement en place. Le même droit serait applicable au traitement des données à caractère personnel dans tous les États membres. Cela signifie également que le règlement constituera un point d'ancrage essentiel de la stratégie Europe 2020 pour une croissance intelligente, durable et inclusive.

19. Cela étant, le CEPD juge la proposition de directive pour la protection des données extrêmement décevante en matière pénale. Un élément positif de la proposition de directive est le fait que, contrairement à la décision-cadre 2008/977/JAI, le traitement national sera également couvert par l'instrument de l'UE. Toutefois, cet élargissement du champ d'application n'offre de plus-value que si la directive renforce substantiellement le niveau de protection des données dans ce domaine, ce qui n'est pas le cas. Par rapport à la proposition de règlement, de nombreuses dispositions dans la proposition de directive sont faibles, sans aucune justification manifeste.

20. Le CEPD regrette que la Commission ait choisi de réglementer cette question dans un instrument juridique autonome offrant un niveau de protection inadéquat, très inférieur à celui de la proposition de règlement. Cet écart ne contribuera manifestement pas à une

[10] Voir notamment l'avis du CEPD du 14 janvier 2011.
[11] Voir le communiqué de presse du 25 janvier 2012, qui figure sur le site internet du CEPD (www.edps.europa.eu).
[12] Voir l'avis du CEPD du 14 janvier 2011, point 64.

approche globale du nouveau cadre de l'UE relatif à la protection des données et pourrait également exercer un impact négatif sur les futures initiatives qui ont été reportées par la Commission à un stade ultérieur (voir partie I.2.a et b ci-dessous).

21. Dans le présent avis, le CEPD analysera les deux propositions législatives de façon plus détaillée. Le chapitre II traitera de la proposition de règlement, le chapitre III de la proposition de directive. Le reste du présent chapitre est consacré à une analyse approfondie de la principale faiblesse du paquet: il n'a pas été remédié à l'absence actuelle d'approche globale du cadre de l'UE relatif à la protection des données.

I.2. Principale faiblesse du paquet: il n'est pas remédié à l'absence d'approche globale du paquet

22. La Commission annonçait l'approche globale d'un cadre révisé de l'UE relatif à la protection des données dans sa communication de novembre 2010, intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne».

23. Elle a été saluée et approuvée par le Parlement européen et le Conseil. Dans sa résolution du 6 juillet 2011, le Parlement européen a exprimé son engagement total envers une approche globale[13]. De même, dans ses conclusions des 24 et 25 février 2011, le Conseil mentionnait un nouveau cadre juridique fondé sur l'approche globale[14]. Dans son avis du 14 janvier 2011, le CEPD considérait l'approche globale comme étant une condition indispensable pour une protection efficace des données à l'avenir[15].

24. À présent que le paquet de réformes a été adopté, il y a lieu d'observer que les propositions – dans leur forme actuelle – ne contribueront malheureusement pas à l'approche globale du cadre juridique de l'UE relatif à la protection des données.

25. S'il est vrai qu'un règlement, en tant que principal instrument proposé pour les règles de l'UE relatives à la protection des données, et l'application de la proposition de directive au traitement national contribueront considérablement à l'approche globale des règles relatives à la protection des données s'appliquant au niveau national dans les deux domaines, ces développements seuls ne débouchent pas sur un système global, ainsi qu'il sera expliqué ci-dessous.

I.2.a. Le cadre relatif à la protection des données n'est que partiellement couvert

26. Les règles relatives à la protection des données pour les institutions, organes et organismes de l'UE, telles qu'exposées dans le règlement (CE) n° 45/2001, sont restées inchangées, de même que tous les actes spécifiques dans le domaine de la coopération policière et judiciaire en matière pénale, tels que les règles pour Europol et Eurojust, ou les règles relatives à la protection des données dans le cadre de la décision de Prüm[16].

[13] Voir la résolution du Parlement européen du 6 juillet 2011, 2011/2025(INI).
[14] Voir les conclusions du Conseil de la 3071e session du Conseil Justice et affaires intérieures des 24 et 25 février 2011.
[15] Voir l'avis du CEPD du 14 janvier 2011, point 34.
[16] Voir la décision du Conseil 2009/371/JAI du 6 avril 2009 portant création de l'Office européen de police (Europol), JO L 121, 15.05.2009, p. 37; la décision du Conseil 2009/426/JAI du 16 décembre 2008, JO L 138, 4.6.2009, p. 14 et la décision du Conseil 2008/615/JAI du 23 juin 2008 (la «décision de Prüm»), JO L 210, 6.8.2008, p. 12.

De même, aucune règle n'est actuellement prévue pour la politique étrangère et de sécurité commune, fondée sur l'article 39 du traité UE.

27. Dans sa communication de novembre 2010, la Commission avait déjà annoncé qu'elle évaluerait la nécessité d'adapter d'autres instruments juridiques sur la protection des données en tant que deuxième étape. Dans son avis de janvier 2011, le CEPD a exprimé son insatisfaction quant au fait que certains domaines resteraient exclus des instruments juridiques généraux[17].

28. Le CEPD regrette que, dans l'actuelle communication, la Commission n'ait pas saisi l'opportunité, à tout le moins, de mieux s'expliquer et s'engager, en utilisant des calendriers concrets présentant des délais stricts, envers la procédure et les futures étapes concernant l'ensemble de la réforme du cadre de l'UE relatif à la protection des données. Il n'est pas fait la moindre mention, dans la communication, de la deuxième étape du processus de réforme. Le CEPD encourage la Commission à annoncer publiquement le calendrier portant sur la deuxième phase du processus de réforme dans les plus brefs délais.

i) Réexamen du règlement (CE) n° 45/2001

29. Le CEPD recommande, dans un souci de sécurité juridique et d'uniformité, l'incorporation des règles de fond pour les institutions et organes de l'UE dans la proposition de règlement. Dans son avis de janvier 2011, le CEPD a déjà exprimé sa préférence pour cette option. Un seul texte juridique éviterait le risque de divergences entre les dispositions et serait le véhicule le plus approprié pour les échanges de données entre le niveau de l'UE et les entités publiques et privées dans les États membres[18].

30. Une autre option – bien que non privilégiée – serait que la Commission s'engage à veiller à ce que les règles pour les institutions et organes européens soient en adéquation avec le nouveau règlement général en matière de protection des données et entrent en vigueur au plus tard lors de l'application de ce dernier. Un stade encore plus précoce pourrait être préférable afin de permettre aux institutions d'acquérir de l'expérience avec le nouveau système avant son utilisation dans tous les États membres. Il serait en tout état de cause manifestement inacceptable que la Commission et les autres institutions et organes de l'UE ne soient pas liés par les mêmes nouvelles règles qui s'appliquent au niveau des États membres.

31. En outre, il serait extrêmement peu souhaitable, pour le CEPD, de superviser la conformité des institutions et organes de l'UE avec des règles de fond qui seraient inférieures aux règles supervisées par ses homologues au niveau national. Cela apparaîtrait tout particulièrement dans le contexte du Comité européen de la protection des données, au sein duquel le CEPD est supposé jouer un rôle actif. Par ailleurs, il y a lieu de noter que le règlement (CE) n° 45/2001 est déjà dépassé en ce qui concerne les communications électroniques, étant donné qu'il est limité à des dispositions en matière de télécommunications fondées sur le prédécesseur de la directive relative à la vie privée et aux communications électroniques[19].

[17] Voir l'avis du CEPD du 14 janvier 2011, point 169.
[18] Voir l'avis du CEPD du 14 janvier 2011, point 45. L'expérience positive avec les délégués à la protection des données dans le contexte du règlement (CE) n° 45/2001 pourrait également contribuer au débat en cours.
[19] Directive 97/66/CE du 15 décembre 1997, JO L24, 30.1.1998, p. 1.

ii) Actes spécifiques dans le domaine de la coopération policière et judiciaire en matière pénale

32. En ce qui concerne les instruments spécifiques dans le domaine de la coopération policière et judiciaire en matière pénale, il est mentionné, à l'article 61, paragraphe 2, de la proposition de directive que la Commission réexamine ces actes dans un délai de trois ans à compter de l'entrée en vigueur de la directive. Le CEPD estime qu'un tel délai entraînerait une période d'une durée inacceptable, durant laquelle la mosaïque actuelle, largement critiquée, resterait en vigueur.

33. Étant donné qu'une clarification de l'ensemble du cadre devrait être apportée dans les plus brefs délais, le CEPD recommande vivement au législateur de fixer un délai beaucoup plus strict qui veille à ce que les règles spécifiques soient modifiées au plus tard au moment de l'entrée en vigueur de la directive.

iii) Politique étrangère et de sécurité commune

34. Le CEPD recommande que la Commission présente dans les plus brefs délais des règles communes pour ce domaine, fondées sur l'article 39 du traité UE et, en principe, identiques aux règles communes dans d'autres domaines.

I.2.b. Les deux instruments proposés considérés conjointement ne créent pas un cadre global relatif à la protection des données

35. Ainsi que le CEPD l'a déclaré précédemment, la cohérence et l'exhaustivité militent en faveur d'une approche en vertu de laquelle un règlement fixe les règles générales en matière de protection des données, complété par des règles sectorielles supplémentaires[20]. Un tel règlement indiquerait les conditions générales pour limiter certains droits et obligations pour la prévention, la détection, les enquêtes et les poursuites des infractions pénales. Des règles spécifiques supplémentaires harmoniseraient les règles nationales adoptées dans ce domaine, telles que visées dans la déclaration 21 annexée au traité de Lisbonne.

36. Malheureusement, la Commission a fait un choix différent. La proposition de directive constitue un instrument autonome qui contient sa propre version, souvent différente, des définitions, des principes, des droits et des obligations pour les autorités répressives. En soi, cela complique la procédure législative et il existe également un risque élevé de voir ces dispositions modifiées davantage encore, dans des sens différents de ceux du règlement.

37. Le CEPD invite instamment le législateur à veiller à ce que les deux instruments contiennent les mêmes dispositions essentielles et entrent en vigueur à la même date. Une divergence entre des dispositions équivalentes ne devrait être autorisée que si elle est dûment justifiée. Nous encourageons la Commission, le Conseil et le Parlement à s'engager à faire tout ce qui est en leur pouvoir pour garantir la cohérence des deux instruments, tant en termes de contenu qu'en termes de calendrier.

38. Le choix d'un instrument autonome est regrettable et constitue une occasion manquée de clarifier et de garantir l'application cohérente des règles applicables aux situations dans lesquelles les activités du secteur privé et des autorités répressives interagissent

[20] Voir l'avis du CEPD du 14 janvier 2011, point 48.

entre elles et où les frontières tendent de plus en plus à s'estomper. Des exemples de ces situations sont le transfert des données PNR et des données sur les transferts financiers vers les autorités répressives. La Commission a elle-même reconnu ce défaut dans le cadre juridique actuel. À l'annexe III de l'analyse d'impact des deux instruments proposés, la décision-cadre 2008/977/JAI est fortement critiquée pour ne pas avoir traité l'insécurité juridique des situations dans lesquelles les données collectées à des fins commerciales sont utilisées à des fins répressives[21].

39. Cela s'applique également à d'autres situations, par exemple, lorsque l'information est transférée entre une autorité répressive et une entité privée ou lorsqu'une autorité répressive transfère des données à une autre autorité publique qui n'est pas responsable de l'application de la loi. La situation devient encore plus complexe si des systèmes d'information publique sont en partie établis dans le domaine de la coopération policière et judiciaire en matière pénale, et en partie dans d'autres domaines. L'exemple le plus clair au niveau de l'UE est le système d'information de Schengen qui, en outre, compte également des éléments nationaux et européens[22].

40. Ainsi qu'il sera discuté dans les observations plus détaillées des chapitres II et III du présent avis, les dispositions qui touchent à la relation entre les deux instruments ne traitent pas clairement de la question[23]. Au contraire, les propositions ne semblent qu'ajouter à la confusion dans ce domaine. Les propositions actuelles pourraient, à cet égard, mener encore à un droit national divergent et une pratique nationale incohérente, et pourraient encore soulever des questions de droit applicable. Elles ne clarifient pas non plus la façon dont la compétence est répartie entre les États membres et l'UE en ce qui concerne les négociations avec les pays tiers sur l'éventuel transfert de ces données.

CHAPITRE II - OBSERVATIONS SUR LA PROPOSITION DE RÈGLEMENT

II.1. Introduction

41. La proposition de règlement constitue un grand pas en avant pour le droit à la protection des données dans l'UE. Le CEPD soutient la proposition car elle est fondée sur le choix adéquat de l'instrument juridique, un règlement, et en raison du contenu très apprécié de bon nombre des propositions de modification des règles actuelles.

42. Néanmoins, la proposition fait naître plusieurs questions horizontales, telles que les relations entre le droit de l'UE et le droit national, qui seront discutées dans la partie II.2 ci-dessous. Dans cette même partie, plusieurs autres questions horizontales sont abordées, à savoir les éventuels actes délégués ou d'exécution en relation avec de nombreuses dispositions de la proposition de règlement, les dispositions particulières pour les micro, petites et moyennes entreprises dans la proposition ainsi que l'utilisation de la notion de l'«intérêt général».

[21] Voir l'annexe III, p. 4.
[22] Voir le règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération, JO L 381, 28.12.2006, p. 4, et la décision du Conseil 2007/533/JAI du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération, JO L 205, 7.08.2007, p. 63.
[23] Voir notamment la partie II.3.a.iv), II.5.f et III.2.c.

43. À partir de la partie II.3, le contenu de la proposition de règlement sera commenté plus en détail, chapitre après chapitre. Le CEPD soulignera bon nombre d'éléments positifs de la proposition, dont les suivants:
    - la clarification du champ d'application de la proposition de règlement (voir la partie II.3);
    - les exigences de transparence accrue envers la personne concernée et le renforcement du droit d'opposition (voir la partie II.5);
    - l'obligation générale pour les responsables du traitement de veiller à, et d'être capables de démontrer la conformité aux dispositions du règlement (voir la partie II.6);
    - le renforcement de la position et du rôle des autorités de surveillance nationales (voir la partie II.8);
    - les principales lignes du mécanisme de contrôle de la cohérence (voir la partie II.9).

44. Le CEPD accordera la plus grande attention aux dispositions de la proposition qui suscitent des préoccupations ou qui doivent encore être améliorées, dont, notamment, les suivantes:
    - les nouvelles exceptions au principe de limitation de la finalité (voir la partie II.4.a);
    - les possibilités de restreindre les principes et droits de base (voir la partie II.2.a.iii) et II.5.f);
    - l'obligation pour les responsables du traitement de conserver la documentation de toutes les opérations de traitement (voir la partie II.6.e);
    - le transfert de données vers des pays tiers par voie de dérogation (voir la partie II.7.d);
    - le rôle de la Commission dans le mécanisme destiné à garantir la cohérence (voir la partie II.9.b.ii));
    - la nature obligatoire de l'imposition de sanctions administratives (voir la partie II.10.c).

II.2. Questions horizontales

45. Un règlement constitue l'instrument le plus complet du droit dérivé de l'UE, étant donné qu'il s'applique directement dans tous les États membres, et créera dès lors un seul droit applicable dans l'ensemble de l'UE, prioritaire sur tout droit national qui ne lui est pas compatible[24]. Il est dès lors important de se pencher de plus près sur la façon dont la proposition de règlement traite des relations entre le droit de l'UE et le droit national dans ce domaine.

46. Plus particulièrement, la question se pose de savoir sur quels points le règlement devrait accorder aux États membres une certaine liberté d'avoir des lois nationales qui soit incorporent des dispositions de la proposition de règlement pour les intégrer dans leur ordre juridique national particulier, soit prescrivent des règles spécifiques qui pourraient se justifier pour certains domaines où apparaissent des différences culturelles entre les États membres.

47. En établissant l'équilibre adéquat, le législateur de l'UE doit déterminer si chacune des marges de manœuvre proposées pour les États membres pourrait peut_être donner inutilement lieu à des droits nationaux divergents qui maintiendraient les difficultés existant dans le cadre de l'actuelle directive 95/46/CE en ce qui concerne la diversité et la complexité du droit applicable et la compétence des autorités de contrôle.

[24] Voir l'article 288 TFUE.

48. Une deuxième question d'importance générale découle des nombreuses dispositions qui habilitent la Commission à adopter des actes délégués ou d'exécution. Le CEPD salue cette approche dans la mesure où elle contribue à l'application cohérente du règlement, mais émet des réserves dans la mesure où elle pourrait, sur certains points, tirer indûment profit de ces actes.

49. D'autres questions générales impliquant l'équilibre approprié entre diversité et cohérence se posent en ce qui concerne les dispositions particulières pour les micro, petites et moyennes entreprises dans la proposition et l'usage intensif de la notion de l'«intérêt général». Ces questions seront plus amplement discutées ci-dessous.

II.2.a. Relations entre le droit de l'UE et le droit national

i) L'approche générale du règlement

50. Bien que la proposition de règlement tende largement à la création d'un seul droit applicable pour la protection des données dans l'UE, une analyse plus approfondie de ses dispositions montre qu'il reste davantage de place pour la coexistence et l'interaction entre le droit de l'UE et le droit national que l'on ne pourrait le croire. En réalité, il y a un grand nombre d'exemples de dispositions où le règlement *se fonde* clairement sur le droit national ou, à l'inverse, permet ou donne mandat au droit national de se fonder sur et donc de donner *effet* à ses dispositions. Il existe également différents exemples de dispositions où le règlement permet ou oblige le droit national à *spécifier* ou à poursuivre le développement de ses règles dans certains domaines, voire à *s'écarter* de ses dispositions dans certaines conditions.

51. Des exemples clairs de la première catégorie – *fondement* sur le *droit national* – figurent à l'article 6 de la proposition de règlement au titre de la licéité du traitement. Conformément à l'article 6, paragraphe 1, le traitement de données à caractère personnel n'est licite que si et dans la mesure où ce traitement est c) nécessaire à l'exécution d'un contrat auquel la personne contrôlée est partie, ou e) nécessaire à l'exécution d'une mission effectuée dans l'intérêt général ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans les deux cas, la proposition de règlement se fonde sur des motifs de traitement essentiellement prévus dans le cadre du droit national, sous réserve uniquement de nouvelles conditions quant à la qualité du droit à l'article 6, paragraphe 3[25].

52. Des exemples de la deuxième catégorie – le droit national *se fondant* sur le *règlement* – ont trait à l'organisation et au fonctionnement des autorités de contrôle (articles 46 à 49). Ces dispositions sont nécessaires pour respecter les systèmes institutionnels et constitutionnels des États membres et les obligent uniquement à établir et organiser des autorités de contrôle qui soient capables d'exécuter les tâches qui leur sont confiées dans le règlement[26].

[25] Étant donné que le «traitement», tel que défini à l'article 4, paragraphe 3, a un vaste champ d'application, cet exemple est pertinent pour de nombreuses dispositions de droit national imposant des obligations de collecter, stocker, conserver ou échanger des données à caractère personnel, que ce soit dans le secteur public ou privé, et pour un éventail d'autres tâches publiques. D'autres exemples figurent à l'article 4, paragraphe 5, concernant la définition de responsable du traitement, à l'article 6, paragraphe 1, point b), sur l'exécution des contrats, et à l'article 8, paragraphe 2, avec une référence au droit national en matière contractuelle.

[26] D'autres exemples figurent à l'article 78 sur l'établissement de sanctions pénales et, de façon plus implicite, aux articles 73 à 76 sur les recours qui sont susceptibles de nécessiter au moins une intégration dans le droit national ou qui seront assujettis à des exigences procédurales prévues dans le droit national.

53. Des exemples de la troisième catégorie – *spécification* ou poursuite du développement du règlement – et de la quatrième catégorie – *éloignement* du règlement – seront discutés plus en détail ci-dessous, étant donné qu'ils sont plus problématiques du point de vue de la cohérence et de la diversité.

54. Dans tous ces cas, la question concernant le champ d'application du droit national peut se poser. Lorsque la proposition de règlement *se fonde* sur le droit national (première catégorie), le champ d'application du droit national est clairement déterminé par ses propres termes et par le système constitutionnel de l'État membre pertinent. Il en ira de même pour la deuxième catégorie (droit national *se fondant* sur le règlement), bien que le règlement puisse, dans certains cas, prévoir un champ d'application supplémentaire pour dépasser les frontières nationales.

55. Dans les troisième et quatrième catégories, le champ d'application territorial du droit national peut s'avérer plus problématique en l'absence d'une disposition spécifique dans le règlement lui-même[27]. Le CEPD recommande dès lors l'inclusion dans le règlement d'une disposition explicite clarifiant la question du champ d'application territorial de ces droits nationaux (voir également, sur ce point, la partie II.3.b).

ii) Situations spécifiques de traitement des données

56. Le chapitre IX de la proposition de règlement laisse une place supplémentaire pour des règles nationales spécifiques concernant certaines situations de traitement des données, mentionnées aux articles 80, 81, 82, 84 et 85. Ces situations ont trait à la liberté d'expression, à la santé, à l'emploi, au secret professionnel et aux églises et associations religieuses.

57. S'il est nécessaire de concilier des règles uniformes en matière de protection des données avec les spécificités nationales, le CEPD n'est pas convaincu que ces exemptions et dérogations soient absolument nécessaires pour tous les secteurs inclus dans le chapitre IX tel que proposé actuellement, bien que cela puisse faire partie d'un problème plus général (voir le point iv) ci-dessous).

58. Plus particulièrement, en ce qui concerne le secteur de l'emploi, les principes de la protection des données s'appliquent déjà en vertu du droit existant, sans préjudice des obligations légales en matière d'emploi, étant donné que les deux cadres juridiques doivent être considérés comme complémentaires. Une obligation légale dans le droit du travail pourrait, par exemple, constituer une base légitime pour le traitement en vertu de l'article 6 de la proposition de règlement.

59. Deuxièmement, les articles 81, 82 et 84 de la proposition de règlement énoncent que les règles nationales spécifiques doivent se situer «dans les limites du présent règlement». Le CEPD présume que l'intention est de prévenir les dérogations aux principes du règlement dans les différents secteurs. Il recommande de remplacer cette formulation par un libellé clair, déclarant que les spécifications de la loi nationale doivent être «sans préjudice» du règlement.

[27] L'article 4 de la directive 95/46/CE prévoit actuellement un certain effet extraterritorial du droit national qui la met en œuvre. Voir l'avis 8/2010 du groupe de travail «Article 29» du 16 décembre 2010 sur le droit applicable (WP 179).

60. Les dispositions du chapitre IX sur les situations spécifiques du traitement des données seront discutées plus en détail dans la partie II.11 ci-dessous.

iii) Autres dispositions permettant de spécifier les règles nationales ou d'y déroger

61. D'autres possibilités pour des règles nationales spécifiques sont prévues dans plusieurs autres dispositions de la proposition de règlement. Le CEPD distingue différents types de dispositions autorisant une marge d'appréciation nationale, comme exposé ci-dessus.

62. Le quatrième type de dispositions est de nature différente et habilite les États membres à *s'écarter* des dispositions du règlement.

63. La principale disposition à cet égard est l'article 21 qui permet au droit de l'Union ou au droit des États membres de limiter la portée de certaines dispositions du règlement. Cette disposition est actuellement située dans le chapitre III de la proposition de règlement sur les droits des personnes concernées, mais a un champ d'application plus large que la prévision de limitations des droits des personnes concernées, puisqu'elle s'étend également aux principes fondamentaux exposés à l'article 5 de la proposition, tels que les principes de licéité, de loyauté, de limitation de la finalité, d'exactitude et de nécessité (voir également la partie II.4.a ci-dessous).

64. Par rapport à l'actuel article 13 de la directive 95/46/CE, l'article 21 de la proposition de règlement étend significativement les motifs de limitation au-delà des intérêts spécifiques liés aux infractions pénales, aux professions réglementées et aux intérêts économiques ou financiers importants, en incluant «d'autres» intérêts publics non définis. Il n'existe toutefois aucune justification pour étendre le champ des limitations à ces intérêts et le CEPD considère cette disposition comme inutile et disproportionnée. Il appelle dès lors à limiter le recours à l'exemption pour des raisons d'intérêt général à des circonstances clairement identifiées et limitées, dont les infractions pénales ou les intérêts économiques et financiers.

65. En outre, le CEPD recommande que le législateur introduise, à l'article 21, des garanties plus détaillées quant à la qualité du droit national. Ce point sera plus amplement discuté dans la partie II.5.f ci-dessous.

66. D'autres dispositions de la proposition de règlement permettent également au droit national de limiter le champ d'application de certaines dispositions. Tel est le cas de l'article 6, paragraphe 4, qui permet au droit national de déroger au principe de limitation de la finalité, et de l'article 17, paragraphe 3, point d), qui permet au droit national d'exiger la conservation des données même si une personne a invoqué son droit à l'oubli. Dans les deux cas, les dérogations sont inutiles et l'article 21 pourrait être invoqué pour limiter si nécessaire le champ d'application des dispositions.

67. Le CEPD estime que l'article 21 ne doit pas être complété par ces possibilités spécifiques de restrictions. Il recommande dès lors de supprimer ou de limiter la portée de l'article 6, paragraphe 4, et de l'article 17, paragraphe 3, point d) (voir également la partie II.4.a et II.5.b).

iv) Autres lois nationales spécifiques

68. Dans la plupart des États membres, il y a un grand nombre de lois nationales qui pourraient ne pas traiter de la protection des données, au sens officiel, mais contenir

néanmoins diverses dispositions sur la collecte, la conservation, la suppression, l'échange ou la publication de données à caractère personnel, ou sur la façon dont les droits des personnes concernées doivent être exercés ou respectés dans un domaine spécifique.

69. Bon nombre de ces lois peuvent s'inscrire dans le champ d'application de la directive 95/46/CE et avoir représenté une partie de la mise en œuvre de cette directive dans le droit national. Dans la plupart des États membres, ces lois seront cohérentes avec la loi nationale sur la protection des données mais peuvent spécifier davantage ses dispositions pour un certain domaine. Ces lois seront plus fréquentes dans le secteur public, mais peuvent également s'avérer pertinentes dans une série d'autres domaines.

70. Il est clair que ces lois doivent être modifiées si elles ne sont pas compatibles avec la proposition de règlement, dans la mesure où leurs dispositions n'offriraient pas une base pour un traitement licite des données à caractère personnel (voir la partie II.2.a.i) ci-dessus) et ne sont pas prévues dans le règlement. Cela nécessiterait une mise en adéquation de ces lois nationales avec les dispositions du règlement, y compris le principe général de la libre circulation des données à caractère personnel dans l'Union, tel qu'exprimé à l'article 1, paragraphe 3, du règlement. La place laissée au droit national par le règlement n'apparaît pas toujours clairement. Par exemple, dans quelle mesure les dispositions des chapitres II et III sont-elles exhaustives et dans quelle mesure des dispositions pour des secteurs spécifiques sont-elles autorisées? Le CEPD recommande un examen plus attentif de cette question afin de décider si une nouvelle disposition est nécessaire, spécifiant la mesure dans laquelle des lois nationales spécifiques sont permises, «sans préjudice du règlement», comme mentionné ci-dessus.

II.2.b. Actes délégués et d'exécution

71. Dans bon nombre des dispositions de la proposition de règlement, la Commission est habilitée à adopter des actes délégués ou d'exécution. Bien que ces nouveaux actes puissent contribuer à l'application uniforme du règlement et permettre une nouvelle mise en adéquation de la pratique nationale fondée sur l'expérience acquise après l'application du règlement, le CEPD émet, comme indiqué, des réserves quant à une approche qui s'appuie aussi lourdement sur ces actes. En outre, le CEPD n'est pas convaincu que toutes les questions soient traitées au niveau législatif adéquat.

72. Premièrement, si les actes délégués ou d'exécution ne sont pas encore adoptés lorsque le règlement s'applique, ce qui semble réaliste au regard du grand nombre d'actes envisagés, à savoir 45, l'application efficace et cohérente du règlement pourrait être compromise. Par exemple, tel pourrait être le cas avec le seuil pour la notification des violations des données à caractère personnel. Si aucun acte délégué n'est en place, chaque violation des données devra être notifiée à l'autorité de contrôle nationale.

73. L'absence d'actes délégués ou d'exécution aurait également des conséquences négatives pour l'application des règles par le biais de l'imposition de sanctions administratives, telles que prévues à l'article 79. Un régime de sanction uniforme dans l'UE dépend fortement de l'existence d'une clarté suffisante concernant le sens précis des règles pertinentes, si nécessaire assurée par les actes délégués ou d'exécution. Par exemple, le non-respect de l'obligation de notifier une violation de la protection des données est passible d'une amende pouvant s'élever jusqu'à 1 000 000 d'euros (voir l'article 79, paragraphe 6, point h)). Sans un seuil clair, la pratique nationale pourrait s'avérer hautement incohérente, avec des conséquences négatives pour le marché intérieur.

74. Deuxièmement, il est permis de se demander si les actes délégués prévus dans la proposition de règlement sont tous limités à des éléments non essentiels tels que requis par l'article 290, paragraphe 1, TFUE. Par exemple, le seuil pour la notification de la violation des données à caractère personnel, aux articles 31 et 32, constitue un élément essentiel qui doit être traité dans le règlement. De même, la spécification de ce qui constitue «un degré élevé de risques particuliers» (article 34, paragraphe 2, point a), et paragraphe 8) ou «des motifs importants d'intérêt général» (article 44, paragraphe 1, point d), et paragraphe 7) ne doit pas, selon le CEPD, être complètement laissée aux actes délégués. L'usage de notions vagues ne peut se justifier en accordant à la Commission la compétence pour adopter des actes délégués à un moment donné, dans l'avenir. La sécurité juridique exige que ces notions soient suffisamment définies dans l'acte législatif.

75. Troisièmement, le choix entre un acte délégué et un acte d'exécution n'est pas toujours justifié. Il y a lieu de souligner que le Parlement européen a un rôle plus limité dans la procédure menant à l'adoption d'un acte d'exécution. À cet égard, le CEPD s'interroge en particulier au sujet de la mise en œuvre des actes prévus en relation avec la notification des violations de la sécurité (article 31, paragraphe 6) et l'analyse d'impact relative à la protection des données («AIPD», article 33, paragraphe 7)[28].

76. Dans ce contexte, le CEPD recommande que le législateur reconsidère au moins la délégation de pouvoir visée aux articles 31, paragraphes 5 et 6, 32, paragraphes 5 et 6, 33, paragraphes 6 et 7, 34, paragraphe 2, point a), et 44, paragraphe 1, point d), et paragraphe 7. Le pouvoir d'adopter des actes d'exécution sur la base de l'article 62 sera discuté séparément, dans la partie II.9.b.ii).

II.2.c. Les dispositions particulières pour les micro, petites et moyens entreprises

77. Le chapitre IV de la proposition de règlement contient plusieurs dispositions relatives au responsable du traitement et au sous-traitant, qui créent des exceptions pour les micro, petites et moyennes entreprises («MPME»). C'est notamment le cas de l'obligation pour les responsables du traitement en dehors de l'UE de désigner un représentant (article 25), de la documentation (article 28) et du devoir de désigner un délégué à la protection des données (article 35).

78. En outre, lorsque la Commission est habilitée à adopter des actes délégués ou d'exécution, il est mentionné à plusieurs reprises qu'elle prend les mesures appropriées ou spécifiques pour les MPME. Tel est le cas en ce qui concerne le traitement des données à caractère personnel relatives aux enfants (article 8, paragraphe 3), les procédures et mécanismes pour l'exercice des droits de la personne concernée (article 12, paragraphe 6), l'obligation d'informer la personne concernée (article 14, paragraphe 7), les obligations incombant au responsable du traitement (article 22, paragraphe 4) et l'obligation de procéder à une analyse d'impact relative à la protection des données (article 33, paragraphe 6).

79. Le CEPD reconnaît que la différence de taille d'une entreprise peut influer sur le poids de la charge administrative supplémentaire découlant des règles en matière de protection des données. Toutefois, la protection des données est un droit fondamental, et les personnes ont droit au même niveau de protection de leurs données, indépendamment du

[28] Pour les observations sur l'article 41, paragraphe 3, voir la partie II.7.f, et sur l'article 62, voir la partie II.9.b.ii).

fait que leurs données soient traitées par une MPME ou une grande entreprise. Cela explique l'absence de facilités spéciales pour les MPME dans le contexte des principes généraux pour la protection des données s'appliquant à tous les responsables du traitement. Dans le même temps, il convient de noter que ces principes doivent toujours être appliqués d'une façon qui tienne compte du contexte pertinent. Les charges administratives supplémentaires peuvent être allégées tant que la protection complète de la personne concernée est assurée.

80. Ainsi qu'il sera discuté dans la partie II.6 ci-dessous concernant le responsable du traitement et le sous-traitant, il devrait également être clair que les exceptions aux dispositions du chapitre IV ne doivent concerner que les obligations *spécifiques* élaborées au chapitre IV et non les obligations générales contenues à l'article 22, paragraphes 1 et 3. Ce point devrait être clarifié dans un considérant. Cela étant, le CEPD considère que certaines des exceptions pour les MPME sont trop larges et suggère de réexaminer les obligations spécifiques et la nécessité d'un seuil, ainsi qu'il sera discuté dans la partie II.6.

81. En ce qui concerne les actes délégués et d'exécution, le CEPD s'interroge en particulier en ce qui concerne les mesures spécifiques pour les MPME que la Commission pourrait envisager en adoptant un acte délégué aux fins de préciser les critères et exigences applicables aux méthodes d'obtention du consentement vérifiable donné ou autorisé par un parent de l'enfant ou par une personne qui en a la garde (voir l'article 8, paragraphe 3). En outre, il n'est pas précisé ce que la Commission fera en ce qui concerne l'analyse d'impact en matière de protection des données, qui, selon le CEPD, est une nouvelle obligation essentielle pour garantir la responsabilisation de tous les responsables du traitement, qu'il s'agisse de petites, moyennes ou de grandes entreprises.

82. Le CEPD recommande que le législateur limite les mesures appropriées et spécifiques pour les MPME aux seuls actes d'exécution sélectionnés, et non aux actes délégués, en se concentrant sur les spécifications administratives plutôt que sur les mesures de fond. Il suggère une modification aux articles 8, paragraphe 3, 14, paragraphe 7, 22, paragraphe 4, et 33, paragraphe 6, en ce sens.

II.2.d. La notion de l'«intérêt général»

83. La notion de l'«intérêt général» est utilisée dans toute la proposition de règlement, généralement afin d'autoriser des exemptions à l'application des principes fondamentaux. Pour citer quelques exemples, ainsi qu'il a déjà été discuté, l'article 21 prévoit des limitations éventuelles aux principes fondamentaux de la proposition de règlement sur la base de mesures législatives prises par les États membres pour des intérêts généraux non définis. Le libellé du considérant 87 de la proposition de règlement, qui mentionne des motifs *importants* d'intérêt général, dans le contexte des transferts de données, montre que la notion d'«intérêt général» est envisagée de façon large, dans une perspective pénale mais aussi économique, s'étendant également aux questions de santé et de sécurité sociale.

84. Le CEPD s'oppose à la large utilisation de la notion d'«intérêt général» dans le contexte de la proposition. Au vu de l'impact qu'elle exercerait sur une conformité efficace à ses principales dispositions, il considère que la notion d'«intérêt général» doit être davantage affinée dans chaque disposition de la proposition où elle est mentionnée. Tel est le cas, par exemple, dans le contexte du traitement des données en matière de santé,

où les intérêts généraux sont énumérés en relation avec le domaine de la santé publique (y compris, par exemple, les normes élevées de qualité et de sécurité pour les médicaments). Le CEPD recommande que les intérêts généraux spécifiques soient explicitement identifiés en relation avec le contexte du traitement visé dans chaque disposition pertinente de la proposition[29]. En outre, le CEPD recommande la prise en considération d'exigences supplémentaires pour invoquer un intérêt général. De telles exigences supplémentaires pourraient être, par exemple, que le motif ne puisse être invoqué que dans des circonstances spécifiquement pressantes ou pour des raisons impérieuses prévues par la loi.

85. Des suggestions concrètes sur ce point seront formulées dans la discussion des différents chapitres de la proposition de règlement.

II.3. Dispositions générales (chapitre I)

86. Le CEPD soutient fermement l'objectif de la proposition de règlement visant à harmoniser et simplifier l'application des principes de protection des données dans l'UE. Dans un environnement technologique, où le traitement des données se limite rarement aux frontières territoriales, cet objectif renforcera la sécurité juridique, tant pour les personnes que pour les responsables du traitement. Le CEPD accueille favorablement la clarification apportée par la proposition sur son champ d'application et l'élaboration de la liste des définitions. Certains aspects du texte pourraient être clarifiés ou renforcés.

II.3.a. Champ d'application matériel (article 2)

87. L'article 2 de la proposition de règlement fait référence au traitement de données à caractère personnel, automatisé, ou de données appelées à figurer dans un fichier, d'une façon similaire à la directive 95/46/CE. Paradoxalement, au regard de l'approche horizontale de la protection des données prévue par le traité de Lisbonne, la liste des exemptions de la proposition est plus élaborée que dans la directive 95/46/CE.

i) Sécurité nationale

88. En ce qui concerne l'exception pour les «activités n'entrant pas dans le champ d'application du droit de l'Union», le CEPD souhaite formuler une observation plus générale. Si la «sécurité nationale» n'entre pas dans le champ d'application du droit de l'Union, ce que cette notion recouvre n'apparaît pas toujours très clairement, étant donné qu'elle relève de la politique nationale des États membres. Au niveau national, l'utilisation du libellé «sécurité nationale» ou «sûreté de l'État», selon les États membres, avec un champ d'application différent, peut également prêter à confusion[30]. De toute évidence, le CEPD ne conteste pas l'exception, mais considère qu'il convient d'éviter qu'elle soit indûment utilisée pour légitimer le traitement des données à caractère personnel en dehors du champ d'application du règlement et de la directive, par exemple dans le cadre de la lutte contre le terrorisme.

[29] Voir notamment le considérant 87, les articles 17, paragraphe 5, 44, paragraphe 1, point d), et 81, paragraphe 1, points b) et c), de la proposition de règlement.
[30] Cette confusion est aggravée par des références au «bien-être économique» d'un pays. Elle entraîne également des problèmes avec les autorisations de sécurité qui sont conçues différemment dans les divers États membres.

ii) Institutions et organes de l'UE

89. Le cas spécifique des institutions, organes et organismes de l'Union, mentionné à l'article 2, paragraphe 2, point b), est actuellement traité par le règlement (CE) n° 45/2001. Ainsi qu'il a été discuté dans la partie I.2.a, le CEPD aurait préféré l'inclusion du traitement des données à caractère personnel au niveau de l'Union dans la proposition de règlement. Le règlement (CE) n° 45/2001 devrait à tout le moins être modifié d'une façon compatible avec les propositions actuelles et en permettant son entrée en vigueur lorsque le règlement commencera à s'appliquer.

iii) Activités personnelles et domestiques

90. En ce qui concerne les activités personnelles ou domestiques mentionnées à l'article 2, paragraphe 2, point d), le CEPD déplore que le champ d'application de cette exception ne soit pas davantage précisé. Le considérant 15 indique que l'exception s'applique en l'absence de but lucratif mais ne traite pas la question commune du traitement des données à des fins personnelles à une échelle plus large, tel que la publication d'informations personnelles dans un réseau social.

91. Conformément aux arrêts *Lindqvist* et *Satamedia* de la Cour de justice, le CEPD suggère l'insertion d'un critère pour différencier les activités publiques et domestiques, fondé sur le nombre *indéfini* des personnes pouvant accéder aux informations[31]. Ce critère doit être entendu comme une indication du fait qu'un nombre indéfini de contacts signifie en principe que l'exemption domestique ne s'applique plus. Il est sans préjudice d'une exigence plus stricte concernant un lien personnel et privé, afin d'éviter que des personnes mettant des données à la disposition de plusieurs centaines, voire plusieurs milliers de personnes ne relèvent automatiquement de l'exemption. Le CEPD souhaiterait également conseiller d'ajouter au considérant 15 une clarification quant aux activités susceptibles de s'inscrire dans un espace un peu flou, tel que le site internet d'une communauté locale ou d'un syndicat, qui pourrait impliquer un nombre limité de personnes mais serait néanmoins assujetti au règlement.

92. Enfin, le CEPD accueille favorablement la précision apportée à la fin du considérant 15, selon laquelle l'exception pour les activités personnelles ou domestiques ne s'applique pas aux responsables du traitement de données ou leurs sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités. Il croit comprendre que cette précision implique que les prestataires de services d'information doivent satisfaire au règlement, même si leurs clients utilisent le service dans un contexte personnel. Cela se justifie par le fait que les prestataires de services tels que les réseaux sociaux ou les services informatiques hébergés suivent un modèle commercial spécifique indépendant des objectifs de leurs clients.

93. Le CEPD relève toutefois que le libellé du considérant 15 n'est pas totalement clair étant donné qu'il mentionne que l'exemption domestique ne devrait pas valoir *non plus* dans ce cas. Cette mention, lue dans le contexte de l'ensemble du considérant, pourrait amener à croire que le mot «règlement» a été remplacé par erreur par «exemption», ce qui modifierait complètement le sens du considérant. Le CEPD recommande dès lors la suppression de «non plus» dans le considérant 15.

iv) Autorités compétentes aux fins répressives

[31] Voir l'arrêt de la CJUE du 6 novembre 2003, *Lindqvist*, C-101/01, Recueil 2003, p. I-12971, et l'arrêt de la CJUE du 16 décembre 2008, *Satamedia*, C-73/07, Recueil 2008, p. I-9831.

94. Conformément à l'article 2, paragraphe 2, point e), la proposition de règlement ne s'applique pas au traitement de 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». Conformément au considérant 16, ce traitement fait l'objet d'un instrument juridique spécifique, à savoir la proposition de directive.

95. Le CEPD croit comprendre, sur la base des propositions, que les «autorités compétentes» assujetties à la proposition de directive sont les autorités répressives, ce qui signifie que leurs tâches principales sont liées aux infractions et sanctions pénales. La proposition de règlement s'appliquerait à toutes les autres autorités publiques.

96. Toutefois, la dernière phrase du considérant 16 n'est pas cohérente avec l'article 2, paragraphe 2, point e). Elle présente comme question spécifique (en utilisant le libellé «toutefois») le traitement des données par des autorités publiques dans le cadre du «présent règlement» mais à des fins répressives, en énonçant que ce traitement devrait être régi par cet instrument juridique plus spécifique (la proposition de directive). Le CEPD suggère de rendre le considérant 16 cohérent avec l'article 2, paragraphe 2, point e), pour éviter tout malentendu quant à savoir si les autorités publiques «non répressives» relèveraient du champ d'application de la proposition de règlement.

97. En outre, les deux propositions font respectivement référence aux «autorités compétentes» à l'article 2, paragraphe 2, point e), du règlement et à l'article 1, paragraphe 1, de la directive, alors que la définition de l'article 3, paragraphe 14, de la directive ajoute le critère d'une autorité «publique». Le CEPD suggère d'aligner les deux propositions en ajoutant, à l'article 2, paragraphe 2, point e), du règlement que l'exception s'applique aux autorités *publiques* compétentes. Une modification comparable pourrait également être apportée à l'article 1, paragraphe 1, de la directive.

98. Enfin, le CEPD accueille avec satisfaction le fait qu'il ressort des deux propositions que des acteurs privés traitant les données en relation avec l'exercice de l'autorité publique sont assujettis au règlement et non à la directive, en vertu d'éventuelles limitations nationales conformément à l'article 21. Il s'agit d'une nette amélioration par rapport à la situation actuelle où certaines activités d'acteurs privés, à des fins répressives, ne s'inscrivent pas dans le champ d'application de la directive 95/46/CE, sur la base de l'arrêt *PNR* de la Cour de justice[32]. Toutefois, le CEPD déplore le fait que les conditions dans lesquelles ce type de traitement peut avoir lieu ne soient pas davantage réglementées (voir la partie II.5.f).

II.3.b. Champ d'application territorial (article 3)

99. L'article 3 de la proposition de règlement traite du champ d'application territorial du règlement. Par rapport aux règles actuelles contenues dans la directive 95/46/CE, l'article 3 contient quelques modifications substantielles. Alors que la proposition conserve le critère existant du traitement des données effectué dans le cadre des activités d'un *établissement* d'un responsable du traitement des données sur le territoire de l'Union (article 3, paragraphe 1), il est complété par l'article 3, paragraphe 2, qui abandonne le critère actuel de l'«équipement» en faveur de nouveaux critères consistant en «l'offre de biens ou de services» et «l'observation du comportement» des personnes concernées dans l'Union.

[32] Voir l'arrêt de la CJUE du 30 mai 2006, *Parlement européen/Conseil et Commission*, C-317/04 et C-318/04, Recueil 2006, p. I-4721.

100. Le CEPD soutient les nouveaux critères visant à déterminer quand le droit de l'UE sera applicable aux responsables du traitement qui ne sont pas établis dans l'Union et accueille avec satisfaction les explications données au considérant 21 sur la notion d'«observation du comportement» des personnes concernées. Cette nouvelle disposition est conforme aux recommandations formulées dans l'avis du groupe de travail «Article 29» sur le droit applicable et dans le précédent avis du CEPD sur l'examen du cadre de protection des données[33]. Il considère que l'offre de biens ou de services et l'observation du comportement des personnes concernées dans l'Union est beaucoup plus logique et davantage conforme à la réalité des échanges mondiaux d'informations que le critère existant de l'utilisation d'équipement dans l'Union, aux termes de l'article 4, paragraphe 1, point c), de la directive 95/46/CE.

101. En ce qui concerne les responsables du traitement établis dans l'Union, le règlement s'appliquera directement dans tous les États membres et l'application de l'article 3, paragraphe 1, sera considérablement simplifiée dans le nouveau cadre. Le CEPD soutient pleinement cette évolution en faveur d'une plus grande simplification et sécurité juridique. Il recommanderait toutefois une plus grande clarification ou spécification du critère d'établissement (principal), tel que défini à l'article 4, paragraphe 13, étant donné qu'il s'agit d'un élément essentiel exerçant un impact sur le rôle des autorités de contrôle. Ce point sera développé plus amplement dans la partie II.3.c ci-dessous.

102. Le CEPD note en outre que l'article 3 de la proposition prévoit uniquement la détermination de l'application du droit *de l'UE*. La proposition ne prévoit aucun critère pour les questions de droit *national* applicable. En principe, un règlement rendrait inutile une disposition sur le droit national applicable. Toutefois, ainsi qu'il est souligné dans la partie II.2.a.i), les États membres gardent la possibilité d'adopter une législation spécifique sur la protection des données, p.ex. dans le domaine du travail ou de la santé. Il n'apparaît pas clairement si, et sur quelle base, une loi nationale et sectorielle relative à la protection des données, ou une autre loi nationale pertinente dans ce contexte pourrait être applicable au-delà des frontières de cet État membre.

103. La question pourrait se poser, par exemple, dans le cas d'une multinationale ayant son établissement principal en Irlande et appliquant des règles irlandaises spécifiques en matière de protection des données dans le domaine du travail: ces règles s'appliqueraient-elles à ses filiales établies ailleurs? Dans le contexte de la directive 95/46/CE, le critère du «cadre des activités d'un établissement du responsable du traitement» visé à l'article 4 pourrait entraîner l'application des règles irlandaises au-delà des frontières irlandaises aux autres filiales (à condition qu'elles n'exécutent que les décisions de l'établissement irlandais). Toutefois, la proposition ne contient pas de critère pour traiter des questions de droit *national* applicable: le critère de l'«établissement principal» de la proposition permet seulement de déterminer la façon dont les autorités de contrôle seront impliquées. Dans l'intérêt de la sécurité juridique, le CEPD demande une disposition supplémentaire clarifiant le statut de ces cas (voir également les observations dans la partie II.2.a.i)).

[33] Voir l'avis 8/2010 du groupe de travail «Article 29» du 16 décembre 2010 sur le droit applicable (WP179) et l'avis du CEPD du 14 janvier 2011, points 122 et suivants.

II.3.c. Définitions (article 4)

104. Les définitions de «personne concernée» et de «données à caractère personnel» sont étroitement liées. Par rapport à la directive 95/46/CE, tous les éléments essentiels qui définissent les «données à caractère personnel» dans le présent cadre ont été repris sous la définition de «personne concernée» dans la nouvelle proposition. Les principaux éléments des définitions restent les mêmes, complétés par des détails sur les données de localisation et les identifiants en ligne, que le CEPD accueille avec satisfaction. Il suggèrerait seulement, sur ce point, de mieux distinguer, dans la définition, les identifiants (tels qu'un numéro d'identité, un identifiant en ligne) des éléments ou attributs tels que des informations physiques, génétiques, économiques.

105. À cet égard, le CEPD a des doutes sérieux quant à la dernière phrase du considérant 24 qui mentionne que des «éléments» spécifiques tels que des numéros d'identification ou des identifiants en ligne «ne doivent pas nécessairement être considérés, en soi, comme des données à caractère personnel dans tous les cas de figure». Bien que, de toute évidence, un numéro unique tel qu'un code-barres, considéré isolément, ne puisse être considéré comme une donnée à caractère personnel, dès que cette information a trait à une personne qui peut être identifiée par le responsable du traitement *ou par toute autre personne*, elle devient une donnée à caractère personnel. Dans la pratique, tel sera le plus souvent le cas pour des numéros d'identification ou des appareils personnels, tels que des téléphones mobiles et des ordinateurs portables. Le CEPD est préoccupé par le fait que l'actuel libellé du considérant puisse donner lieu à une compréhension générale erronée de la notion de données à caractère personnel. Il demande une explication plus claire dans ce considérant, dans le sens expliqué ci-dessus, en insistant sur le fait que dès qu'il existe une relation étroite entre un identifiant et une personne, cela générera habituellement l'application des principes relatifs à la protection des données.

106. La notion d'«établissement principal» est développée à l'article 4, paragraphe 13. Si le CEPD accueille avec satisfaction les précisions du considérant 27 concernant le lieu où sont prises les *décisions* principales quant aux finalités, aux conditions et aux modalités du traitement, il déplore que la proposition ne traite pas de la situation des groupes d'entreprises, où plusieurs entités juridiques et leurs établissements dans différents pays peuvent avoir un rôle dans la détermination des finalités, des conditions et des modalités d'une activité de traitement, indépendamment de la localisation de l'administration centrale. Cette situation est traitée dans le contexte des règles d'entreprise contraignantes («REC») mais sans tenir compte de la définition de l'établissement principal, qui se concentre sur le responsable du traitement et non sur le groupe d'entreprises auquel appartiennent le responsable du traitement et d'autres entités juridiques dans le groupe.

107. Le CEPD suggère que les critères pour identifier l'établissement principal du responsable du traitement pertinent soient affinés dans la définition et dans les considérants, en tenant compte de l'«influence dominante» d'un établissement sur d'autres, en lien étroit avec le pouvoir de mettre en œuvre les règles relatives à la protection des données à caractère personnel ou les règles pertinentes pour la protection des données[34]. À titre subsidiaire, la définition pourrait se concentrer sur l'établissement principal de l'ensemble du groupe. Ces différentes options pourraient donner des résultats différents, avec différents avantages et inconvénients pour les autorités de contrôle et les entreprises concernées. Toutefois, il y a lieu de noter que les obligations

[34] Comme, par exemple, les règles en matière de dénonciation.

pertinentes continueraient en tout état de cause à s'adresser aux responsables du traitement, de sorte que les droits des personnes concernées ne seraient pas affectés.

108. Enfin, le CEPD demande une définition de la notion de «transfert» des données à caractère personnel. Il rappelle que cette question s'est avérée problématique et que la Cour de justice a spécifiquement laissé au législateur le soin de la résoudre[35]. La définition de ce qu'est, et de ce que n'est pas, un transfert doit être clairement traitée dans la proposition, notamment en ce qui concerne l'environnement du réseau, où la différence entre un transfert actif et la mise à disposition de données devient théorique alors que les conséquences, en termes de droit applicable, sont énormes pour les responsables du traitement et les personnes.

109. Dans l'arrêt *Lindqvist*, la Cour de justice a précisé qu'une publication sur l'internet ne représentait pas un transfert de données[36]. Toutefois, il n'apparaît pas clairement dans quelle mesure ce raisonnement s'applique également aux autres types d'échanges sur des réseaux, tels que les serveurs d'entreprises. Le CEPD souhaite présenter les éléments éventuels qui pourraient contribuer à l'identification d'un transfert. Le fait qu'il soit destiné à communiquer des données aux destinataires identifiés (au lieu de mettre ouvertement des données à disposition) pourrait être pris en considération, étant donné qu'il justifie le niveau de protection garanti par le (pays du) destinataire, ainsi que les éventuelles mesures à prendre pour assurer la protection des données. D'autres éléments à prendre en considération sont le fait que les données aient été mises librement à disposition dans le but d'y donner accès et le fait que le transfert soit susceptible d'avoir réellement atteint un ou plusieurs destinataires à l'étranger.

110. Enfin, le CEPD note qu'à l'article 3, paragraphe 4, de la proposition de directive, une définition est donnée de la notion de «limitation du traitement». Dans la proposition de règlement, cette notion est utilisée à l'article 17, paragraphe 4, en relation avec le droit à l'oubli. Par souci de cohérence et de clarté du concept de limitation du traitement dans les deux propositions, le CEPD recommande d'insérer également une définition de la notion de «limitation du traitement» à l'article 4 de la proposition de règlement et de développer davantage cette définition (dans les deux propositions) dans le sens de l'article 17, paragraphe 5, de la proposition de règlement (voir également la partie III.5.e).

II.4. Principes (chapitre II)

111. Le chapitre II de la proposition de règlement présente les principes à respecter pour tout traitement de données à caractère personnel (article 5) et les conditions dans lesquelles un traitement est licite (article 6). Il traite également de certaines situations spécifiques, notamment le traitement de catégories particulières de données («données sensibles») et du traitement de données qui ne permet pas l'identification d'une personne physique.

112. Les consultations publiques lancées par la Commission à partir de 2009 ont confirmé que les principes fondamentaux consacrés par la législation de l'Union en matière de protection des données restent applicables[37]. Toutefois, elles ont également montré que ces principes doivent être reconsidérés afin de tenir compte du rythme rapide de l'évolution technologique et de la mondialisation accrue.

[35] Voir l'arrêt *Lindqvist* de la CJUE, cité à la note de bas de page 31.
[36] *Ibidem*.
[37] Voir l'exposé des motifs joint à la proposition de règlement, p. 4.

113. Le CEPD accueille avec satisfaction le fait que le chapitre II de la proposition de règlement se fonde sur ces principes bien établis de la protection des données et présente des améliorations significatives. La notion de «consentement» est notamment la bienvenue.

II.4.a. Principes concernant le traitement des données à caractère personnel, y compris la limitation de la finalité (article 5)

114. L'article 5 de la proposition apporte plusieurs améliorations à l'article 6 de l'actuelle directive 95/46/CE:
- conformément à l'article 5, point a), les données à caractère personnel doivent être traitées non seulement de manière licite et loyale, mais aussi avec transparence au regard de la personne concernée. Cet ajout utile reflète l'introduction d'obligations plus strictes pour le responsable du traitement d'informer les personnes concernées (voir notamment l'article 14);
- le principe de la «minimisation des données» est explicitement mentionné à l'article 5, point c). Conformément à cette disposition, les données à caractère personnel doivent être limitées au minimum nécessaire et ne sont traitées que si les finalités du traitement ne peuvent être atteintes par d'autres moyens. Bien que, sur le fond, cette obligation existe déjà en vertu des règles actuelles, le CEPD se réjouit de la visibilité qui lui est donnée par l'ajout à l'article 5, point c);
- conformément à l'article 5, point f), le responsable du traitement doit non seulement veiller à la conformité au règlement, mais aussi démontrer celle-ci. Cette disposition établit le principe de la responsabilité du responsable du traitement qui est plus amplement spécifiée au chapitre IV.

115. Conformément au principe de limitation de la finalité, les données à caractère personnel doivent être collectées pour des finalités déterminées et ne pas être traitées ultérieurement de manière incompatible avec cette finalité. Le principe fondamental de la directive 95/46/CE est conservé à l'article 5, point b).

116. Toutefois, l'efficacité du principe de limitation de la finalité dépend 1) de l'interprétation de la notion de «compatibilité d'utilisation» et 2) des éventuelles dérogations au principe de limitation de la finalité, en d'autres termes, des possibilités et conditions pour une utilisation *incompatible*.

117. Le CEPD est conscient du fait que la notion de «compatibilité d'utilisation» est interprétée différemment d'un État membre à l'autre. Dès lors, le CEPD demande une précision supplémentaire dans la proposition de règlement.

118. La proposition de règlement constitue l'instrument adéquat pour développer ce principe, en s'inspirant éventuellement des meilleures pratiques dans la façon dont la «compatibilité» a été interprétée au niveau national. Le CEPD soutient le fait que la question de la compatibilité soit mentionnée comme l'un des principaux sujets à traiter par le groupe de travail «Article 29» dans son programme de travail pour 2012-2013[38]. Il devrait en résulter une contribution précieuse pour une compréhension commune de la notion de «compatibilité».

119. En ce qui concerne les possibilités et conditions d'une utilisation incompatible, la logique de la directive 95/46/CE veut que cette utilisation incompatible ne soit autorisée

[38] Voir le programme de travail 2012-2013 du groupe de travail «Article 29» du 1er février 2012 (WP 190).

que sous réserve des conditions de l'article 13 pour certaines raisons d'intérêt général. Dans la proposition de règlement, il s'agirait de l'article 21 (voir les observations plus approfondies sur cette disposition dans la partie II.5.f ci-dessous).

120. Toutefois, le CEPD relève qu'un nouveau paragraphe 4 est ajouté à l'article 6 sur la licéité du traitement qui ouvre des possibilités de traitement pour d'autres finalités incompatibles que celles énoncées à l'article 21, et n'est pas rédigé en tant que dérogation au principe de limitation de la finalité. Le traitement est autorisé pour autant qu'il trouve une base juridique dans l'article 6, paragraphe 1, points a) à e). Seul le motif contenu à l'article 6, paragraphe 1, point f), l'équilibre des intérêts, ne peut être invoqué en vue d'une utilisation ultérieure pour une finalité incompatible aux termes de l'article 6, paragraphe 4.

121. Le CEPD émet de fortes réserves à l'égard de cette nouvelle disposition, qui suppose de larges conséquences pratiques et modifie l'esprit du principe de limitation de la finalité tel que nous le connaissons actuellement. Elle offre de vastes possibilités de réutilisation des données à caractère personnel, notamment dans le secteur public, dans les cas fondés sur l'article 5, points c) et e), où le responsable du traitement est soumis à une obligation légale, ou en cas d'intérêt général ou d'exercice d'une autorité dont le responsable du traitement est officiellement investi, sans aucune assurance que la violation du principe de limitation de la finalité a été considérée séparément et de manière adéquate.

122. De même, en cas de traitement des données pour une finalité incompatible dans le cadre d'un contrat avec la personne concernée, cette disposition n'est pas la bienvenue. Bien que l'on puisse argumenter, à première vue, que dans cette situation, la personne concernée retrouve le contrôle de la situation, dans la pratique, l'influence des parties à un contrat n'est pas toujours équilibrée et il existe de solides doutes qu'une personne soit réellement en mesure de réagir à une utilisation incompatible de ses données à caractère personnel dans une relation contractuelle.

123. Le CEPD rappelle que l'exigence de la compatibilité d'utilisation et l'exigence de la licéité sont deux conditions cumulatives qui visent à garantir un traitement conforme des données à caractère personnel. L'exigence de la compatibilité ne peut être levée en se référant simplement à une condition de licéité du traitement. Cela serait contraire à l'article 5 de la convention 108 du Conseil de l'Europe. C'est plutôt l'article 21 qui doit veiller à ce qu'un changement de finalité s'effectue dans des conditions strictes.

124. Dès lors, le CEPD recommande de maintenir la logique de la directive 95/46/CE et de ne pas affaiblir le principe de limitation de la finalité, en supprimant l'article 6, paragraphe 4, ou à tout le moins en limitant son champ d'application au traitement ultérieur des données pour des finalités incompatibles aux motifs contenus à l'article 6, paragraphe 1, point a), le consentement, et à l'article 6, paragraphe 1, point d), les intérêts vitaux de la personne concernée. Cela nécessiterait également une modification du considérant 40.

II.4.b. Licéité du traitement (articles 6, 7 et 8)

i) Consentement

125. Le consentement de la personne concernée constitue le premier motif légal, à l'article 6, paragraphe 1, pour le traitement des données à caractère personnel, à condition que certaines conditions soient remplies.

126. Le CEPD se réjouit de constater que, se fondant sur l'avis récent du groupe de travail «Article 29»[39], la proposition traite de la notion de «consentement» de manière complète et adéquate afin de spécifier davantage et renforcer ces conditions.

127. L'article 7 introduit de nouveaux éléments positifs, notamment en imposant la charge de la preuve au responsable du traitement, en introduisant des garanties dans le contexte d'une déclaration écrite et en excluant la validité du consentement lorsqu'il existe un déséquilibre significatif entre la position de la personne concernée et du responsable du traitement. Le considérant 34 présente certains exemples de situations où il existe un déséquilibre manifeste, tel que le contexte de l'emploi ou lorsque le responsable du traitement est une autorité publique.

128. L'article 8 traite séparément la question du consentement donné par un enfant dans un environnement en ligne. L'exigence d'une autorisation donnée par un parent de l'enfant ou par une personne qui en a la garde pour les enfants de moins de 13 ans constitue une approche raisonnable.

129. Le considérant 25, qui traite de façon plus générale de la question du consentement dans un environnement en ligne, a été précisé à l'aide d'ajouts utiles. Le CEPD considère que ce considérant doit spécifier en outre que lors de la visite d'un site internet, il est nécessaire de cocher activement une case pour garantir un consentement valide, étant donné que les cases pré-cochées ne satisfont pas aux exigences en matière de consentement. Il rappelle également que la charge de la preuve incombe au responsable du traitement et que la fiabilité du consentement peut varier largement en fonction des moyens utilisés, qui vont des cases à cocher aux signatures électroniques. Le responsable du traitement doit dès lors être attentif au niveau de fiabilité des moyens utilisés pour obtenir un consentement, notamment en tenant compte de la sensibilité du traitement. Tous ces points doivent être spécifiés dans les considérants. Étant donné que le responsable du traitement supporte la charge de la preuve d'un consentement valide, il est dans son intérêt de prévoir des moyens fiables pour obtenir le consentement.

130. Dans ce contexte, le CEPD relève que la proposition de règlement ne traite pas de la question de la représentation (légale) de la personne concernée de manière plus générale. Le CEPD recommande l'inclusion d'une disposition sur cette question, couvrant la représentation de toutes les personnes ne disposant pas d'une capacité (juridique) suffisante ou n'étant pas en mesure d'agir. Cette disposition doit non seulement traiter des conditions du consentement, mais doit également traiter de la façon dont un représentant peut exercer les droits de ces personnes en leur nom. Il convient de ce fait de tenir dûment compte d'un éventuel conflit d'intérêts entre la personne et son représentant.

[39] Voir l'avis 15/2011 du groupe de travail «Article 29» du 13 juillet 2011 sur la définition du consentement (WP 187).

ii) Autres bases juridiques pour un traitement licite

131. L'article 6, paragraphe 1, établit cinq motifs en vertu desquels une opération de traitement est licite sans consentement. Cette disposition est dans une large mesure similaire à l'article 7 de la directive 95/46/CE.

132. La principale différence réside dans le fait que les intérêts légitimes du responsable du traitement, visés à l'article 6, paragraphe 1, point f), seraient exclus en tant que motif valide pour un traitement effectué par les autorités publiques dans l'exécution de leurs missions[40]. Comme expliqué au considérant 38, cela est lié au fait qu'aux termes de l'article 6, paragraphe 3, le fondement de leur traitement doit être uniquement prévu dans le droit.

133. Le CEPD recommande l'ajout, dans un considérant, d'une nouvelle indication de ce que peut exactement couvrir l'obligation légale ou les missions effectuées «dans l'intérêt général ou relevant de l'exercice de l'autorité publique» comme mentionné à l'article 6, paragraphe 1, point e), de la proposition de règlement. Le considérant pourrait mentionner, dans le même esprit que le considérant 27 du règlement (CE) n° 45/2001, que les missions effectuées dans l'intérêt général comprennent le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces autorités.

II.4.c. Traitement portant sur des catégories particulières de données (article 9)

134. Les données relatives aux condamnations pénales et aux mesures de sûreté connexe font partie des données à caractère personnel qui, de par leur nature, sont particulièrement sensibles et méritent une attention spécifique. L'article 9, paragraphe 2, point j), de la proposition introduit une certaine flexibilité supplémentaire dans le régime juridique actuel, conformément à l'article 8, paragraphe 5, de la directive 95/46/CE, pour le traitement de ces données par d'autres personnes que l'autorité officielle, par exemple, par un responsable du traitement soumis à une obligation légale ou réglementaire.

135. Toutefois, il n'apparaît pas clairement de quelle façon l'article 9, paragraphe 2, point j), se rapporte aux autres motifs d'exception visés à l'article 9, paragraphe 2. Plus particulièrement, la référence à l'exécution d'une mission effectuée dans l'intérêt général doit être clarifiée par rapport au motif exposé à l'article 9, paragraphe 2, point g). Si l'intention est de fixer un seuil plus élevé à l'article 9, paragraphe 2, point j), cela doit être rendu explicite. En outre, le CEPD ne distingue aucune raison pour laquelle l'exigence de contrôle de l'autorité officielle ne devrait pas s'étendre à tous les motifs indiqués à l'article 9, paragraphe 2, point j), y compris lorsqu'une mission est effectuée pour des raisons importantes d'intérêt général.

136. Le CEPD note également que la proposition de règlement n'inclut plus le traitement de données liées à des infractions dans les catégories particulières de données. Sur ce point, le champ d'application de cette disposition est à présent limité aux condamnations pénales ou aux mesures de sûreté connexes. Le CEPD n'est pas convaincu que la suppression de cette catégorie de données soit justifiée. En outre, le traitement de données relatives à des questions n'ayant pas donné lieu à des condamnations (telles que des soupçons) devrait également être inclus, étant donné qu'il peut entraîner des décisions injustes à l'égard de la personne concernée. Elles méritent, à son avis,

[40] Une autre différence (inexpliquée), aux conséquences pratiques, est le fait que l'article 6, paragraphe 1, points e) et f), fait à présent uniquement référence au responsable du traitement et non plus aux «tiers auxquels les données sont communiquées».

l'adoption de garanties spécifiques, au moins égales à celles s'appliquant aux condamnations.

137. Les règles spécifiques pour le traitement des données concernant la santé (voir l'article 81) seront traitées au chapitre III.11 ci-dessous.

II.4.d. Traitement ne permettant pas l'identification (article 10)

138. L'article 10 de la proposition de règlement est une nouvelle disposition établissant qu'un responsable du traitement n'est pas tenu d'obtenir des informations à caractère personnel pour identifier la personne concernée à la seule fin de respecter le règlement. Le CEPD croit comprendre que cette disposition ne modifie pas la notion de données à caractère personnel, ni le champ d'application du règlement, mais a été ajoutée afin de traiter les questions pratiques spécialement soulevées par les responsables du traitement des données qui ne peuvent identifier directement la personne derrière les données, notamment dans l'environnement en ligne tel que décrit au considérant 24.

139. Toutefois, le CEPD considère que l'article 10 ne doit en aucune façon entraver les droits des personnes concernées, notamment en ce qui concerne l'accès à leurs informations. Le considérant 45 traite déjà de cette question mais doit être rendu plus explicite en expliquant que le responsable du traitement des données ne doit pas être en mesure d'invoquer une éventuelle absence d'informations pour rejeter une demande d'accès, lorsque ces informations peuvent être fournies par la personne concernée pour permettre cet accès.

II.5. Droits de la personne concernée (chapitre III)

140. Le CEPD accueille favorablement le renforcement des droits des personnes concernées au moyen, d'une part, de mesures renforçant les obligations incombant aux responsables du traitement pour garantir l'exercice efficace de ces droits (par exemple, l'obligation d'adopter des procédures et des mécanismes, de répondre aux demandes d'accès dans les délais impartis, de motiver leur refus de prendre des mesures ou d'informer les destinataires de toute rectification ou effacement) et, d'autre part, du renforcement de la portée des droits actuels (tels que le droit à l'effacement, qui a été renforcé dans un droit à l'oubli) ainsi que de la création d'un nouveau droit à la portabilité des données.

141. Toutefois, la mesure dans laquelle le droit à l'oubli peut être applicable dans la pratique reste peu claire. En outre, la portée des limitations qui peuvent être appliquées à l'exercice des droits des personnes concernées a été étendue sans être bien définie, ce qui demanderait l'application de garanties supplémentaires afin de veiller à ce que ces droits ne soient pas indûment limités.

II.5.a. Transparence et informations à fournir à la personne concernée (articles 11 et 14)

142. Les dispositions sur la transparence de l'information et de la communication constituent une amélioration importante des dispositions existantes exposées aux articles 10 et 11 de la directive 95/46/CE. Le CEPD accueille favorablement l'obligation générale et explicite, faite aux responsables du traitement, de communiquer avec la personne concernée sur la protection des données, en utilisant un langage clair et simple (voir l'article 11 de la proposition de règlement). En outre, le CEPD accueille favorablement la spécification du type d'informations qui doivent être fournies par le responsable du

traitement à la personne concernée lorsque ses données à caractère personnel sont collectées.

143. À cet égard, l'article 14 prévoit une liste de toutes les informations qui doivent être fournies par le responsable du traitement à la personne concernée sur une base obligatoire. Celles-ci peuvent inclure «toute autre information nécessaire pour assurer un traitement loyal des données» (voir l'article 14, paragraphe 1, point h)).

144. Le CEPD recommande de préciser, à l'article 14, que ces informations supplémentaires doivent notamment couvrir les informations sur l'existence de certaines opérations de traitement qui exercent un impact particulier sur les personnes, telles que celles pour lesquelles une analyse d'impact relative aux données à caractère personnel indique qu'il existe un risque élevé (voir l'article 33) et les mesures fondées sur le profilage (article 20), ainsi que les conséquences d'un tel traitement sur les personnes. Cette modification rendrait également l'article 14 cohérent avec d'autres dispositions de la proposition de règlement où ce droit à l'information sur le profilage est clairement mentionné, à savoir l'article 15, paragraphe 1, point h), sur le droit d'accès et l'article 20, paragraphe 4, sur les mesures fondées sur le profilage.

145. Il y a lieu de noter, dans le même temps, que l'article 14 ne s'oppose pas aux meilleures pratiques utilisant des «notifications à plusieurs niveaux», qui permettent différentes couches d'informations, offrant aux personnes toutes les informations nécessaires pour comprendre leur position et prendre des décisions sous une forme plus compréhensible[41]. Il ne requiert pas non plus la fourniture d'informations lorsque la personne concernée les a déjà reçues précédemment, permettant dès lors aux responsables du traitement d'organiser les activités d'information de la façon la plus efficace et la plus adéquate possible.

II.5.b. Droit à l'oubli et à l'effacement (article 17)

146. Le droit à l'effacement a été renforcé par un droit à l'oubli afin de permettre une application plus efficace de ce droit dans l'environnement numérique. Le responsable du traitement sera tenu pour responsable dans les cas où il aura rendu publiques des données à caractère personnel ou dans les cas où il aura autorisé la publication des données par un tiers[42]. Toutefois, les obligations se limitent à la prise de «toutes les mesures raisonnables» en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci. Ces «mesures raisonnables» pourraient consister en la mise en œuvre de mesures techniques.

147. Dès lors, l'article 17 contient une obligation d'*effort* faite au responsable du traitement qui est plus réaliste, d'un point de vue pratique, qu'une obligation de *résultat*. Il reflète également l'article 13 (sur les droits à l'égard des destinataires) qui dispose que le responsable du traitement doit être exempté de l'obligation d'informer tous les destinataires de toute rectification ou tout effacement lorsqu'une telle communication «se révèle impossible ou suppose un effort disproportionné».

[41] Voir notifications à plusieurs niveaux: avis 10/2004 du groupe de travail «Article 29» du 25 novembre 2004 sur les dispositions davantage harmonisées en matière d'informations (WP 100).
[42] La notion d'«autorisation» d'un tiers à publier des données n'est pas définie et a besoin d'être clarifiée davantage.

148. Le CEPD accueille favorablement cette disposition, mais souligne que le droit à l'oubli doit être effectif dans la réalité. Dans certains cas, ce peut être un effort énorme d'informer tous les tiers qui peuvent être occupés à traiter ces données, étant donné qu'il n'y aura pas toujours une compréhension claire des lieux où les données ont pu être diffusées. Avoir un droit à l'oubli effectif implique que la portée de ce droit doit être claire dès le moment où le règlement s'applique. L'article 17 pourrait devoir être développé davantage à cet égard.

149. L'article 17, paragraphe 3, prévoit des motifs pour une exception à l'effacement des données sans délai. Ce paragraphe fait double emploi et ne présente dès lors aucune valeur ajoutée pour le système des exemptions, des restrictions et des règles spécifiques déjà prévues dans la proposition de règlement (voir également les observations dans la partie II.2.a.iii)). Plus particulièrement, l'article 17, paragraphe 3, point d), ne fera que susciter la confusion. Une restriction du principe de limitation de la finalité et des droits de la personne concernée (y compris l'article 17) doit être fondée sur l'article 21, sous réserve des observations formulées dans la partie II.5.f ci-dessous. Dès lors, le CEPD recommande la suppression de l'article 17, paragraphe 3.

II.5.c. Droit à la portabilité des données (article 18)

150. L'article 18 crée un nouveau droit permettant aux personnes concernées d'obtenir une copie de leurs données à caractère personnel faisant l'objet d'un traitement dans un format électronique et de les transmettre d'un prestataire de services électroniques à un autre. Selon le CEPD, la relation du droit pour les personnes concernées d'obtenir une «copie» de leurs données en vertu de cette disposition avec leur droit d'obtenir «une communication des données à caractère personnel faisant l'objet d'un traitement» dans le cadre de l'exercice de leur droit d'accès devrait être précisée davantage.

151. En outre, le texte de l'article 18, paragraphe 2, semble limiter la portée du droit à la portabilité des données aux données à caractère personnel qui ont été fournies par la personne concernée sur la base d'un consentement ou d'un contrat. Cela soulève la question de savoir si le droit ne devrait pas être étendu aux données qui ont été collectées pour d'autres motifs également.

152. En ce qui concerne le contenu du droit, il n'apparaît pas clairement, dans le texte actuel, de quelle façon le droit à la portabilité des données se rapporte au droit à l'effacement et si les données doivent être effacées par le responsable du traitement une fois que le droit a été invoqué. L'utilisation du mot «copie» à l'article 18, paragraphe 1, semble impliquer le contraire. Toutefois, le responsable du traitement est toujours soumis à l'obligation d'effacer les données lorsqu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été traitées (article 5, point e)), hormis dans les cas où le responsable du traitement aurait toujours une base juridique valable pour continuer à traiter certaines des données (par exemple, pour satisfaire à une obligation légale, telle que des fins fiscales). Le CEPD recommande qu'il soit précisé, à l'article 18, que l'exercice du droit à la portabilité des données est sans préjudice de l'obligation d'effacer les données lorsqu'elles ne sont plus nécessaires, conformément à l'article 5, paragraphe e).

II.5.d. Droit d'opposition (article 19)

153. Le CEPD accueille favorablement l'intention de la Commission de renforcer le droit d'opposition. Les modifications apportées au droit d'opposition sont destinées à améliorer le droit actuellement prévu, à l'article 14 de la directive 95/46/CE. En

particulier, parce qu'il ne sera plus requis de la part de la personne concernée de démontrer des «raisons impérieuses et légitimes» en relation avec la situation spécifique de la personne (voir l'article 14, point a), de la directive 95/46/CE). La charge de la preuve reviendrait au responsable du traitement chaque fois qu'il refuserait de faire droit à l'opposition reçue d'une personne concernée.

154. Toutefois, il convient de préciser davantage quelles sont les conséquences pratiques si le droit est invoqué. À l'article 19, paragraphe 3, il est mentionné que lorsqu'il est «fait droit» à une opposition, le responsable du traitement *n'utilise plus ni ne traite plus* les données à caractère personnel concernées. Cela soulève la question de savoir quand et comment il «est fait droit» à une opposition. En outre, il n'est pas précisé ce que le responsable du traitement est supposé faire des données en cas de désaccord avec la personne concernée et si aucune décision d'une autorité de contrôle, par exemple, n'a encore été prise.

155. Il semble résulter de l'article 17, paragraphe 1, point c), que les données doivent en principe être effacées: la personne concernée a le droit d'obtenir du responsable du traitement l'*effacement* de ses données à caractère personnel et l'abstention à l'égard d'une diffusion ultérieure si elle s'oppose au traitement conformément à l'article 19. Il n'apparaît pas clairement si les exceptions prévues à l'article 17, paragraphe 4, point b), qui permettent la restriction au lieu de l'effacement des données, peuvent être invoquées en cas de désaccord concernant la question de savoir si le droit d'opposition doit être observé. Le CEPD recommande au législateur de préciser la relation entre l'article 17 et l'article 19 et de traiter clairement la question de savoir ce que le responsable du traitement doit faire en cas de désaccord avec la personne concernée.

156. En outre, le CEPD recommande d'expliquer dans un considérant ce qui peut être qualifié de «raisons impérieuses et légitimes» justifiant le refus de l'exercice du droit d'opposition.

II.5.e. Mesures fondées sur le profilage (article 20)

157. L'article 20 se fonde sur l'article 15 existant de la directive 95/46/CE sur les décisions individuelles automatisées et étend son champ d'application à tous les types de mesures qui produisent des effets juridiques sur une personne physique, et pas seulement aux décisions. Il s'appliquerait non seulement au traitement destiné à évaluer certains aspects personnels, mais aussi aux activités destinées à analyser ou prévoir ces aspects, incluant dès lors une plus large catégorie de traitement. Il introduit également plusieurs catégories d'aspects personnels qui relèvent du champ d'application de cette disposition, telles que le traitement concernant la situation économique d'une personne, sa localisation, son état de santé et ses préférences personnelles.

158. L'article 20, paragraphe 2, expose les conditions dans lesquelles ce type de traitement peut avoir lieu par voie de dérogation. L'article 20, paragraphe 2, point a), donne aux personnes concernées le droit d'obtenir une intervention humaine, mais non le droit de soumettre leur point de vue, tel que le prévoit actuellement l'article 15 de la directive 95/46/CE. Le CEPD recommande que ce dernier droit soit restauré à l'article 20, paragraphe 2, point a). Il permettrait notamment aux personnes d'être entendues avant que ne soit prise une mesure qui les affecte de façon significative, ce qui renforcerait l'équité d'un tel traitement.

II.5.f. Limitations (article 21 et considérant 59)

159. À l'article 21, la proposition de règlement introduit plusieurs limitations possibles aux droits et obligations exposés dans le règlement. Cette disposition a déjà été brièvement discutée dans la partie II.2.a.iii) ci-dessus. Ainsi qu'il y est mentionné, la disposition est placée dans un chapitre erroné de la proposition de règlement, étant donné qu'elle ne se rapporte pas uniquement aux droits des personnes concernées. En outre, le CEPD demande de limiter le recours à l'exemption pour des raisons d'intérêt général dans cette disposition à des circonstances clairement identifiées et limitées, dont les infractions pénales ou les intérêts économiques et financiers (voir également la partie II.2.d ci-dessus).

160. La portée des limitations éventuelles a été considérablement élargie par rapport à ce qui est actuellement prévu à l'article 13 de la directive 95/46/CE. Tous les droits de la personne concernée peuvent à présent être limités sur le fondement de l'article 21 (y compris le droit d'opposition et les mesures fondées sur le profilage). En outre, des limitations sont possibles en ce qui concerne les principes fondamentaux en matière de protection des données contenus à l'article 5, points a) à e), et l'obligation de notifier une violation des données à caractère personnel à la personne concernée (article 32).

161. Les limitations doivent être imposées dans le droit de l'Union ou d'un État membre. Le CEPD considère qu'une loi fondée sur l'article 21 doit satisfaire aux critères de tout droit dérogatoire à un droit fondamental, ainsi qu'il est rappelé dans le considérant 59, et notamment aux critères de nécessité et de proportionnalité. Il ne suffit pas que ce droit se limite à spécifier les objectifs et le responsable du traitement, comme prévu à l'article 21, paragraphe 2.

162. Le CEPD recommande dès lors l'introduction de garanties détaillées dans le texte de l'article 21, à savoir que ce droit doit spécifier les objectifs poursuivis par le traitement, les catégories de données à caractère personnel à traiter, les finalités et moyens spécifiques du traitement, le responsable du traitement, les catégories de personnes autorisées à traiter les données, la procédure à suivre pour le traitement et les garanties contre toute interférence arbitraire de la part des autorités publiques. Il est nécessaire de définir avec une clarté et une certitude suffisantes les domaines spécifiques pour lesquels le droit doit prévoir des garanties détaillées afin de préserver les intérêts légitimes des personnes concernées dans les cas où une telle limitation s'applique. Afin d'éviter des interprétations divergentes, ces limitations devraient être davantage harmonisées au niveau de l'UE.

163. En outre, des garanties supplémentaires devraient également être incluses à l'article 21 dans le sens de celles prévues à l'article 20, paragraphes 2 à 5, du règlement (CE) n° 45/2001, telles que la communication aux personnes concernées d'une limitation et de leur droit de saisir l'autorité de contrôle afin d'obtenir un accès indirect par le biais de l'autorité de contrôle chaque fois que leur droit à un accès direct est limité conformément à l'article 21.

164. Cette situation amène une autre question plus spécifique, à savoir l'application des limitations, conformément à l'article 21, aux données collectées par des responsables du traitement privés, à des fins répressives, qui pourraient donner lieu à un traitement ultérieur sans devoir respecter aucune des garanties fondamentales énoncées à l'article 5. Il doit être précisé, à l'article 21, que la possibilité d'appliquer des limitations au traitement effectué par des responsables du traitement privés à des fins répressives ne

doit pas les forcer à conserver des données en plus de celles qui sont strictement nécessaires pour la finalité originale poursuivie, ni à modifier leur architecture informatique afin de répondre à toute requête éventuelle de la part d'une autorité répressive.

165. Le CEPD suggère de supprimer le motif contenu à l'article 21, paragraphe 1, point e), qui autorise des limitations en cas de «mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique» dans les cas de sûreté publique, infraction pénale ou autres intérêts généraux. Bien que ce libellé ne soit pas nouveau (voir l'article 13, paragraphe 1, point f), de la directive 95/46/CE), le CEPD estime qu'il est trop vague au regard de la nature du lien avec l'exercice de l'autorité officielle, notamment si, et dans la mesure où, des acteurs privés traiteraient des données à caractère personnel en liaison avec l'exercice de l'autorité publique. En tout état de cause, les autres motifs visés à l'article 21, paragraphe 1, offrent déjà une flexibilité suffisante.

II.6. Responsable du traitement et sous-traitant (chapitre IV)

166. Le CEPD accueille favorablement les importantes améliorations exposées au chapitre IV. Ce chapitre introduit le «principe de responsabilité» de plus en plus connu, qui met davantage l'accent sur la responsabilité du responsable du traitement[43]. En règle générale, le responsable du traitement doit adopter des politiques et mettre en œuvre des mesures appropriées afin de pouvoir *démontrer* la conformité aux règles en matière de protection des données et veiller à ce que l'efficacité des mesures soit vérifiée (voir l'article 22, paragraphes 1 et 3). En dépit de la difficulté de la traduction de ce concept, le CEPD recommande de faire explicitement référence au principe de responsabilité, en tout état de cause au considérant 60.

167. Dans ce contexte, la proposition de règlement introduit les principes de la protection des données dès la conception et par défaut et les obligations de conserver les documents relatifs à toutes les opérations de traitement, de notifier les infractions à la sécurité, de réaliser une analyse d'impact relative à la protection des données avant d'entreprendre certaines opérations de traitement qui pourraient donner lieu à une consultation préalable de l'autorité de contrôle, et de désigner un délégué à la protection des données.

168. Dans tout ce chapitre, des exceptions sont prévues pour les MPME ainsi que pour les autorités publiques. À cet égard, le CEPD souhaite réitérer l'observation formulée dans la partie II.2.c selon laquelle ces exceptions ne doivent concerner que les obligations spécifiques exposées au chapitre IV et non les obligations générales contenues à l'article 22, paragraphes 1 et 3. Cette observation est reflétée dans le texte actuel de la proposition de règlement, que le CEPD soutient pleinement.

169. Cela étant, bien qu'il soit nécessaire de prendre en considération la taille d'une entreprise spécifique avant de mettre en œuvre l'obligation spécifique, le CEPD considère que certaines des exemptions pour les MPME sont trop larges et que certaines des obligations spécifiques sont trop détaillées. En outre, les exceptions pour les autorités publiques ne sont pas toujours justifiées. Ces points seront plus amplement discutés ci-dessous.

[43] Avis 3/2010 du groupe de travail «Article 29» du 13 juillet 2010 sur le principe de la responsabilité (WP 173).

II.6.a. Obligations incombant au responsable du traitement (article 22)

170. L'article 22, paragraphe 1, développe le principe général contenu à l'article 5, point f), de la proposition de règlement, à savoir que le responsable du traitement doit garantir et démontrer la conformité au règlement. Cela entraîne l'obligation générale d'adopter des politiques et de mettre en œuvre des «mesures appropriées» qui lui permettent de satisfaire à ce principe. Comme indiqué, le CEPD accueille favorablement cette obligation générale étant donné qu'elle souligne la nouvelle approche fondée sur la responsabilité du responsable du traitement.

171. L'article 22, paragraphe 2, énumère les mesures qui sont particulièrement visées par le premier paragraphe de l'article 22. Le CEPD accueille favorablement cette spécification, sous réserve de quelques nouvelles observations, et soutient également le fait que la liste ne soit pas présentée comme exhaustive. Le principe général de responsabilité ne doit pas être interprété comme étant limité aux obligations spécifiques visées à l'article 22, paragraphe 2.

172. L'article 22, paragraphe 3, contient un important élément supplémentaire pour le responsable du traitement, à savoir qu'il doit également mettre en œuvre des mécanismes pour vérifier l'«efficacité» des mesures énoncées ci-dessus. Cette obligation s'applique sans exception, bien que la façon dont la vérification doit être réalisée – par exemple, par un auditeur indépendant interne ou externe – dépende des circonstances spécifiques (proportionnalité).

173. Au cœur des obligations générales se trouvent dès lors les exigences selon lesquelles les mesures doivent être *appropriées* et *efficaces*. Ce second élément résulte directement des termes de l'article 22, paragraphe 3. Le CEPD estime qu'il serait préférable d'exprimer les deux éléments à l'article 22, paragraphe 1, et recommande de modifier la disposition en conséquence.

174. Le terme «appropriées» implique que les mesures doivent tenir compte du contexte et des circonstances spécifiques de l'affaire. Il s'agit d'un élément important qui garantit la «modularité» de l'obligation générale dans la pratique, à savoir que des mesures efficaces peuvent être requises dans *toutes* les circonstances, d'une façon appropriée au cas pertinent.

175. Il n'apparaît pas clairement quelles mesures peuvent être requises – en dehors de celles spécifiquement visées à l'article 22, paragraphe 2 – bien que l'article 22, paragraphe 4, prévoie des actes délégués pour les spécifier. Toutefois, il ressort de l'article 37, sur les missions du délégué à la protection des données, que la répartition des responsabilités, la formation du personnel et les instructions adéquates en font partie. Il est également raisonnable d'escompter que le responsable du traitement doive au moins avoir une vue d'ensemble et un inventaire général des opérations de traitement dans ses responsabilités. Le CEPD recommande d'inclure ces éléments dans une disposition générale précédant les obligations spécifiques à l'article 22, paragraphe 2, et de développer davantage le concept du «contrôle de la gestion».

176. Afin de renforcer la responsabilité publique des responsables du traitement, le CEPD recommande également d'insérer un nouveau paragraphe à l'article 22 disposant que le responsable du traitement – volontairement ou en vertu d'une obligation légale – publie un rapport régulier de ses activités. Ce rapport doit également contenir des informations

sur les politiques et mesures visées à l'article 22, paragraphe 1, et la vérification de leur efficacité en vertu de l'article 22, paragraphe 3.

II.6.b. Protection des données dès la conception et des données par défaut (article 23)

177. Le CEPD se réjouit du fait que les principes de protection des données dès la conception et de protection des données par défaut aient été explicitement inclus dans la proposition de règlement.

178. Conformément au principe de «protection des données dès la conception», le responsable du traitement doit prendre en considération les exigences de protection des données dès le début, lors de la définition d'une opération de traitement. Le CEPD accueille favorablement le fait que le principe ait été davantage étayé à l'article 23, paragraphe 1. Plus particulièrement, le CEPD soutient l'introduction de références aux «techniques les plus récentes et aux coûts liés à leur mise en œuvre», d'une part, et aux «mesures et procédures techniques et organisationnelles appropriées», d'autre part.

179. L'article 23 ne traite pas de la façon dont un sous-traitant peut être lié par le principe de protection des données dès la conception. Toutefois, le CEPD distingue un lien entre cette disposition et l'article 26 qui traite du sous-traitant en général. Conformément à l'article 26, paragraphe 1, le responsable du traitement doit choisir un sous-traitant qui présente des garanties suffisantes de mise en œuvre des mesures et procédures techniques et organisationnelles appropriées, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement. Toutefois, le CEPD souhaiterait recommander que le législateur souligne également l'obligation du sous-traitant lui-même de tenir compte du principe de protection des données dès la conception lors du traitement des données à caractère personnel pour le compte du responsable du traitement. Cette obligation pourrait être ajoutée à la liste des spécifications contenues à l'article 26, paragraphe 2.

180. L'article 23, paragraphe 2, contient le principe de protection des données par défaut mais ne présente pas un contenu clair. La première phrase n'ajoute pas beaucoup aux principes généraux du traitement des données à l'article 5, et au principe de minimisation des données visé à l'article 5, point c), notamment, hormis la confirmation selon laquelle ces principes doivent également être intégrés dans la conception des systèmes pertinents.

181. Le principe de protection des données par défaut vise à protéger la personne concernée dans les situations où il pourrait y avoir un manque de compréhension ou de contrôle du traitement de leurs données, notamment dans un contexte technologique. L'idée qui sous-tend le principe est que les caractéristiques qui portent atteinte à la vie privée d'un certain produit ou service sont initialement limitées à ce qui est nécessaire pour sa simple utilisation. La personne concernée doit en principe avoir le choix d'autoriser une utilisation de ses données à caractère personnel de façon plus large. Le CEPD recommande d'inclure à l'article 23, paragraphe 2, une référence à cette position de la personne concernée et d'apporter la clarification nécessaire au considérant 61.

182. Les principes de protection des données dès la conception et par défaut ne s'adressent actuellement pas aux conseillers, développeurs et producteurs de matériels ou de logiciels. Toutefois, ils seront pertinents pour eux dès le début, étant donné que les responsables du traitement sont liés par eux et sont responsables de la conformité. En d'autres termes, les obligations pour les responsables du traitement (et pour les sous-

traitants, comme mentionné ci-dessus) sont susceptibles de créer certains incitants pour le marché des produits et services pertinents.

II.6.c. Responsables conjoints du traitement (article 24)

183. L'article 24 traite de la situation où un responsable du traitement définit, conjointement avec d'autres, un traitement des données à caractère personnel («responsables conjoints du traitement»). Le CEPD soutient l'idée de rendre obligatoire un accord entre eux. Toutefois, la responsabilité dans les situations où il n'y a pas de détermination des obligations respectives dans l'accord ou pas d'accord du tout doit être clarifiée. Une solution pourrait consister à rendre conjointement responsables les responsables du traitement et à prévoir que les personnes concernées pourront exercer leurs droits avec chacun d'eux.

II.6.d. Représentants des responsables du traitement qui ne sont pas établis dans l'Union (article 25)

184. Conformément à l'article 3, paragraphe 2, et à l'article 25, paragraphe 1, un responsable du traitement qui n'est pas établi dans l'Union et qui traite des données à caractère personnel de personnes concernées résidant dans l'Union doit désigner un représentant dans l'Union. Ce représentant a un rôle important à jouer en vertu du règlement, notamment en tant que point de contact pour les personnes concernées (article 14, paragraphe 1, point a)) ou pour l'autorité de contrôle (article 28, paragraphe 3, et article 29) ainsi qu'en cas de violation des dispositions du règlement (voir l'article 78).

185. L'article 25, paragraphe 2, prévoit des exceptions importantes à cette obligation, notamment pour les entreprises employant moins de 250 salariés, les autorités publiques et les responsables du traitement établis dans un pays tiers et dont il a été constaté qu'ils assuraient un niveau de protection adéquat ou dans le cas d'offres occasionnelles de biens ou de services.

186. Le CEPD ne comprend pas pourquoi il devrait y avoir une dérogation à l'obligation d'avoir un représentant pour les responsables du traitement situés dans des pays tiers assurant un niveau de protection des données adéquat. Le fait que le pays tiers assure un niveau de protection adéquat dans ce pays tiers n'a aucune incidence sur le fait que l'UE doive disposer d'un point de contact pour faire respecter la conformité aux règles relatives à la protection des données *sur le territoire de l'UE*. Dès lors, le CEPD recommande au législateur de supprimer l'article 25, paragraphe 2, point a).

II.6.e. Documentation (article 28)

187. L'article 28 de la proposition de règlement introduit l'obligation pour les responsables du traitement et les sous-traitants de tenir à jour la documentation des opérations de traitement dont ils sont responsables. Cette obligation remplace l'obligation générale de notifier les opérations de traitement individuelles à l'autorité de contrôle conformément aux articles 18, paragraphe 1, et 19 de la directive 95/46/CE. La documentation doit, sur requête, être mise à la disposition de l'autorité de contrôle. Cette modification a pour but de réduire la charge administrative qui pèse sur les responsables du traitement. L'article 28, paragraphe 4, prévoit une dérogation pour les personnes physiques sans intérêts commerciaux ou pour les entreprises ou organisations employant moins de 250 salariés lorsque les opérations de traitement ne se rapportent pas à ses activités principales.

188. Le CEPD accueille favorablement cette modification de l'approche, qui doit être perçue à la lumière du principe général de responsabilité, mais émet de sérieuses réserves quant à la façon dont elle a été mise en œuvre, qui suscite des doutes quant au fait qu'elle réduise effectivement la charge administrative générée par les règles de protection des données autant qu'escompté.

189. Il y a lieu de noter que la directive 95/46/CE prévoit actuellement des dérogations et des simplifications du devoir général de notification des opérations de traitement à l'autorité de contrôle, qui ont été largement utilisées dans plusieurs États membres. L'obligation de tenir à jour une documentation détaillée de toutes les opérations de traitement est dès lors susceptible de créer une charge considérable pour de nombreux responsables du traitement. La question se pose également de savoir si la tenue à jour d'une documentation détaillée de toutes les opérations de traitement est une «mesure appropriée et efficace» pour assurer et démontrer la conformité aux règles relatives à la protection des données dans un environnement de plus en plus dynamique, tant pour les petites et moyennes que pour les grandes organisations, et ce, encore plus dans un avenir prévisible.

190. Le CEPD préférerait dès lors une approche différente pour l'obligation de tenir à jour une documentation adéquate, de façon à la rendre appropriée, en principe, pour tous les responsables du traitement. Cela pourrait être réalisé en combinant les éléments les plus généraux du texte actuel de l'article 28, paragraphe 2, points a), b) et h), avec un devoir de maintenir un inventaire[44] de toutes les opérations de traitement dont est responsable le responsable du traitement, ainsi qu'une description de la façon dont le responsable du traitement a veillé à ce que ces opérations de traitement satisfassent aux règles relatives à la protection des données. Cela soutiendrait également l'obligation générale de responsabilité et se concentrerait davantage sur les résultats souhaités. L'actuelle obligation à l'article 28, paragraphe 3, de mettre la documentation à la disposition de l'autorité de contrôle pourrait alors être complétée par une obligation supplémentaire d'informer l'autorité de contrôle, sur demande, quant aux sujets actuellement mentionnés à l'article 28, paragraphe 2, points c) à g).

191. À la lumière des éléments qui précèdent, le CEPD recommande que les dérogations actuelles prévues à l'article 28, paragraphe 4, soient reconsidérées. Il se pourrait bien qu'elles puissent être complètement supprimées.

II.6.f. Sécurité des traitements (article 30)

192. À l'article 30, sur la sécurité des traitements, il est fait référence au responsable du traitement et au sous-traitant. Le CEPD accueille favorablement le fait que les deux acteurs soient mentionnés, mais recommande au législateur de clarifier la disposition de telle façon qu'il n'y ait pas de doute quant à la responsabilité générale du responsable du traitement. Il ressort du texte, tel qu'il se présente actuellement, que le sous-traitant et le responsable du traitement semblent responsables de manière égale. Cela ne va pas dans le sens des dispositions précédentes, notamment les articles 22 et 26 de la proposition de règlement.

[44] Un outil de gestion pour assurer une vue d'ensemble et soutenir la mise en œuvre des exigences en matière de protection des données, qui est beaucoup moins détaillé qu'un registre de notifications, tel qu'exigé actuellement en vertu de la directive 95/46/CE.

193. L'article 30 est assez général en ce qui concerne les exigences de fond. Le CEPD accueille favorablement le fait que les risques représentés par le traitement et la nature des données à caractère personnel devant être protégées soient mentionnés en tant qu'éléments servant à déterminer le niveau de sécurité approprié. Toutefois, pour que la disposition soit efficace, des règles plus détaillées sont nécessaires. Une plus ample description dans un considérant pourrait se fonder sur les trois principes de sécurité, à savoir la confidentialité, l'intégrité et la disponibilité. Selon le CEPD, le règlement devrait obliger le responsable du traitement à adopter une approche de gestion de la sécurité des informations au sein de l'organisation, incluant le cas échéant la mise en œuvre d'une politique de sécurité des informations spécifique au traitement des données réalisé, lorsqu'il y a lieu.

194. Comme déjà évoqué dans la partie II.2.b, les sanctions administratives prévues pour la non-conformité aux mesures appropriées relatives à la sécurité (voir l'article 79, paragraphe 6, point e)) ne peuvent être imposées tant que de plus amples spécifications ne sont pas données dans les actes délégués et d'exécution annoncés à l'article 30, paragraphes 3 et 4. Ces actes devraient dès lors être adoptés au moment de l'application du règlement.

195. Le CEPD note un lien entre l'article 30, paragraphe 2, et l'analyse d'impact relative à la protection des données, telle qu'exposée à l'article 33, et suggère de préciser ce lien, en incluant une référence spécifique à cette analyse à l'article 30. Il convient de noter cependant que l'évaluation des risques, dans le dernier cas, est un concept plus large que l'analyse visée à l'article 33.

II.6.g. Violation de données à caractère personnel (articles 31 et 32)

196. Sur la base de la communication de la violation des données à caractère personnel visée à l'article 4, paragraphe 3, de la directive 2002/58/CE, sur la protection de la vie privée dans le secteur des communications électroniques, la Commission propose d'introduire, à l'article 31, l'obligation générale pour le responsable du traitement de notifier à l'autorité de contrôle les violations de données à caractère personnel. En outre, aux termes de l'article 32, le responsable du traitement est obligé de communiquer à la personne concernée une violation de données à caractère personnel qui est susceptible d'affecter sa protection, sauf lorsque le responsable du traitement a démontré à l'autorité de contrôle qu'il a mis en œuvre les mesures de protection technologiques appropriées et les a appliquées aux données concernées.

197. Le CEPD est heureux de constater l'introduction de ces dispositions qui peuvent contribuer à renforcer à la fois la sécurité du traitement et la responsabilité du responsable du traitement.

198. Toutefois, ainsi qu'il a déjà été mentionné dans la partie II.2.b, la proposition de règlement ne spécifie pas les critères et les exigences pour établir une violation des données ainsi que les circonstances dans lesquelles elle doit être notifiée. Les deux dispositions habilitent la Commission à adopter des actes délégués à cette fin. Comme mentionné, le CEPD estime qu'en l'absence de ces actes délégués, les nouvelles obligations ne peuvent être mises en œuvre efficacement. Ces actes devraient dès lors être adoptés au moment de l'application du règlement.

199. En outre, le CEPD recommande que le règlement prévoie, à l'article 31, un délai plus réaliste que 24 heures après en avoir pris connaissance pour notifier la violation des données à l'autorité de contrôle (par exemple, 72 heures au plus tard). Le fait de fixer un délai trop strict pourrait saper l'efficacité des deux dispositions.

II.6.h. Analyse d'impact relative à la protection des données (article 33)

200. L'article 33, paragraphe 1, de la proposition oblige le responsable du traitement ou le sous-traitant à effectuer une analyse de l'impact sur la protection des données à caractère personnel des opérations de traitement envisagées chaque fois qu'elles présentent des risques spécifiques. L'article 33, paragraphe 2, prévoit une liste non exhaustive de ces opérations de traitement. Certaines de ces opérations doivent ou pourraient requérir une consultation préalable de l'autorité de contrôle (voir l'article 34, paragraphes 2 et 4, et la partie II.6.i ci-dessous). L'article 33, paragraphe 3, expose de façon très détaillée ce qu'une analyse de l'impact devrait impliquer.

201. Le CEPD accueille favorablement l'insertion de cette nouvelle disposition étant donné qu'elle constitue un mécanisme important pour assurer la responsabilité du responsable du traitement. En outre, elle contribue à la mise en œuvre des principes de «protection des données dès la conception» ainsi que «protection des données par défaut». Toutefois, le CEPD n'est pas complètement satisfait de la liste des opérations de traitement contenue à l'article 33, paragraphe 2. Plus particulièrement, la limitation des opérations de traitement aux points b), c) et d) aux traitements à grande échelle ne se justifie pas. Le CEPD estime que même à petite échelle, les opérations indiquées dans ces trois points nécessiteraient une analyse de l'impact de la protection des données. En outre, ce qui pourrait être qualifié de «à grande échelle» n'est pas du tout clair.

202. L'article 33, paragraphe 5, prévoit des dérogations à cette obligation pour les autorités ou les organismes publics lorsque le traitement est effectué en exécution d'une obligation légale conforme à l'article 6, paragraphe 1, point c), sauf si les États membres en décident autrement. Au considérant 73, il est mentionné qu'une autorité ou un organisme public ne devrait réaliser une analyse d'impact relative à la protection des données que 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 public concerné ainsi que l'opération de traitement spécifique en question. Ce considérant semble également faire référence au traitement fondé sur l'article 6, paragraphe 1, point e), de la proposition de règlement.

203. L'article 33, paragraphe 5, devrait être mis en équation avec le considérant 73 afin d'éviter tout malentendu. Il devrait être précisé que, pour les deux motifs, l'exception pour la réalisation d'une analyse d'impact relative à la protection des données ne s'applique que si une évaluation spécifique, égale à une analyse de l'impact de la protection des données, a déjà été effectuée dans le contexte législatif.

204. L'article 33, paragraphe 6, habilite la Commission à adopter des actes délégués aux fins de préciser davantage les critères et conditions applicables aux traitements susceptibles de présenter les risques particuliers visés aux paragraphes 1 et 2 de l'article 33. De même, les exigences pour l'analyse au paragraphe 3 peuvent être davantage précisées dans un acte délégué. En agissant de la sorte, la Commission doit prendre en considération des mesures spécifiques pour les MPME.

205. Le CEPD appelle le législateur à réexaminer cette disposition (voir également la partie II.2.b et c). En l'état actuel, elle est trop vague en ce qui concerne exactement ce qui peut être spécifié dans l'acte délégué par la Commission. Il convient de s'assurer que les éléments essentiels sont suffisamment définis dans l'acte législatif. Il doit également être clair que la taille d'une entreprise ne devrait jamais supprimer l'obligation d'effectuer une analyse d'impact relative à la protection des données en ce qui concerne les opérations de traitement qui présentent des risques spécifiques.

II.6.i. Autorisation et consultation préalables (article 34)

206. L'article 34 traite tant de l'autorisation préalable que de la consultation préalable. Toutefois, seul le premier paragraphe traite de l'autorisation préalable qui ne s'applique qu'à une question spécifique, à savoir le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale. Le CEPD recommande de déplacer le premier paragraphe vers le chapitre V, sur le transfert de données vers des pays tiers, et de limiter l'article 34 à la seule consultation préalable[45]. Cela tiendrait davantage compte du fait que les cas pour une autorisation préalable ont été limités dans la proposition de règlement et du fait que l'analyse de l'impact de la protection des données est liée à la consultation préalable et non à l'autorisation préalable.

207. De façon générale, le CEPD accueille favorablement l'article 34 qui se fonde sur la procédure de contrôle préalable exposée à l'article 20 de la directive 95/46/CE et qui prévoit une implication appropriée de l'autorité de contrôle avant les opérations de traitement susceptibles de présenter des risques spécifiques, avec la possibilité d'une nouvelle intervention si elle est justifiée.

II.6.j. Délégué à la protection des données (article 35)

208. La proposition de règlement introduit à l'article 35 une obligation pour le responsable du traitement ou le sous-traitant de désigner un délégué à la protection des données afin de contrôler au niveau interne la conformité à la proposition de règlement lorsque le traitement est effectué dans le secteur public ou dans le secteur privé par une grande entreprise ou lorsque les activités principales du responsable du traitement requièrent un contrôle régulier et systématiques des personnes concernées.

209. Le CEPD note que la fonction d'un délégué à la protection des données n'est pas vraiment une nouveauté étant donné qu'il s'agit d'une option ouverte aux États membres en vertu de la directive 95/46/CE et une obligation des institutions et organismes de l'Union en vertu du règlement (CE) n° 45/2001. Le CEPD accueille favorablement le fait qu'en se fondant sur l'expérience positive acquise, la proposition de règlement consacre une section complète (section 4 du chapitre 4) au délégué à la protection des données et généralise sa désignation obligatoire[46]. En effet, le CEPD considère que le délégué à la protection des données, exécutant ses devoirs et ses missions indépendamment, constitue un élément clé du nouveau cadre juridique proposé étant donné que non seulement il devrait informer et conseiller le responsable du

[45] Cela impliquerait également une modification du titre de la section 3 du chapitre IV du règlement, qui est actuellement quelque peu trompeur.

[46] Voir également le document de référence du CEPD du 28 novembre 2005 sur le rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n° 45/2001, disponible à l'adresse http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_délégué à la protection des données_paper_FR.pdf.

traitement ou le sous-traitant de leurs obligations, mais il devrait également contrôler au niveau interne l'application du règlement et, enfin, agir en tant que point de contact de l'autorité de contrôle.

210. Il convient de souligner, cependant, que le délégué à la protection des données ne doit pas être perçu comme la *seule* personne impliquée dans le fait de veiller à la conformité aux exigences en matière de protection des données. S'il s'agit de la principale responsabilité du responsable du traitement et du personnel participant aux opérations de traitement pertinentes pour assurer la conformité, le délégué à la protection des données joue un rôle spécial en conseillant le responsable du traitement et en contrôlant la mise en œuvre et l'application des politiques ainsi que des mesures appropriées adoptées par le responsable du traitement. Cela explique également la raison pour laquelle le délégué à la protection des données doit effectuer ses devoirs et mission indépendamment et ne recevoir aucune instruction en ce qui concerne l'exercice de sa fonction, comme explicitement mentionné à l'article 36, paragraphe 2.

211. Étant donné, notamment, que selon l'article 35, paragraphe 2, et l'article 35, paragraphe 3, un groupe d'entreprises ou plusieurs entités publiques peuvent désigner un délégué unique à la protection des données, le CEPD recommande que le règlement fixe un seuil inférieur à 250 salariés pour exiger la désignation d'un délégué à la protection des données dans une entreprise. Bien que cette recommandation puisse ne pas aller dans le sens de la définition des (M)PME, il n'existe pas de raison convaincante d'abaisser le seuil dans le domaine spécifique de la protection des données. En outre, la proposition de règlement devrait préciser davantage le champ d'application de l'article 35, paragraphe 1, point c), qui prévoit la désignation obligatoire d'un délégué à la protection des données lorsque les activités principales du responsable du traitement consistent en des traitements qui exigent un suivi régulier et systématique des personnes concernées.

212. Conformément à l'article 36, paragraphe 1, le délégué à la protection des données doit être impliqué, par le responsable du traitement, dans toutes les questions concernant la protection de données à caractère personnel, et comme mentionné, selon l'article 36, paragraphe 2, le responsable du traitement doit veiller à ce que le délégué à la protection des données puisse agir de manière indépendante. Afin de renforcer davantage ces dispositions, le CEPD recommande que le règlement offre des garanties supplémentaires, notamment:
    - des conditions plus strictes pour le renvoi du délégué à la protection des données, par exemple en établissant à l'article 35, paragraphe 7, une obligation pour le responsable du traitement d'informer l'autorité de contrôle;
    - une spécification de l'obligation pour le responsable du traitement ou pour le sous-traitant, exposée à l'article 36, paragraphe 1, en disposant que le délégué à la protection des données doit avoir accès, notamment, à toutes les informations pertinentes pour les politiques relatives à la protection des données, la documentation, les violations des données à caractère personnel, les analyses d'impact ainsi que tous les contacts pertinents avec l'autorité de contrôle;
    - le fait de donner accès, à tout moment, au délégué à la protection des données, aux données et aux locaux tel que nécessaire pour l'exécution de ses devoirs, comme indiqué au point 4 de l'annexe au règlement (CE) n° 45/2001.

213. En outre, en se basant sur l'expérience acquise au sein des institutions et organismes de l'UE, le CEPD estime que le délégué à la protection des données a un rôle important à jouer en fournissant des informations sur, et en sensibilisant à la protection des données

au sein de l'organisation qui l'a désigné. Dès lors, le CEPD recommande que l'article 37, paragraphe 1, point a), soit développé dans cette mesure.

II.7. Transfert vers des pays tiers (chapitre V)

214. Les dispositions sur les transferts vers des pays tiers ont été considérablement développées et précisées. L'interdiction actuelle de tous transferts vers des pays qui ne sont pas jugés adéquats est remplacée par un principe général à l'article 40 selon lequel des transferts ne peuvent avoir lieu que si les conditions pour les transferts exposées dans la proposition de règlement sont remplies. La proposition précise que les règles sur les transferts s'appliquent non seulement aux responsables du traitement mais aussi aux sous-traitants ainsi qu'aux destinataires supplémentaires dans le cas de transferts ultérieurs.

215. La proposition maintient le pouvoir de la Commission d'adopter des décisions reconnaissant le caractère adéquat ou inadéquat d'un pays tiers, impliquant également à présent des organisations internationales. Elle introduit de nouveaux critères pour l'analyse qui ne tiennent plus compte des modalités spécifiques du traitement entourant une opération de transfert de données ou un ensemble d'opérations de transfert des données. À la place, l'article 41, paragraphe 2, se concentre plus clairement sur la primauté du droit et l'existence de mécanismes de recours efficaces et d'une autorité de contrôle indépendante dans le pays tiers en question, bien qu'un certain rôle pour une autoréglementation reste une option.

216. La proposition de règlement introduit une certaine flexibilité en exposant de nouveaux mécanismes qui pourraient être utilisés pour assurer des garanties adéquates pour les transferts de données vers des pays tiers qui ne bénéficient pas d'une décision relative au caractère adéquat (telles qu'un mécanisme détaillé pour le recours à des règles d'entreprise contraignantes et les conditions pour l'utilisation de divers types de clauses contractuelles). Le CEPD accueille favorablement ces mécanismes qui sont déjà en usage dans la pratique et qui bénéficieront assurément d'une base juridique claire dans le règlement.

II.7.a. Applicabilité de la proposition de règlement aux accords internationaux existants

217. Le considérant 79 prévoit que le règlement ne remet pas en cause les accords internationaux conclus entre l'Union et les pays tiers en vue de réglementer le transfert des données à caractère personnel. Le CEPD recommande que la non-applicabilité du règlement aux accords internationaux soit limitée dans le temps afin de s'appliquer uniquement aux accords internationaux déjà existants. En outre, une clause transitoire devrait être insérée dans la proposition, prévoyant l'examen de ces accords internationaux dans un délai fixé afin de les mettre en équation avec le règlement (par exemple, comme prévu au considérant 72 de la proposition de directive). Cette clause devrait être incluse dans les dispositions de fond de la proposition et contenir un délai qui n'excède pas deux ans après l'entrée en vigueur du règlement.

II.7.b. Transferts vers des pays tiers qui ont été déclarés inadéquats (article 41)

218. Il n'apparaît pas clairement si les transferts vers les pays tiers pour lesquels la Commission a adopté une décision de caractère non adéquat seraient totalement interdits ou resteraient possibles sous certaines conditions. Cette incertitude découle d'une contradiction entre le texte du considérant 82, qui est totalement opposé à un transfert

dans de tels cas, et l'article 41, paragraphe 6, qui déclare que cette interdiction est «sans préjudice des articles 42 à 44».

219. L'article 42 prévoit que des transferts moyennant des garanties appropriées peuvent être effectués «lorsque la Commission n'a *pas adopté de décision* en vertu de l'article 41» (mise en italique ajouté). Cela impliquerait que des transferts moyennant des garanties appropriées ne seraient plus une option lorsque la Commission a adopté une décision de caractère non adéquat. Ce résultat serait injustifié étant donné qu'une telle décision confirmerait uniquement la nécessité de garanties appropriées dans certains cas spécifiques et assurément en cas de transferts de données répétés ou systématiques, comme c'est actuellement d'application en vertu de la directive 95/46/CE.

220. Le CEPD recommande dès lors que l'article 42 (et le considérant 82) soient modifiés pour préciser qu'en cas de décision de caractère inadéquat, les transferts vers ce pays ne seraient permis que sous réserve de garanties appropriées ou en vertu des dérogations exposées à l'article 44[47].

II.7.c. Transferts moyennant des garanties appropriées (article 42)

221. L'article 42, paragraphe 1, expose le principe selon lequel des transferts vers un pays tiers, en l'absence de toute décision[48] de la Commission quant au niveau du caractère adéquat de ce pays, ne peuvent avoir lieu que si le responsable du traitement ou le sous-traitant a offert des garanties appropriées «dans un instrument juridiquement contraignant». Toutefois, l'article 42, paragraphe 8, autorise de tels transferts, même si les garanties ne sont pas offertes dans instrument juridiquement contraignant, à condition qu'une autorisation préalable ait été obtenue de l'autorité de contrôle. En pareils cas, des garanties appropriées peuvent consister en «d'autres mesures adaptées et proportionnées qui se justifient au regard des circonstances» qui entourent un transfert (selon le considérant 83), telles que des «dispositions à insérer dans un régime administratif constituant le fondement du transfert» (conformément à l'article 42, paragraphe 5).

222. De l'avis du CEPD, la possibilité de recourir à des instruments qui ne soient pas juridiquement contraignants pour offrir des garanties appropriées doit être clairement justifiée et limitée uniquement aux cas où la nécessité de se fier à ce type de mesure non contraignante a été démontrée. En principe, notamment en ce qui concerne les responsables du traitement et les sous-traitants du secteur privé, le CEPD ne voit aucune raison pour laquelle il devrait y avoir une dérogation à l'obligation d'avoir des garanties clairement définies dans un instrument juridiquement contraignant. L'article 42 devrait être modifié en conséquence.

223. La nécessité d'avoir recours à des garanties non légalement contraignantes dans le secteur public doit être analysée avec soin, au vu de la finalité du traitement et de la nature des données. Si un tel recours se justifie clairement, l'article 42 devrait spécifier les conditions pour le recours à cette possibilité.

[47] Conformément aux observations formulées dans la partie II.7.d, les transferts entre autorités publiques pourraient être autorisés s'il existe un accord international juridiquement contraignant, autorisant le transfert dans des conditions spécifiques garantissant une protection adéquate.
[48] Voir également les observations, dans la partie II.7.b, sur la signification de ces termes.

II.7.d. Dérogations (article 44)

224. Il doit être précisé à l'article 44 que le recours à *toute* dérogation en tant que justification pour un transfert doit être interprété de façon restrictive et ne s'appliquer qu'aux transferts ne pouvant être qualifiés de fréquents, massifs ou structurels. Ce raisonnement est conforme à l'interprétation donnée par le groupe de travail «Article 29» à l'actuel article 26, paragraphe 1, de la directive 95/46 sur les dérogations[49]. Il existe un risque que la protection accordée aux personnes en vertu du règlement ne soit significativement affaiblie si tout ensemble de transferts, y compris ceux qui sont répétés ou massifs, pouvaient toujours être justifiés par l'une des dérogations et dès lors échapper à l'exigence de conclure des garanties appropriées. L'article 44, paragraphe 1, point h), proposé est insuffisant pour éviter ce risque.

225. La dérogation à l'article 44, paragraphe 1, point d), dans les cas où un transfert est nécessaire pour des «motifs importants d'intérêt général», lu conjointement avec le considérant 87, est trop large et permettrait des transferts de données lorsqu'ils sont «nécessaires» pour un large éventail de motifs importants d'intérêt général, tels que la sécurité sociale, les administrations fiscales ou douanières ainsi que pour la prévention, la détection et les poursuites en matière pénale, sans aucune garantie spécifique en matière de protection des données.

226. Le large caractère des motifs d'intérêt général qui peuvent être utilisés conformément à cette disposition ainsi que dans d'autres parties de la proposition a été critiqué précédemment (voir la partie II.2.d). Si elles ne sont pas soigneusement rédigées, ces dispositions pourraient permettre de nombreux transferts entre les autorités publiques et/ou entités privées et les autorités répressives sans aucune autre garantie. Ce serait contraire à l'esprit du règlement et au respect du droit fondamental des personnes à la protection des données.

227. Il ne suffit pas que l'article 41, paragraphe 8, exige que l'intérêt général soit reconnu dans le droit de l'Union ou le droit national pour légitimer tous les transferts en vertu de ce motif juridique. Il doit être vérifié avec soin, au cas par cas, si la dérogation pour un motif important d'intérêt général serait applicable à un transfert particulier. Le CEPD souligne que si des transferts sont répétés, massifs ou structurels, ils ne doivent avoir lieu que sur la base d'un accord international qui prévoit des garanties appropriées. Le CEPD recommande dès lors que l'article 44 (et le considérant 87) soit modifié afin de préciser que la possibilité de transférer des données en vertu d'un tel motif ne devrait concerner que les transferts occasionnels et être fondés sur une analyse soigneuse de toutes les circonstances du transfert, au cas par cas.

228. La référence aux «garanties appropriées», à l'article 44, paragraphe 1, point h), et à l'article 44, paragraphe 3, doit être précisée ou de préférence remplacée par une notion différente, étant donné qu'en principe, les garanties appropriées pour les transferts sont celles énumérées à l'article 42, et éventuellement plus amplement détaillées dans des actes délégués conformément à l'article 44, paragraphe 7. Les dérogations s'appliquent précisément lorsqu'il n'y a pas de garanties conformément à l'article 42.

[49] Voir le document de travail du groupe de travail «Article 29» du 26 novembre 2005 sur une interprétation commune de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (WP114).

II.7.e. Divulgations aux pays tiers en vertu des lois, des règlements et d'autres instruments législatifs (considérant 90)

229. Le CEPD recommande que les principes articulés au considérant 90 soient exposés dans une disposition de fond dans le règlement. Cette disposition devrait préciser les conditions sous lesquelles de telles demandes pourraient être satisfaites.

230. Le considérant 90 implique que les conditions pour ces transferts seraient satisfaites «lorsque la divulgation est nécessaire pour un motif important d'intérêt général reconnu par le droit de l'Union ou par le droit d'un État membre auquel le responsable des données est soumis». Toutefois, ainsi qu'il est mentionné dans la section II.5.f ci-dessus, le fait qu'un droit de l'UE ou national reconnaisse un motif important d'intérêt général ne constitue pas, en soi, une justification pour un transfert vers un pays tiers.

231. En outre, des garanties appropriées devraient être en place en pareils cas, impliquant des garanties judiciaires ainsi que des garanties relatives à la protection des données (y compris l'existence d'accords de coopération internationaux ou bilatéraux sur des questions spécifiques). Il conviendrait en outre d'analyser de quelle façon les autorités de contrôle pourraient intervenir en pareils cas, que ce soit en rendant un avis ou une autorisation sur le transfert.

232. L'article 44, paragraphe 7, lu conjointement avec le considérant 90, prévoit que la Commission spécifiera plus amplement, dans un acte délégué, les conditions sous lesquelles un motif important d'intérêt général existe. Toutefois, le CEPD considère que les motifs spécifiques d'intérêt général ne doivent pas être abandonnés aux actes délégués mais doivent être mentionnés explicitement dans le texte de la proposition lui-même, étant donné qu'ils constituent un élément essentiel de la proposition.

II.7.f. L'utilisation de la procédure d'examen dans le contexte des transferts vers les pays tiers (article 41, paragraphe 3)

233. La procédure pour l'adoption d'actes d'exécution afin d'analyser le caractère adéquat est exposée à l'article 41, paragraphe 3, qui fait référence à la procédure d'examen. Le CEPD considère que ces décisions ne doivent pas être prises uniquement dans le cadre de la procédure d'examen, mais traitées par le biais d'un mécanisme d'analyse approfondie, avec la totale implication des autorités de contrôle, comme c'est actuellement le cas en ce qui concerne l'analyse du caractère adéquat en vertu de l'article 30, paragraphe 1, point b) de la directive 95/46/CE. Le CEPD suggère d'ajouter explicitement à l'article 66 que le comité européen de la protection des données («le comité») doit être consulté dans ce contexte.

II.8. Compétences et pouvoirs des autorités de contrôle (chapitre VI)

234. Le CEPD accueille favorablement les dispositions du chapitre VI de la proposition de règlement qui renforcent l'indépendance des autorités de contrôle. Ces dispositions reconnaissent que le contrôle par une autorité indépendante constitue un élément essentiel des règles de l'UE relatives à la protection des données. Cela résulte de l'article 16 TFUE et de l'article 8 de la charte et a été souligné par la Cour de justice dans l'arrêt *Commission/Allemagne* de mars 2010[50].

[50] Voir l'arrêt de la CJUE du 9 mars 2010, *Commission/Allemagne*, C-518/07, Recueil 2010, p. I-1885, points 23 et 50.

235. Il est essentiel que cette indépendance soit assurée d'un point de vue tant fonctionnel qu'institutionnel. À cet égard, le CEPD considère que les dispositions qui précisent les pouvoirs des autorités et la nécessité de ressources et d'infrastructures adéquates ont une importance cruciale[51]. Les dispositions de la proposition développées à l'article 48, paragraphe 1, concernant les membres de l'autorité revêtent également une importance particulière.

236. En ce qui concerne les conditions de nomination des membres (article 48), le CEPD considère qu'une analyse plus approfondie est nécessaire au niveau du libellé actuel de la proposition. La disposition autorise des nominations soit par le parlement, soit par le gouvernement, ce qui signifie qu'elles peuvent être décidées par le gouvernement sans implication substantielle du parlement. Le CEPD suggère le renforcement des garanties démocratiques des nominations en exigeant un rôle plus systématique pour les parlements nationaux dans la procédure de nomination des membres des autorités de contrôle[52].

237. L'article 51, paragraphe 2, prévoit une «autorité chef de file» déterminée par le principal établissement du responsable du traitement ou du sous-traitant. Le CEPD souhaiterait d'abord renvoyer aux observations formulées dans la partie II.3.c sur l'actuelle définition du principal établissement. Toutefois, indépendamment du résultat de cette analyse, il estime que le rôle d'une autorité chef de file ne doit pas être perçu comme une compétence exclusive, mais plutôt comme un mode structuré de coopération avec d'autres autorités de contrôle compétentes, étant donné que l'«autorité chef de file» dépendra fortement de la contribution et du soutien des autres autorités de contrôle à différents points dans le processus.

238. Le CEPD accueille favorablement la liste explicite des pouvoirs pour les autorités de contrôle exposée à l'article 53. Cette liste contient plusieurs exemples de pouvoirs de l'autorité de contrôle, y compris la possibilité d'imposer une interdiction temporaire ou définitive sur le traitement ou la suspension des flux de données. Une absence de conformité à une telle décision fera l'objet de la catégorie la plus élevée des sanctions administratives en vertu de l'article 79, paragraphe 6, point m).

239. Un des pouvoirs mentionnés est le pouvoir «le cas échéant, d'ordonner au responsable du traitement ou au sous-traitant de remédier à cette violation par des mesures déterminées, afin d'améliorer la protection de la personne concernée» (article 53, paragraphe 1, point a)). Ce pouvoir permet à l'autorité de contrôle d'imposer une conduite spécifique lorsqu'un responsable du traitement ou un sous-traitant n'a pas agi en conformité avec une obligation, et pourrait être utilisé dans des situations très diverses. Cela souligne le besoin de flexibilité et d'une large marge de manœuvre pour les autorités de contrôle, comme l'exprime également le terme «le cas échéant».

240. Le CEPD souligne que ce pouvoir *réparateur* pourrait bien être exercé conjointement avec et en sus du pouvoir *punitif* d'imposer une sanction administrative comme prévu à l'article 79. Toutefois il requiert un pouvoir d'appréciation plus large que celui actuellement exprimé dans cette disposition. La non-conformité à un ordre spécifique devrait en tout état de cause mériter une sanction administrative plus lourde qu'une seule violation de la même disposition générale (voir également les observations dans la

[51] Voir l'article 47, paragraphe 5, de la proposition de règlement.
[52] Voir de façon plus générale, concernant l'implication des parlements dans le fonctionnement des autorités de contrôle, l'arrêt *Commission/Allemagne* de la CJUE, à la note de bas de page 50.

partie II.10.c). Il en va aussi, généralement, de l'intérêt des personnes concernées. Le CEPD recommande de modifier la proposition de règlement en conséquence.

II.9. Coopération et cohérence (chapitre VII)

241. Le CEPD exprime un fort soutien aux mécanismes de coopération et cohérence développés au chapitre VII de la proposition de règlement, sous réserve des observations ci-dessous sur certains détails. Il considère que ces mécanismes apporteront une simplification au profit des personnes concernées ainsi que des responsables du traitement des données. Ils assureront également une mise en application plus forte de manière cohérente dans l'UE, ce qui est également important dans les cas où les responsables du traitement des données opèrent de l'extérieur de l'UE.

242. Le rôle renforcé du comité européen de protection des données, en tant que successeur du groupe de travail «article 29», est un aspect essentiel du nouveau cadre harmonisé. Le CEPD soutient ce rôle renforcé mais demande en même temps un meilleur équilibre entre, d'une part, le rôle du comité et des autorités de contrôle représentées au sein du comité, et, d'autre part, les larges pouvoirs accordés à la Commission. Les pouvoirs de la Commission dans le contexte du mécanisme de cohérence sont actuellement excessivement importants.

II.9.a. Coopération (chapitre VII, section 1)

243. Le CEPD accueille favorablement l'intention d'organiser la coopération de manière plus structurée et soutient les obligations d'échanger les informations ou d'organiser des enquêtes conjointes. Il croit comprendre que ces dispositions se rapportent aux procédures et ne doivent pas entraver la souveraineté nationale (voir également la partie II.8).

244. Le CEPD n'a pas d'autres observations spécifiques en ce qui concerne la procédure de coopération telle qu'élaborée aux articles 55 et 56.

II.9.b. Cohérence (chapitre VII, section 2)

i) Nouvelle amélioration du mécanisme de cohérence

245. En ce qui concerne les circonstances susceptibles d'actionner le mécanisme de contrôle de la cohérence, le CEPD note que, bien que l'article 58, paragraphe 2, définisse de manière exhaustive les mesures à communiquer au comité européen de protection des données, le champ d'application du mécanisme est considérablement élargi au paragraphe 3: toute autorité peut demander que toute question soit traitée par le comité. Cela signifie qu'un nombre beaucoup plus élevé de cas peuvent actionner la première phase du mécanisme de contrôle de la cohérence, par rapport à ce qui est prévu par la Commission dans la fiche financière législative jointe à la proposition de règlement. Conjointement avec la nécessité de traductions dans tous les cas pertinents, ce mécanisme doit forcément entraîner des conséquences importantes en termes de soutien administratif de la part du secrétariat du comité. Voir, pour des observations plus détaillées et des recommandations sur la répartition du budget relatif au secrétariat du comité, l'annexe au présent avis.

246. Dans la deuxième phase, discutée plus amplement à l'article 58, paragraphe 7, le comité décidera s'il émettra un avis à la majorité simple *ou* à la demande de toute autorité de

contrôle ou de la Commission. Le CEPD s'interroge sur le sens d'un vote si toute autorité peut toujours demander qu'un avis soit adopté. Il recommande d'affiner le champ d'application de l'article 58, paragraphe 7, et d'accorder plus de poids à la règle de la majorité, afin d'éviter que le comité ne soit tenu d'émettre un avis à tout moment où une demande est formulée par une seule autorité. Il suggère qu'une demande de la part d'une autorité pourrait être soumise au vote dans le cas où la question en jeu ne se rapporte pas à l'une des principales mesures décrites à l'article 58, paragraphe 2.

247. Le CEPD demande également des délais plus souples en ce qui concerne le rôle du comité lorsqu'il est saisi dans le contexte du mécanisme de contrôle de la cohérence. Il renvoie notamment aux délais visés à l'article 58, paragraphes 6 et 7, exigeant la transmission «sans délai» des informations aux membres du comité, en relation également avec la fourniture des traductions des documents, et au délai d'un mois pour l'adoption de l'avis du comité. Le CEPD suggère de remplacer le terme anglais «immediately» *[immédiatement]* à l'article 58, paragraphe 6, par «without delay» *[sans délai]* et d'étendre le délai d'un mois visé à l'article 58, paragraphe 7, à deux mois/huit semaines au moins.

(ii) Le rôle de la Commission dans le mécanisme de contrôle de la cohérence (articles 59 et 60)

248. La Commission peut intervenir en différentes occasions dans le contexte du mécanisme de contrôle de la cohérence. Outre le fait d'actionner le mécanisme de contrôle de la cohérence en saisissant le comité, la Commission peut adopter un avis et une décision de suspension conformément aux conditions visées aux articles 58 et 59. En outre, la Commission peut annuler la décision d'une autorité de contrôle nationale *sur une question spécifique* en adoptant un acte d'exécution (voir l'article 60, paragraphe 1, et 62, paragraphe 1, point a)). Le CEPD est fondamentalement en désaccord avec cette approche dans la mesure où elle se rapporte à des projets de mesures d'une autorité de contrôle sur des questions spécifiques.

249. En ce qui concerne la possibilité d'émettre un avis, le CEPD note que la Commission peut adopter un avis indépendamment 1) de l'évolution de la procédure devant le comité, 2) du contenu de l'avis du comité et 3) de la réaction de l'autorité de contrôle à l'avis du comité. Le CEPD déplore que tout avis de la Commission ne soit pas lié plus étroitement à la procédure devant le comité et à l'issue de cette procédure. Selon lui, la Commission devrait uniquement intervenir au moyen d'un avis si la procédure n'a pas permis de concilier la position de l'autorité avec l'avis du comité, ou si l'issue de la procédure pourrait éventuellement violer le droit de l'UE. Le CEPD recommande de compléter l'article 59 en ce sens.

250. En ce qui concerne les mesures de suspension prévues à l'article 60, le CEPD considère que des «doutes sérieux» quant à la bonne application de la proposition de règlement ne justifient pas une décision de suspension d'une mesure prise par une autorité de contrôle nationale. Il conseille de limiter toute suspension à une violation manifeste du droit de l'UE avec des risques d'effets irrémédiables, soumise à la vérification de la Cour de justice.

251. La possibilité pour la Commission d'annuler une décision d'une autorité de contrôle nationale *sur une question spécifique* par l'adoption d'un acte d'exécution[53] suscite les

[53] Voir l'article 60, paragraphe 1, et l'article 62, paragraphe 1, point a), de la proposition de règlement.

mêmes préoccupations. Le pouvoir de la Commission s'étend au point d'autoriser l'adoption d'actes d'exécution avec effet immédiat (et donc, sans aucun avis préalable ou décision motivée) aux motifs de l'urgence concernant les intérêts des personnes concernées[54].

252. Le CEPD est fermement opposé à ce pouvoir de la Commission. Il porte préjudice à l'indépendance des autorités de contrôle nationales, garantie au chapitre VI, et ne peut être considéré comme nécessaire pour l'exécution par la Commission de ses tâches en tant que gardienne des traités.

253. La Cour de justice a clairement déclaré que les autorités de contrôle devaient être libres de «toute influence externe»[55]. Selon le CEPD, les autorités de contrôle ne sont pas libres de toute influence si la Commission a le pouvoir d'intervenir dans des cas individuels. Le fait que la Commission ait elle-même un statut indépendant ne signifie pas qu'elle soit, dans tous les cas, indépendante des acteurs que les autorités de contrôle nationales supervisent. Il convient de garder à l'esprit que la Commission exécute plusieurs fonctions différentes. Il n'est pas exclu que des autorités de contrôle nationales doivent examiner la conduite d'acteurs publics ou privés dans lesquels la Commission a un intérêt spécifique (par exemple, dans les questions de droit de la concurrence ou les cas de soutien financier par les fonds de l'UE).

254. Le pouvoir d'annuler les décisions d'une autorité de contrôle nationale n'est pas nécessaire pour l'exécution par la Commission de ses tâches en tant que gardienne des traités. Le pouvoir proposé ressemble, de façon superficielle, aux compétences de la Commission dans le domaine du droit de la concurrence, dans lequel elle coopère avec les autorités nationales compétentes. Cette compétence est, cependant, explicitement prévue à l'article 105 TFUE. Il n'existe pas de base juridique similaire en ce qui concerne la protection des données. Le CEPD considère que les principaux outils pour l'exécution par la Commission de ses tâches en tant que gardienne des traités dans ce domaine sont la procédure d'infraction normale telle qu'exposée aux articles 258 à 260 (dirigée contre les États membres) et son rôle consultatif dans le mécanisme de contrôle de la cohérence. Le CEPD suggère que ces compétences pourraient être complétées par un pouvoir pour la Commission de demander des mesures provisoires devant la Cour de justice, lesquelles pourraient inclure une ordonnance de suspension.

255. En conclusion, le CEPD recommande que le rôle de la Commission dans le mécanisme de contrôle de la cohérence consiste, dans une phase initiale, en le pouvoir de saisir le comité, comme prévu à l'article 58, paragraphe 4, et, dans une phase ultérieure, le pouvoir d'adopter des avis. L'article 59 devrait être développé dans cette perspective, dans le sens des suggestions formulées ci-dessus. Cette disposition doit notamment établir un lien clair entre le rôle du comité et toute position éventuelle de la Commission. Des procédures ultérieures initiées par la Commission doivent consister en des actions devant la Cour de justice, dans le contexte d'une procédure d'infraction ou une demande de mesures provisoires.

[54] Voir l'article 62, paragraphe 2, de la proposition de règlement.
[55] Voir l'arrêt *Commission/Allemagne* de la CJUE, à la note de bas de page 50.

II.9.c. Le comité européen de protection des données (chapitre VII, section 3)

256. Le CEPD accueille favorablement les dispositions de la proposition de règlement visant à davantage de cohérence et d'efficacité dans le rôle du comité européen de protection des données, agissant en tant que successeur du groupe de travail «Article 29». La proposition garantit également l'indépendance du comité en prévoyant un secrétariat indépendant de la Commission et par le biais d'une référence explicite à cette indépendance dans le texte de la proposition[56].

II.10. Recours, responsabilités et sanctions (chapitre VIII)

257. La proposition prévoit des possibilités détaillées de recours et de sanctions et elle précise la responsabilité des responsables du traitement par rapport aux dommages subis par les personnes concernées. Ces mesures sont conformes à l'objectif général de la proposition de règlement de renforcer l'application concrète des principes relatifs à la protection des données.

258. Si le CEPD soutient ces efforts visant à rendre le droit plus efficace, il soulignera également, dans les chapitres qui suivent, certaines complexités inhérentes au nouveau système des recours et aux rigidités indues dans la façon dont les sanctions doivent s'appliquer. Des suggestions seront émises dans le but de rendre le système plus accessible et plus flexible.

II.10.a. Recours

259. Le CEPD accueille favorablement le fait que la proposition de règlement prévoie plusieurs mécanismes de recours dans le but de faciliter son application par la personne concernée. Toutefois, il note que si l'un des fils rouges de la proposition est d'apporter une simplification au cadre actuel, les recours prévus dans la proposition ne soutiennent pas toujours cet objectif[57]. Les observations suivantes identifieront la nécessité d'une clarification ou d'une amélioration à cet égard.

260. Le CEPD accueille favorablement le (nouveau) droit pour les organisations ou associations qui défendent les droits et intérêts des personnes concernées d'introduire une réclamation auprès d'une autorité de contrôle ou de saisir une juridiction (voir les articles 73 et 76). Le CEPD note que, dans les deux cas, l'organisation ou l'association doit agir «au nom d'une ou plusieurs personnes concernées». Le CEPD suggère de préciser la nature du mandat que l'organisation doit obtenir des personnes concernées et le degré de formalité requis.

261. Le CEPD déplore qu'aucune action collective plus large n'ait été introduite dans la proposition, en parallèle avec la possibilité pour les organisations et les associations de défendre les droits des personnes concernées. Comme déjà mentionné dans son avis sur la communication de la Commission concernant un nouveau cadre relatif à la protection des données, des mécanismes de recours collectifs habilitant des groupes de citoyens à rassembler leurs réclamations dans une action unique pourraient constituer un outil très

[56] Voir l'article 65 de la proposition de règlement.

[57] De nombreuses procédures différentes peuvent être engagées au niveau des autorités de contrôle, dans le cadre ou en dehors des mécanismes de cohérence (par exemple, dans le cadre de contacts préliminaires ou d'enquêtes), ainsi qu'au niveau des tribunaux, dans différents pays et en relation avec diverses mesures.

puissant pour faciliter l'application des règles relatives à la protection des données[58]. Ces actions seraient notamment utiles dans les affaires ayant un impact plus faible, où il est peu probable que les victimes d'une violation des règles relatives à la protection des données intentent des actions individuelles à l'encontre d'un responsable du traitement, étant donné les frais, les retards, les incertitudes, les risques et les charges auxquels elles seraient exposées. Il suggère d'inclure une disposition plus large sur des actions collectives dans la proposition de règlement.

262. Le CEPD note que l'article 75, paragraphe 2, permet aux personnes concernées de disposer d'un recours juridictionnel dans le pays où elles résident. Bien que ce droit soit le bienvenu, il pourrait entraîner des situations complexes impliquant un tribunal d'un État membre et une autorité de contrôle d'un autre État membre, sur la base de l'établissement principal du responsable du traitement ou de son représentant. Il signifie également que des tribunaux pourraient être saisis dans tous les États membres où les personnes résident, indépendamment de l'État membre de l'autorité de contrôle compétente.

263. Le CEPD note que l'article 76, paragraphes 3 et 4, traite en partie de cette question étant donné qu'il prévoit des possibilités de suspendre une procédure devant un tribunal lorsque des procédures parallèles sont menées dans un autre État membre. Il suggère de développer davantage ce point, en prenant en considération la nécessité d'une harmonisation accrue et de procédures d'information plus systématiques au niveau des tribunaux.

264. Le CEPD soulève également la question de la compatibilité des critères déterminant la compétence des tribunaux conformément à la proposition avec les critères du règlement Bruxelles-I en ce qui concerne les actions délictuelles[59]. Dans ce contexte, le lieu où l'événement dommageable s'est produit ou peut *se produire* ainsi que le lieu de l'événement dommageable ou le lieu où le dommage a été *subi* pourrait être invoqué par la personne. Même si, dans les deux cas, le but est de garantir l'accès le plus direct au tribunal, au bénéfice de la victime, dans la pratique, cela peut entraîner un cumul du nombre de tribunaux éventuellement compétents. Le CEPD demande une précision dans la proposition sur son interaction avec le règlement Bruxelles-I.

265. Conformément à l'article 75, paragraphe 2, le droit de la personne concernée d'intenter une procédure devant le tribunal de son lieu de résidence ne s'appliquera pas si le responsable du traitement est une autorité publique. Le CEPD demande au législateur de veiller à ce que la dérogation ne s'applique pas à une autorité publique d'un pays tiers étant donné qu'en pareil cas, la dérogation priverait les personnes concernées d'un moyen de recours essentiel.

266. Le CEPD note également l'insertion dans la proposition d'un nouveau droit pour les personnes de demander à l'autorité de contrôle d'entamer une procédure contre l'autorité compétente dans un autre État membre si elles sont préoccupées par la

---

[58] Voir l'avis du CEPD du 14 janvier 2011, points 95 et suivants. Voir également l'avis du CEPD du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil sur le suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, JO C 255, 27.10.2007, p. 10.

[59] Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, JO L 12, 16.01.2001, p. 1. Voir également la proposition de règlement du Parlement et du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, COM(2010)748 final.

décision de cette autorité[60]. Une telle disposition peut se justifier par la nécessité de veiller à ce que les personnes concernées ne soient pas privées d'une possibilité de protection lorsque l'autorité «chef de file» dans une affaire spécifique, est située dans un autre État membre. Elle peut toutefois avoir des effets contreproductifs en termes de renforcement de la confiance et de la coopération entre autorités de contrôle.

267. Le CEPD considérerait extrêmement peu souhaitable que deux autorités de contrôle indépendantes deviennent des parties adverses dans une affaire devant un tribunal national: il se demande si une telle procédure renforcerait effectivement les droits des personnes concernées. Il privilégierait très fortement un renforcement du rôle du comité en cas de litige entre deux autorités plutôt qu'un règlement par le biais de procédures juridiques.

268. En tout état de cause, il conseille de préciser le type de «préoccupation» d'une personne concernée qui pourrait déclencher la procédure et de la limiter à un risque plus précis d'impact sur les droits de la personne concernée. En outre, l'autorité de contrôle qui est saisie par la personne concernée devrait avoir une liberté d'appréciation en ce qui concerne cette demande et pouvoir déterminer s'il existe des raisons suffisantes pour entamer une procédure contre une autre autorité de contrôle. Dans la pratique, il pourrait bien exister d'autres options disponibles pour parvenir à une issue satisfaisante.

II.10.b. Responsabilité (article 77)

269. L'article 77 se fonde sur la responsabilité des responsables du traitement pour les dommages subis par les personnes concernées, telle qu'établie à l'article 23 de la directive 95/46/CE. Il confirme que le responsable du traitement supporte le risque de ces dommages, hormis s'il peut prouver que le fait qui a provoqué le dommage ne lui est pas imputable. Cette approche est à présent étendue au sous-traitant et aux autres responsables du traitement ou aux sous-traitants impliqués dans le traitement, qui sont solidairement responsables de la totalité du montant du dommage, sous réserve de la même exception.

270. Cette approche est raisonnable et équitable du point de vue de la personne concernée. Elle ne sera généralement pas en mesure de faire beaucoup plus qu'alléguer une violation et un dommage subi du fait de cette violation. Par contre, les responsables du traitement et les sous-traitants ont davantage accès aux faits pertinents de l'événement une fois qu'ils ont été établis.

271. Toutefois, eu égard à la responsabilité du responsable du traitement, une personne concernée ne devrait pas avoir à choisir entre le responsable du traitement et le sous-traitant. Il devrait toujours être possible de s'adresser au responsable du traitement, indépendamment du lieu et de la façon dont le dommage est survenu. Le règlement devrait prévoir un règlement ultérieur des dommages entre le responsable du traitement et le sous-traitant, une fois que le partage des responsabilités entre eux a été clarifié. Il en va de même dans le cas de plusieurs responsables du traitement et sous-traitants.

272. Le CEPD recommande que l'article 77 soit modifié en ce sens. Il conviendrait également de prévoir une compensation pour les dommages immatériels ou le préjudice moral, étant donné que cela pourrait s'avérer particulièrement pertinent dans ce domaine.

[60] Voir l'article 74, paragraphe 4, de la proposition de règlement.

273. Enfin, il rappelle les questions qui se posent dans le contexte de groupes d'entreprises. Il pourrait être utile d'introduire également une disposition utilisant le concept d'une entité économique unique ou d'une entreprise unique[61]. Cela permettrait de tenir un groupe responsable des violations commises par une filiale.

II.10.c. Sanctions (article 79)

274. Le CEPD accueille favorablement le droit des autorités de contrôle d'ester en justice et d'infliger des sanctions réparatrices et administratives. Ces sanctions sont des éléments essentiels garantissant des pouvoirs d'exécution effectifs aux autorités de contrôle. Toutefois, aux fins d'assurer une clarté complète et la sécurité juridique, le CEPD demande des précisions supplémentaires concernant les circonstances dans lesquelles des sanctions administratives sont infligées.

275. Le CEPD note que la proposition semble accorder une très faible marge d'appréciation à une autorité en ce qui concerne les circonstances dans lesquelles elle aurait à infliger une sanction. Ce n'est que dans certains cas très limités de premier manquement non intentionnel qu'un avertissement peut remplacer la sanction. Il est dès lors d'autant plus important que les obligations en vertu de la proposition de règlement soient claires, notamment pour les responsables du traitement des données. Le CEPD demande une certaine flexibilité supplémentaire du système. Une liberté d'appréciation pour les autorités de contrôle en ce qui concerne les sanctions administratives est un élément indispensable d'un système d'exécution cohérent et modulaire. C'est d'autant plus vrai au regard des différentes options dont disposent les autorités de contrôle lorsqu'une violation particulière a été établie (voir également les observations formulées dans la partie II.8 sur les sanctions réparatrices).

276. À cet égard, il n'apparaît pas clairement si et comment une sanction est appliquée à un responsable du traitement des données qui n'a satisfait que partiellement à une obligation, par exemple, en prenant des mesures organisationnelles générales en ce qui concerne sa responsabilité en tant que responsable du traitement des données conformément à l'article 22, mais sans mettre en œuvre toutes les mesures qui y sont détaillées. Le CEPD considère que ce point doit être précisé dans le texte.

277. En outre, bien qu'il doive être clair qu'une violation s'est produite, des sanctions ne doivent pas être systématiquement infligées et une marge de manœuvre doit être laissée à l'autorité de contrôle, notamment dans les cas où les obligations de la proposition de règlement doivent être précisés dans un acte délégué ou un acte d'exécution (voir également la partie II.2.b ci-dessus) et où cet acte n'a pas (encore) été adopté. Tel est le cas, par exemple, en ce qui concerne la notification des violations de la sécurité, où le seuil à définir par la Commission apparaît comme un élément essentiel de l'obligation (article 79, paragraphe 6, point h)), ou dans le cas des obligations de «protection des données dès la conception», qui peuvent être spécifiées par le biais d'actes délégués et de normes techniques (voir l'article 79, paragraphe 6, point e)).

278. Le texte ne laisse pas non plus apparaître clairement dans quelle mesure des sanctions cumulatives, en relation avec des infractions liées, peuvent être infligées au même responsable du traitement et si plusieurs autorités de contrôle peuvent infliger la même

[61] Ce concept est couramment utilisé dans le droit européen de la concurrence vis-à-vis des multinationales; voir, par exemple, l'arrêt de la CJUE du 10 septembre 2009, *Akzo Nobel/Commission*, C-97/08 P, Recueil 2009, p. I-08237.

sanction administrative au même responsable du traitement. En tout état de cause, la relation et la coexistence éventuelle entre les décisions prises par des autorités de contrôle conformément à l'article 53 (par exemple, l'imposition d'une interdiction à un traitement, ou une ordonnance de réparation d'une violation d'une manière spécifique) et les sanctions ou amendes conformément aux articles 78 et 79 doivent être précisées, éventuellement dans des considérants, en tenant compte du principe du *ne bis in idem*, tel qu'interprété par la Cour de justice[62].

279. Des lignes directrices sur l'utilisation des différents pouvoirs d'exécution devraient être élaborées par les autorités de contrôle dans la pratique. Cela peut nécessiter une stratégie d'exécution soigneusement élaborée et cohérente, le cas échéant, coordonnée au niveau de l'UE au sein du comité, et rendue publique à large échelle pour un effet optimal. Le CEPD suggère de faire référence à ces lignes directrices à l'article 52, paragraphe 1, sur les devoirs des autorités, et éventuellement à l'article 66 également (sur les missions du comité).

280. Les relations entre les pouvoirs des autorités de contrôle et l'imposition de sanctions administratives ou d'amendes soulèvent également des questions de procédure plus générales. Le CEPD se demande dans quelle mesure les informations collectées auprès d'un responsable du traitement des données sur la base de l'article 53, paragraphe 1, point c), peuvent être utilisées pour infliger une sanction à ce responsable du traitement sans contrevenir au droit général de ne pas contribuer à sa propre incrimination.

II.11. Situations particulières de traitement des données (chapitre IX)

281. Dans la partie II.2.a, le CEPD a déjà formulé certaines observations générales concernant les dispositions relatives aux situations particulières de traitement des données contenues dans le chapitre IX de la proposition de règlement. Le CEPD s'interroge sur la nécessité des règles supplémentaires, rendues possibles en vertu de l'article 82. En outre, le CEPD recommande au législateur de remplacer le libellé «Dans les limites du présent règlement» par «Sans préjudice du présent règlement» aux articles 81, 82 et 84.

282. Dans cette partie, certaines observations supplémentaires seront formulées sur l'article 80 relatif à la liberté d'expression, l'article 81 sur le traitement de données à caractère personnel relatives à la santé et l'article 83 sur le traitement de données à des fins de recherche historique, statistique et scientifique.

II.11.a. Liberté d'expression et accès public aux documents (article 80)

i) Liberté d'expression

283. La conciliation de la liberté d'expression avec le droit au respect de la vie privée et la protection des données est une question complexe. Ce qui est considéré comme représentant un juste équilibre entre les deux droits fondamentaux est déterminé dans une large mesure par les traditions culturelles nationales. Pour ce motif, en vertu de la Convention européenne des droits de l'homme («CEDH»), les États membres du Conseil de l'Europe conservent un pouvoir d'appréciation, ainsi qu'il résulte de nombreuses affaires devant la Cour européenne des droits de l'homme sur cette

[62] Voir, par exemple, l'arrêt de la CJUE du 11 février 2003, *Gözütok et Brügge*, C-187/01 et C-385/01, Recueil 2003, p. I-1345.

question[63]. Le CEPD soutient pleinement la flexibilité accordée aux États membres, en vertu de l'article 80, de mettre en place des exemptions ou des dérogations aux dispositions du règlement.

284. Toutefois, le CEPD estime que la révision des règles existantes sur la protection des données devrait améliorer la façon dont les règles de l'UE permettent cette flexibilité, mais ne devrait pas réduire leur impact. L'article 80 proposé est presque entièrement fondé sur l'article 9 de la directive 95/46/CE, avec une différence significative qui sera discutée ci-dessous.

285. Selon le CEPD, il existe un motif pour une plus grande modification de fond en raison du fait que, depuis l'adoption de la directive 95/46/CE, l'internet s'est développé dans le monde entier comme étant le principal support pour l'expression des informations, des avis et des idées. Bien que la liberté de la presse ait toujours été considérée comme étant au cœur de la liberté d'expression, en raison du rôle joué par la presse en tant qu'organe de vigilance, il est clair que dans notre société contemporaine, ce rôle n'est plus exclusivement joué par la presse traditionnelle. Par exemple, au moyen d'un blog, chaque citoyen peut agir en tant qu'organe de vigilance.

286. Ce développement a été reconnu par la Cour de justice, dans l'arrêt *Satamedia*, mentionné au considérant 121 de la proposition de règlement[64]. Le libellé potentiellement restrictif de l'actuel article 9 de la directive 95/46/CE («aux seules fins de journalisme») a été interprété de façon si large par la Cour de justice que ce libellé n'a pas de véritable valeur substantielle. Dès lors, le CEPD recommande de supprimer ce libellé de l'article 80 et de simplifier la disposition en faisant uniquement référence à la notion générale de liberté d'expression. En outre, la référence aux fins d'expression artistique ou littéraire peut être supprimée étant donné qu'elle est également couverte par la notion de liberté d'expression.

287. Le CEPD suggère que l'article 80 déclare que les États membres prévoient des exemptions ou des dérogations aux dispositions incluses dans le règlement (comme déjà indiqué dans le texte actuel) si cela s'avère nécessaire pour concilier le droit à la protection des données avec le droit à la liberté d'expression. En outre, il pourrait être ajouté, dans la disposition ou dans un considérant, que lors de la conciliation des deux droits fondamentaux, il ne doit pas être porté atteinte au contenu essentiel des deux droits[65].

288. Le CEPD recommande également fermement le maintien du mot «nécessaires», tel qu'il figure dans l'actuel article 9 de la directive 95/46/CE, et de ne pas introduire le libellé plus faible «pour» tel que proposé à l'article 80. Bien entendu, des exceptions aux deux droits fondamentaux devraient être nécessaires, ce qui pourrait être perçu comme neutralisant la notion. Toutefois, la proposition de règlement élabore les règles pour un seul des deux droits fondamentaux concernés, à savoir le droit à la protection des données. Il y a tout lieu de souligner dans le présent instrument qu'il n'est possible de déroger à ces règles que dans la mesure réellement nécessaire pour concilier le droit à la protection des données avec le droit à la liberté d'expression.

[63] Voir, par exemple, l'arrêt de la CEDH du 24 juin 2004, *Von Hannover/Allemagne*, 59320/00, *RJD* 2004-VI.
[64] Voir l'arrêt *Satamedia*, cité à la note de bas de page 31.
[65] Voir l'arrêt de la CJUE du 12 juin 2003, *Schmidberger*, C-112/00, Recueil 2003, p. I-5659, point 80.

289. La condition de nécessité souligne le fait que les États membres doivent soigneusement examiner pour quelles activités de traitement des données il est réellement nécessaire de déroger aux règles générales relatives à la protection des données.

ii) Accès public aux documents

290. Tout comme pour la liberté d'expression, la conciliation de la protection des données avec les règles en matière d'accès public est une question sensible. Les États membres disposent de lois et pratiques largement divergentes dans ce domaine et la compétence de l'UE pour harmoniser la question est, contrairement au droit à la protection des données, limitée par le traité de Lisbonne à l'accès aux documents des institutions de l'UE (article 15 TFUE).

291. Le considérant 18 de la proposition de règlement est largement similaire au considérant 72 de l'actuelle directive 95/46/CE. Il mentionne que le règlement autorise la prise en considération, dans la mise en œuvre de ses dispositions, du principe d'accès du public aux documents administratifs. Toutefois, avec l'instrument d'un règlement, la façon dont cela peut réellement se faire est encore moins évidente. Le CEPD estime qu'une disposition substantielle doit être incluse dans la proposition de règlement.

292. Le CEPD recommande que le législateur ajoute une disposition dans la proposition de règlement, déclarant que les données à caractère personnel dans les documents détenus par les autorités et organismes publics peuvent être divulguées publiquement si cela 1) est prévu par le droit de l'UE ou le droit national, 2) est nécessaire pour concilier le droit à la protection des données avec le droit d'accès du public aux documents administratifs et 3) constitue un juste équilibre entre les divers intérêts concernés.

II.11.b. Traitements de données à caractère personnel relatives à la santé (article 81)

293. Il y plusieurs modifications proposées en ce qui concerne le traitement des données relatives à la santé. D'une part, ces modifications clarifient et harmonisent certaines questions, l'article 4, paragraphe 12, et le considérant 26 de la proposition de règlement définissent la notion de «données relatives à la santé» et l'article 81 illustre la liste des motifs pour lesquels les données relatives à la santé peuvent être traitées, si nécessaires sans le consentement de la personne concernée. De même, la référence «Dans les limites du présent règlement», comme discuté dans la partie II.2.a.ii), qui devrait plutôt être remplacée par «sans préjudice au règlement», devrait veiller à ce que les règles relatives à la protection des données soient également applicables au secteur des soins de santé. Le CEPD accueille favorablement ces modifications.

294. D'autre part, les modifications proposées soulèvent également de nouvelles questions qui nécessitent une clarification. Plus particulièrement, la relation entre l'article 9 et l'article 81 prête à confusion. En outre, considérées globalement, les modifications ne traitent pas tous les obstacles qui se sont présentés en vertu de l'article 8 de la directive 95/46/CE.

295. Le lien entre l'article 9 et l'article 81 est établi à l'article 9, paragraphe 2, point h). Cet article énonce que l'interdiction de traitement des données relatives à la santé est levée si le traitement est nécessaire à des fins liées à la santé, sous réserve des conditions et des garanties prévues à l'article 81. Toutefois, le traitement des données relatives à la santé est également possible pour d'autres motifs énoncés à l'article 9, paragraphe 2,

sans référence à l’article 81. Le fait que plusieurs de ces autres motifs se chevauchent avec les motifs énoncés à l’article 81, paragraphes 1 et 2, prête à confusion.

296. À l'article 81, paragraphe 1, points b) et c), il est fait référence à des «motifs d'intérêt général», ce qui ressemble au libellé de l'article 9, paragraphe 2, point g), qui lève l'interdiction de traitement de catégories particulières de données, si le traitement est nécessaire à l'exécution d'une mission effectuée «dans l'intérêt général». Le traitement de données relatives à la santé à des fins de recherche historique, statistique et scientifique est traité à l'article 81, paragraphe 2, mais est également autorisé en vertu de l'article 9, paragraphe 2, point i), dans les deux cas, sous réserve des conditions et garanties visées à l'article 83. Il convient de souligner que l'article 81 n'établit pas de distinction entre entités publiques ou privées. En outre, la Commission est habilitée à deux reprises (à l'article 9, paragraphe 3, et à l'article 81, paragraphe 3) à adopter des actes délégués dans le domaine des données relatives à la santé; toutefois, les dispositions sont formulées de manière légèrement différente.

297. À la lumière de ces observations, le CEPD recommande au législateur de mettre ces deux dispositions en équation et de préciser le champ d'application et la nature de l'article 81.

298. Ceci amène à une autre préoccupation. Plusieurs complications se sont produites dans le contexte national et transfrontalier concernant la protection des données relatives à la santé. Pour citer quelques exemples, les différentes exigences en matière de consentement dans ce domaine ont été relevées comme constituant des obstacles à l'échange transfrontalier des données relatives à la santé. En outre, la détermination de la responsabilité peut être très compliquée dans le secteur des soins de santé, étant donné que de longues chaînes de praticiens peuvent être concernées. Cela devient encore plus compliqué avec le développement des applications dans le domaine de la santé en ligne, étant donné que des acteurs extérieurs au secteur des soins de santé (producteurs de dispositifs techniques, prestataires de services de communication, etc.) sont également impliqués. En outre, les exigences en matière de sécurité sont insuffisamment harmonisées et, actuellement, un traitement ultérieur à des fins historiques, statistiques ou scientifiques est dépourvu de base juridique claire dans l'actuelle directive 95/46/CE. Seule cette dernière question a été résolue dans l'actuelle proposition.

299. Le CEPD est conscient des sensibilités nationales dans le domaine des soins de santé et de la compétence limitée de l'UE dans ce domaine. Toutefois, il recommande que le législateur harmonise davantage la législation nationale en donnant une nouvelle orientation sur l'exigence du consentement, la détermination des responsabilités et les exigences en matière de sécurité. Il semble y avoir un déséquilibre dans l'actuelle proposition entre les motifs détaillés pour le traitement des données relatives à la santé, d'une part, et l'absence d'assurance correspondante pour la protection des personnes concernées dans ce domaine, d'autre part.

II.11.c. Traitements de données à des fins de recherche historique, statistique et scientifique (article 83)

300. Le CEPD accueille favorablement la disposition spécifique sur les traitements de données à des fins de recherche historique, statistique et scientifique. Il déplore toutefois qu'aucune distinction n'y soit établie entre le traitement, à ces fins, de catégories particulières de données et d'autres données à caractère personnel. Il devrait être précisé que des garanties supplémentaires doivent être mises en place si des catégories particulières de données (telles que des données relatives à la santé) sont traitées.

301. En outre, le CEPD recommande au législateur de remplacer le libellé «Dans les limites du présent règlement» par «Sans préjudice du présent règlement»[66]. Contrairement aux articles 81, 82 et 84, la disposition de l'article 83 n'autorise pas de règles nationales spécifiques. La disposition contient des conditions supplémentaires et est mentionnée dans tout le règlement. Il doit être clairement mentionné que cette disposition est sans préjudice d'autres dispositions dans le règlement. Par exemple, les fins de recherche, en tant que telles, doivent être légitimes et conformes au règlement.

302. Le point de départ pour le traitement des données à des fins de recherche historique, statistique et scientifique doit être que ce traitement est effectué en utilisant des données rendues anonymes. Ce point devrait être mentionné de façon plus explicite au premier paragraphe de l'article 83. Il ne pourrait en aller autrement que si cela s'avérait impossible pour effectuer les recherches. Le responsable du traitement doit pouvoir justifier et démontrer la nécessité de traiter les données des personnes concernées. Le CEPD accueille favorablement la garantie explicite mentionnée à l'article 83, paragraphe 1, point b), mais voudrait encourager le législateur à préciser ce que signifie le mot «séparément» et à veiller à ce que cette conservation séparée protège réellement les personnes concernées.

303. L'article 83, paragraphe 1, point b), fait référence aux «données permettant de rattacher des informations à une personne concernée identifiée ou identifiable». Le CEPD recommande vivement de mettre cette phrase en équation avec les définitions proposées à l'article 4, paragraphes 1 et 2. Il serait plus approprié de faire référence aux «données qui permettent de relier certaines informations à une personne concernée».

304. Une dernière observation concerne le pouvoir accordé à la Commission, en vertu de l'article 83, paragraphe 3, d'adopter des actes délégués. Le CEPD est préoccupé par la délégation à la Commission du pouvoir d'établir «toute limitation nécessaire des droits d'information et d'accès de la personne concernée» et de préciser les conditions et garanties applicables aux droits de la personne concernée dans les circonstances en cause. Le CEPD estime qu'une limitation des droits des personnes concernées ne doit pas être effectuée au moyen d'un acte délégué. Si des limitations sont nécessaires, elles doivent être incluses dans la disposition elle-même.

CHAPITRE III - COMMENTAIRES SUR LA PROPOSITION DE DIRECTIVE

III.1. Introduction

305. Le traitement de données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale, qui, par sa nature même, pose des risques spécifiques pour le citoyen, requiert un niveau de protection des données au moins aussi élevé que dans le cadre de la proposition de règlement, voire plus élevé en raison de sa nature intrusive et de l'impact majeur que ce traitement peut avoir sur la vie de la personne.

306. Si le domaine répressif exige certaines règles spécifiques, toute déviation des règles générales relatives à la protection des données doit être dûment justifiée, sur la base d'un équilibre approprié entre l'intérêt général dans le contexte répressif et les droits fondamentaux des citoyens.

[66] La même recommandation a été formulée à l'égard des articles 81, 82 et 84 de la proposition de règlement.

307. Dans une société démocratique, des divergences importantes entre la protection des données dans le domaine répressif et dans d'autres domaines saperait non seulement le droit fondamental à la protection des données à caractère personnel, mais aurait également un effet préjudiciable sur l'efficacité de la répression, la confiance mutuelle entre les États membres et la confiance du citoyen dans le fait que l'État se comportera d'une façon respectueuse de la loi et responsable.

308. Au considérant 7 de la proposition de directive, il est mentionné que le niveau de protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes devrait être équivalent dans tous les États membres. Le CEPD accueille favorablement cette déclaration. L'un des principaux arguments en faveur de ce paquet de réformes tient au fait que, dans le cadre du traité de Lisbonne, il est nécessaire de disposer d'un système robuste de protection des données qui offre une protection égale à toutes les personnes concernées, indépendamment de leur lieu de résidence. Cet argument s'applique pleinement au domaine de la coopération policière et judiciaire en matière pénale.

309. Le CEPD accueille favorablement le fait que la proposition de directive, contrairement à la décision-cadre 2008/977/JAI, couvre également le traitement national des données à caractère personnel. Toutefois, comme mentionné au chapitre I du présent avis, cette garantie n'offre de plus-value que si la directive renforce substantiellement le niveau de protection des données dans ce domaine, ce qui n'est pas le cas.

310. Le CEPD estime que la proposition de directive, à bien des égards, ne satisfait pas à l'exigence d'un niveau cohérent et élevé de protection des données, décrit par la Commission elle-même comme étant «crucial» (voir le considérant 7). Dans de nombreux cas, il n'existe pas la moindre justification pour s'écarter des dispositions des règles générales dans la proposition de règlement. Le CEPD est préoccupé en particulier en ce qui concerne:
- le manque de clarté dans la rédaction du principe de limitation de la finalité (voir la partie III.4.a);
- l'absence d'une obligation pour les autorités compétentes de démontrer la conformité avec la directive (voir la partie III.6);
- les conditions insuffisantes pour les transferts vers des pays tiers (voir la partie III.7);
- les pouvoirs indûment limités des autorités de contrôle (voir la partie II.8.a).

III.2. Questions horizontales

311. Cette partie traitera brièvement de l'absence d'une obligation générale d'évaluer les opérations existantes de traitement, du manque de clarté concernant les règles applicables aux transferts de données entre les autorités compétentes répressives et d'autres autorités ou des entités privées, et du traitement des données relatives aux enfants.

III.2.a. Actes spécifiques dans le domaine de la coopération policière et judiciaire en matière pénale

312. Ainsi qu'il est déclaré dans la partie I.2.a, le CEPD déplore que la proposition de directive laisse intacts tous les actes spécifiques dans le domaine de la coopération

policière et judiciaire en matière pénale (voir l'article 59 de la proposition de directive)[67].

313. Il est mentionné à l'article 61, paragraphe 2, de la proposition de directive que dans un délai de trois ans à compter de l'entrée en vigueur de la présente directive, la Commission réexamine ces actes. Comme mentionné, le CEPD estime qu'un tel délai entraînerait une période d'une durée inacceptable, durant laquelle la mosaïque actuelle, largement critiquée, resterait en vigueur.

314. Étant donné qu'une clarification de l'ensemble du cadre doit être apportée dans les plus brefs délais, le CEPD recommande vivement au législateur de fixer un délai beaucoup plus strict qui veille à ce que les règles spécifiques soient modifiées au plus tard au moment de l'entrée en vigueur de la directive.

III.2.b. Mécanismes d'évaluation

315. Le CEPD se réjouirait d'une disposition obligeant les États membres à introduire des mécanismes d'évaluation pour des évaluations régulières basées sur la preuve que les activités de traitement des données d'une certaines envergure constituent réellement une mesure nécessaire et proportionnée à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. Ces mécanismes sont des bonnes pratiques normales dans les administrations publiques modernes. Un tel mécanisme constituerait une garantie efficace contre des activités inutiles de traitement des données et un développement indu de telles activités.

III.2.c. Transferts vers d'autres autorités publiques ou parties privées

316. Le CEPD souhaite répéter les observations formulées dans la partie I.2.b selon lesquelles les deux instruments proposés n'offrent pas un cadre juridique clair pour les situations où il existe un éventail d'acteurs et de finalités couverts par les deux instruments différents.

317. Cela ne concerne pas uniquement l'utilisation par les autorités répressives de données collectées par des entités privées à des fins commerciales, mais aussi la situation où une autorité répressive transfère les données qu'elle a collectées à une partie privée à des fins d'exécution de la loi ou à une autre autorité publique à des fins non liées[68]. La proposition de directive devrait préciser les conditions dans lesquelles un tel traitement est autorisé.

318. L'actuel article 7, point b), semble offrir une base juridique générale pour un tel transfert de données (voir également, en ce qui concerne cette disposition, la partie III.4.a. i) ci-dessous). Toutefois, la proposition de directive n'établit aucune garantie spécifique pour les transferts de données à caractère personnel à des parties privées ou des autorités non répressives. À cet égard, le principe 5 de la recommandation n° R(87)15 du Conseil de l'Europe prévoit que la communication de données à caractère personnel par des services de police à d'autres organes publics ou à des personnes privées ne devrait être permise qu'à des conditions strictes et spécifiques.

[67] Voir, par exemple, la décision du Conseil 2008/615/JAI citée à la note de bas de page 16.

[68] Par exemple, les services de police pourraient être tenus, en vertu du droit national, de communiquer des informations aux services de l'immigration, à l'administration fiscale ou aux tribunaux civils (ou ces destinataires pourraient être autorisés, en vertu du droit national, à recevoir des informations fournies par les autorités répressives compétentes).

319. Le CEPD recommande dès lors que le législateur insère une disposition imposant ces conditions strictes et spécifiques.

III.2.d. Traitement des données relatives aux enfants

320. Le CEPD relève que, contrairement à la proposition de règlement, aucune attention particulière n'est accordée à la position des enfants dans le cadre de la proposition de directive. Toutefois, dans le domaine couvert par la proposition, les enfants méritent un traitement particulier.

321. Une attention spécifique doit être accordée en particulier à la question de la précision des données d'identification des enfants et de leur fiabilité au fil du temps: par exemple, le niveau de précision des données biométriques, telles que les empreintes digitales ou l'image faciale, est différent de celui des adultes, et ces données peuvent changer beaucoup plus rapidement au fil du temps. Étant donné que certaines décisions en relation avec un enfant sont également fondées sur la vérification de l'âge, des garanties spécifiques doivent être prises afin que seules les données nécessaires soient collectées et conservées. En outre, les données des enfants peuvent être assujetties à des périodes de conservation différentes, en relation avec la fiabilité et la finalité de leur conservation et en raison de règles spéciales de la procédure pénale pour les mineurs.

322. Le CEPD recommande dès lors que la nécessité de garanties spécifiques en ce qui concerne le traitement des données des enfants soit spécifiquement mentionnée dans la proposition de directive, dans une disposition de fond.

III.3. Dispositions générales (chapitre I)

323. Conformément à l'article 1, paragraphe 1, la proposition de directive établit les règles visant à assurer la protection de données à caractère personnel au cours des activités de coopération policière et judiciaire en matière pénale. L'article 1, paragraphe 1, doit être lu conjointement avec l'article 2, paragraphe 1, déclarant que la proposition s'applique au traitement de données à caractère personnel effectué par les autorités compétentes aux fins de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière (mentionnées dans cet avis comme étant les «finalités répressives»).

324. L'article 2, paragraphe 3, exclut du champ d'application de la proposition le traitement des données à caractère personnel au cours d'une activité n'entrant pas dans le champ d'application du droit de l'Union, en ce qui concerne notamment la sécurité nationale. Tout comme pour la disposition équivalente dans la proposition de règlement (article 2, paragraphe 2, point a), voir la partie II.3.a.i)), le CEPD souhaiterait faire une observation générale selon laquelle, si la «sécurité nationale» n'entre pas dans le champ d'application du droit de l'Union, ce que cette notion couvre n'apparaît pas toujours très clairement, étant donné qu'elle dépend de la politique nationale des États membres. Au niveau national, l'utilisation du libellé «sécurité nationale» ou «sûreté de l'État», selon les États membres, avec un champ d'application différent, peut également prêter à confusion. De toute évidence, le CEPD ne conteste pas l'exception, mais considère qu'il convient d'éviter son utilisation indue pour légitimer le traitement des données à caractère personnel en dehors du champ d'application du règlement et de la directive, par exemple dans le cadre de la lutte contre le terrorisme.

325. Une autorité compétente est définie à l'article 3, paragraphe 14), comme étant toute autorité compétente pour la prévention, l'enquête, la détection et l'exécution d'infractions pénales,. Le CEPD a mentionné ci-dessus que la notion d'autorité compétente devrait être appliquée de façon cohérente dans les deux instruments proposés (voir la partie II.3.a.(iv)).

III.4. Principes (chapitre II)

326. Il existe des différences considérables entre les dispositions contenues dans le chapitre II de la proposition de directive et celles contenues dans le chapitre II de la proposition de règlement.

327. L'article 4 de la proposition de directive contient les principes concernant le traitement des données et constitue l'équivalent de l'article 5 de la proposition de règlement. Toutefois, par rapport à la proposition de règlement, certains principes font défaut ou doivent être précisés davantage dans le contexte de la proposition de directive. En particulier, le principe de limitation de la finalité contenu à l'article 4, point b), lu conjointement avec l'article 7 de la proposition de directive, a besoin d'une clarification.

328. Les dispositions qui diffèrent de la proposition de règlement sont la distinction entre les différentes catégories de personnes concernées et les différents degrés de précision et de fiabilité des données à caractère personnel. Le CEPD accueille favorablement ces dispositions mais conseillerait au législateur de les renforcer.

329. Dans la proposition de directive, une attention spécifique est également accordée au traitement de catégories particulières de données. Toutefois, l'actuelle disposition (article 8) ne fournit pas d'indications suffisantes quant à la façon dont ces données devraient être traitées différemment.

III.4.a. Principes relatifs au traitement des données à caractère personnel (article 4) et licéité du traitement (article 7)

i) Limitation de la finalité (article 4, point b)) et licéité du traitement (article 7)

330. L'article 4, point b), contient le principe de limitation de la finalité dans un libellé qui est similaire à l'actuel article 6, paragraphe 1, point b), de la directive 95/46/CE et à l'article 5, point b), de la proposition de règlement: «les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités».

331. Le CEPD accueille favorablement cette approche cohérente. Toutefois, la véritable valeur du principe de limitation de la finalité dépend 1) de l'interprétation de la notion d'utilisation compatible, et 2) des éventuelles dérogations au principe de limitation de la finalité, en d'autres termes, des possibilités et des conditions pour une utilisation *incompatible*.

332. Il va sans dire qu'il devrait exister une sécurité juridique quant à l'utilisation ultérieure des données à caractère personnel par les autorités répressives. Malheureusement, cette spécification est absente de la proposition de directive.

333. Quant à la notion d'utilisation compatible, le CEPD a formulé certaines observations ci-dessus, sur l'article 5, point b), de la proposition de règlement (voir la partie II.4.a). Si

les considérants de la proposition de règlement tentent au moins de proposer une certaine orientation sur ce qui constitue une finalité compatible, une telle précision est absente de la proposition de directive.

334. Le CEPD recommande dès lors d'introduire une telle précision dans les considérants de la proposition de directive. Plus particulièrement, la proposition de directive devrait préciser que la notion d'utilisation compatible doit être interprétée de façon restrictive. Il doit également être précisé qu'une finalité pour une utilisation ultérieure n'est pas nécessairement compatible avec la finalité initiale, au simple motif que cette finalité ultérieure est également une finalité répressive. En d'autres termes, il devrait être clair que dans le contexte répressif, des finalités différentes peuvent être incompatibles. Toute autre interprétation rendrait l'exigence contenue à l'article 4, point b), (déterminées, explicites et légitimes) vide de sens.

335. En ce qui concerne une utilisation ultérieure pour une finalité *incompatible*, qu'il s'agisse d'une finalité qui s'inscrit dans ou en dehors du contexte répressif, la proposition de directive, à proprement parler, n'offre aucune base juridique justifiant un tel traitement. Conformément à la logique de l'actuelle directive 95/46/CE, un tel traitement devrait être abordé dans une disposition séparée qui, pour un nombre limité de motifs et sous réserve de conditions strictes, autorise une dérogation au principe de limitation de la finalité (voir l'article 13 de la directive 95/46/CE). Une telle disposition est absente de la proposition de directive.

336. Toutefois, la possibilité de s'écarter du principe de limitation de la finalité semble être implicitement acceptée dans la disposition sur la licéité du traitement, à savoir l'article 7 de la proposition de directive. Bien qu'il ne soit fait aucune référence à une éventuelle dérogation au principe de limitation de la finalité, les motifs énoncés à l'article 7, points b), c) et d), peuvent faire référence à des situations qui supposent un traitement des données pour des finalités incompatibles, y compris des finalités qui s'inscrivent hors du contexte répressif. Cela est contraire à la logique de la directive 95/46/CE, dans laquelle la disposition sur la licéité du traitement (article 7) a trait aux motifs légitimes pour la finalité *initiale* du traitement des données (et une utilisation ultérieure compatible).

337. Le CEPD ne voit pas de raison de s'écarter de la logique de la directive 95/46/CE et d'affaiblir les exigences existantes (voir également, à cet égard, la critique sur la modification apportée dans la proposition de règlement, dans la partie II.4.a ci-dessus). Le CEPD recommande dès lors d'établir une distinction claire entre la licéité du traitement des données à caractère personnel pour une finalité déterminée, explicite et légitime et les dérogations conformément auxquelles des données à caractère personnel peuvent être utilisées ultérieurement pour une finalité incompatible avec la finalité initiale.

338. Cela nécessiterait la modification de l'article 7, point a), en une disposition autonome garantissant, de manière générale, que toutes les opérations de traitement des données sont prévues par la loi, satisfaisant ainsi aux exigences de la Charte des droits fondamentaux et de la CEDH, notamment en ce qui concerne l'accessibilité et la prévisibilité de la loi, telles que développées par la Cour européenne des droits de l'homme, en vertu de l'article 8, paragraphe 2, CEDH.

339. L'article 7, points b) à d), devrait être remplacé par une disposition supplémentaire, séparée, qui énonce de façon exhaustive les motifs d'intérêt général pour lesquels une

dérogation au principe de limitation de la finalité peut être autorisée. Cette disposition devrait fixer les conditions dans lesquelles la dérogation peut être invoquée. Toute modification de la finalité devrait satisfaire aux exigences de proportionnalité et nécessité. Une modification de la finalité devrait également, comme indiqué ci-dessus, être prévue par la loi, conformément à la Charte et à la CEDH. Une utilisation accessoire ne doit avoir lieu qu'en cas de nécessité, dans un cas spécifique, par exemple, pour la protection immédiate des intérêts vitaux de la personne concernée ou d'une autre personne ou pour prévenir une menace immédiate et sérieuse contre la sécurité publique.

340. Comme à l'article 6, paragraphe 2, de la proposition de règlement, la proposition de directive devrait également inclure une disposition sur le traitement des données à caractère personnel à des fins de recherche historique, statistique et scientifique, contenant des garanties similaires à celles visées à l'article 83 de la proposition de règlement.

ii) Qualité des données (article 4, points c) à e))

341. L'article 4, points c) à e), énonce des principes sur la qualité des données qui, dans une grande mesure, sont similaires à ceux incorporés à l'article 6, paragraphe 1, point d), de la directive 95/46 et à l'article 5 de la proposition de règlement.

342. Dans le contexte répressif, en particulier, le CEPD recommande de prévoir, dans la proposition de directive, une obligation pour l'autorité compétente de mettre en place des mécanismes pour garantir que des délais sont établis pour l'effacement des données à caractère personnel et pour une révision périodique de la nécessité de conservation des données.

343. Cette obligation pour un examen périodique est typique du domaine de la coopération policière et judiciaire. Elle est présente dans les instruments existants tels que l'article 20 de la décision Europol et l'article 112 de la convention de Schengen[69].

344. En outre, conformément à la recommandation 87/15 du Conseil de l'Europe, des règles visant à fixer des périodes de conservation pour différentes catégories de données à caractère personnel (voir ci-dessous) ainsi que des vérifications régulières de leur qualité doivent être établies afin de s'assurer que les fichiers de police sont tenus à jour et purgés des données superflues ou inexactes[70].

345. Ainsi que le CEPD l'a souligné dans son troisième avis sur la décision-cadre 2008/977/JAI, les distinctions entre les différentes catégories de données à caractère personnel sont nécessaires non seulement pour la protection des données à caractère personnel de la personne mais aussi pour le bon fonctionnement des services de police[71]. Des informations anciennes et désuètes sont, au mieux, inutiles et, au pire, trompeuses, détournant des ressources de leurs priorités actuelles vers des questions qui

[69] Voir la décision du Conseil 2009/371/JAI, citée à la note de bas de page 16 et le règlement (CE) n° 1987/2006 du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS), JO L 381, 28.12.2006, p. 4.

[70] Voir le principe 7 de la recommandation (durée du stockage et mise à jour des données) ainsi que les points 96 à 98 de l'exposé des motifs. Une attention particulière doit être accordée, en l'espèce, aux fichiers temporaires, aux fichiers «morts» et aux fichiers de renseignements.

[71] Voir le troisième avis du CEPD du 27 avril 2007 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO C 139, 23.06.2007, p. 1, point 32.

ne sont pas, et ne doivent pas être, la cible des enquêtes nécessaires pour la capacité des destinataires.

iii) Démonstration de la conformité avec la proposition de directive (article 4, point f))

346. L'article 5, point f), de la proposition de règlement expose le principe général selon lequel les responsables du traitement doivent *assurer et démontrer* la conformité aux dispositions du règlement pour chaque opération de traitement. Toutefois, la disposition équivalente de la proposition de directive (article 4, point f)) fait uniquement référence à une obligation générale incombant au responsable du traitement de *veiller à* la conformité avec les dispositions adoptées conformément à la directive.

347. Rien ne justifie que l'on n'exige pas du responsable du traitement qu'il *démontre* également la conformité. L'obligation de conserver une trace documentaire en vertu de l'article 23 de la proposition de directive doit être liée à l'obligation générale de démontrer la conformité, comme dans le cadre de l'article 5, point f), l'article 22 et l'article 28 de la proposition de règlement. En outre, le responsable du traitement doit être tenu d'assurer et de démontrer la conformité *pour chaque opération de traitement*.

348. Le CEPD recommande dès lors de mettre en adéquation le libellé de l'article 4, point f), de la proposition de directive avec l'article 5, point f), de la proposition de règlement et de modifier les articles 18 et 23 de la proposition de directive en conséquence.

III.4.b. Distinction entre les catégories de personnes concernées (article 5)

349. L'article 5 énonce l'obligation pour le responsable du traitement d'établir une distinction claire entre les données à caractère personnel de différentes catégories de personnes (suspects, condamnés, victimes, informateurs, contacts, autres).

350. Le CEPD soutient pleinement l'introduction de cette obligation en tant que règle spécifique de protection des données dans le domaine répressif. Il est essentiel, non seulement du point de vue de la personne concernée, mais aussi pour les autorités répressives, que les données liées aux différentes catégories de personnes soient distinguées selon les différents degrés d'implication dans une infraction, et soient traitées différemment. Des distinctions comparables sont également prévues dans la législation de l'UE pour la coopération policière, telle que l'article 14, paragraphe 1, de la décision Europol[72].

351. Le CEPD recommande d'ajouter la catégorie des personnes non suspectes à l'article 5. Des conditions et garanties spécifiques sont nécessaires pour assurer une utilisation proportionnée des données concernant ces personnes et pour éviter de porter préjudice à des personnes qui ne sont pas activement impliquées dans une infraction.

352. En outre, le CEPD considère que l'article 5 devrait être renforcé par la suppression du libellé «dans la mesure du possible» et par la spécification des conséquences de la catégorisation pour les différents personnes concernées.

353. Le libellé «dans la mesure du possible» n'est pas nécessaire étant donné que, lors de la collecte des données, les autorités répressives doivent avoir une finalité spécifique et doivent dès lors, au moment de la collecte, avoir un avis *prima facie* sur la catégorie à

[72] Voir la décision du Conseil 2009/371/JAI, citée à la note de bas de page 69.

laquelle les données sont liées. Si les autorités répressives ont encore des doutes concernant la façon de catégoriser les données collectées durant la première phase de l'enquête (par exemple, des données à caractère personnel contenues dans un répertoire), elles peuvent utiliser la catégorie «autres». Bien sûr, cette catégorisation sera ajustée en fonction des besoins, au fur et à mesure que l'enquête progressera.

354. Le CEPD recommande en outre d'inclure, dans la disposition, l'obligation pour les États membres de spécifier les conséquences de la catégorisation, en reflétant les particularités des différentes catégories de données traitées et les différentes finalités pour lesquelles ces données sont collectées par des autorités répressives et judiciaires. Ces conséquences doivent concerner les conditions pour la collecte des données, les délais, les limitations aux droits d'accès et d'information des personnes concernées, les modalités d'accès aux données par les autorités compétentes.

III.4.c. Différents niveaux de précision et de fiabilité des données à caractère personnel (article 6)

355. L'article 6 de la proposition de directive prévoit que les différentes catégories de données seront distinguées conformément à leurs niveaux de précision et de fiabilité et que les données à caractère personnel fondées sur des faits seront distinguées de celles fondées sur des appréciations personnelles. Il s'agit d'une disposition importante étant donné que les autorités répressives utilisent également des données non vérifiées, fondées sur des présomptions plutôt que sur des faits.

356. Le CEPD accueille favorablement cette disposition et souligne son importance tant pour les personnes concernées que pour les autorités répressives. Il est possible de le constater, notamment, dans l'échange de données entre autorités répressives, lorsque les données peuvent être traitées loin de leur source et totalement en dehors du contexte dans lequel elles ont été collectées et utilisées à l'origine. Le fait de ne pas désigner leur niveau de précision et de fiabilité pourrait en réalité saper l'efficacité de l'échange des données, étant donné que les autorités policières ne seraient pas en mesure de déterminer si les données doivent être considérées comme des «preuves», des «faits», des «renseignements vérifiés» ou des «renseignements non vérifiés». La personne concernée pourrait être affectée de façon disproportionnée par l'éventuel manque de précision des données relatives aux soupçons pesant à son encontre.

357. Toutefois, à la lumière des observations qui précèdent, le CEPD considère que cette disposition doit être renforcée et rendue obligatoire en supprimant le libellé «dans la mesure du possible». Comme expliqué ci-dessus, (voir la partie III.4.b sur les catégories de personnes concernées), les autorités répressives doivent avoir un avis *prima facie* sur le niveau de fiabilité des données et cette appréciation de la fiabilité est un élément indispensable de leur traitement.

358. Le CEPD recommande dès lors la suppression du libellé «dans la mesure du possible» aux paragraphes 1 et 2 de l'article 6 de la proposition de directive.

III.4.d. Traitement de catégories particulières de données (article 8)

359. Le CEPD accueille favorablement les dispositions spécifiques, dans la proposition de directive, sur le traitement des catégories particulières de données. Toutefois, dans sa forme actuelle, l'article 8 ne donne aucune indication sur la façon dont ces données doivent être traitées avec un soin particulier dans le cadre des exceptions. L'article 8,

paragraphe 2, point a), déclare seulement, de façon très large, que l'interdiction relative au traitement de ces données ne s'applique pas si le traitement «est autorisé par une législation prévoyant des garanties appropriées». Le considérant 26 explique que le traitement est uniquement permis s'il est «spécifiquement autorisé par une loi prévoyant des mesures appropriées de sauvegarde des intérêts légitimes de la personne concernée».

360. Le CEPD recommande que le législateur inclue le libellé plus restrictif du considérant à l'article 8 lui-même et précise en outre à l'article 8 et aux considérants ce qui est visé par des mesures adéquates qui vont au-delà des garanties ordinaires s'appliquant à tout type de traitement des données.

III.5. Droits des personnes concernées (chapitre III)

361. Le chapitre III de la proposition de directive traite des droits de la personne concernée en matière d'information, d'accès, de rectification et d'effacement, d'une manière qui est généralement cohérente avec l'actuelle législation en matière de protection des données et l'article 8 de la Charte. Le CEPD accueille favorablement ces dispositions étant donné qu'elles prévoient un ensemble harmonisé de droits pour les personnes concernées tout en tenant compte de la nature particulière du traitement par les autorités répressives et judiciaires. Toutefois, le CEPD considère que certaines améliorations sont encore nécessaires.

III.5.a. Transparence et informations à la personne concernée (articles 10 and 11)

362. Dans la partie II.5.a, le CEPD a déjà souligné que la transparence constitue un élément crucial de la protection des données, non seulement en raison de sa valeur intrinsèque mais aussi parce qu'elle permet l'exercice d'autres principes en matière de protection des données. Les personnes ne sont capables d'exercer leurs droits que si elles ont connaissance du traitement de leurs données. Cet aspect est d'autant plus important dans le domaine répressif, où l'utilisation des données à caractère personnel exerce inévitablement un impact énorme sur la vie et la liberté des personnes privées.

363. Le CEPD accueille dès lors favorablement l'obligation générale, faite aux responsables du traitement, de disposer de politiques transparentes et aisément accessibles sur les questions de protection des données et de communiquer avec la personne concernée sur ces questions, en utilisant un langage clair et simple (voir l'article 10, paragraphes 1 et 2, de la proposition de directive). En outre, le CEPD accueille favorablement la spécification très détaillée du type d'information qui doit être fournie par le responsable du traitement à la personne concernée lorsque ses données à caractère personnel sont collectées (voir l'article 11).

364. Toutefois, le CEPD déplore que cette obligation soit fortement affaiblie par l'ajout, à l'article 10, paragraphe 1, de la limitation selon laquelle le «responsable du traitement prend toutes les mesures raisonnables». Si les spécificités du secteur répressif peuvent exiger, dans une certaine mesure, une approche moins libérale de la transparence, la proposition de directive en tient déjà compte en prévoyant des exemptions spécifiques au droit à l'information à l'article 13 de la proposition de directive. Lorsque ces exemptions ne sont pas applicables, il n'y a pas de justification pour réduire davantage l'obligation à l'article 10.

365. Le CEPD recommande dès lors de supprimer la référence à «toutes les mesures raisonnables» au paragraphe 1 ainsi qu'au paragraphe 3 de l'article 10.

III.5.b. Modalités de l'exercice des droits de la personne concernée (article 10)

366. Contrairement à l'article 12, paragraphe 2, de la proposition de règlement, l'article 10, paragraphe 4, de la proposition de directive n'impose pas un délai au responsable du traitement pour informer la personne concernée en ce qui concerne sa demande. La notion de remplacement de «sans retard injustifié» à l'article 10, paragraphe 4, serait inefficace dans la pratique, étant donné qu'il n'y a pas de délai. Étant donné que la vie privée des personnes concernées peut être particulièrement affectée par la nature intrusive du contexte répressif et le niveau de sensibilité des données traitées, il est particulièrement nécessaire de leur donner une sécurité juridique lors de l'exercice de ces droits et certainement pas d'affaiblir leurs droits dans la pratique.

367. Le CEPD recommande dès lors que la proposition de directive intègre un délai explicite à l'article 10, paragraphe 4, et que ces informations soient communiquées dans un délai d'un mois au moins, à compter de la réception de la demande, conformément à la proposition de règlement.

368. En outre, si l'article 12, paragraphe 4, de la proposition de règlement fait référence à des demandes «au caractère manifestement excessif», l'article 10, paragraphe 5, de la proposition de directive utilise le mot «abusives». Par souci de clarté, le CEPD préférerait l'utilisation du libellé «au caractère manifestement excessif». En outre, le CEPD recommande de donner davantage d'indications sur cette notion dans un considérant.

369. Enfin, le CEPD recommande d'inclure, dans la proposition de directive, une disposition similaire à l'article 13 de la proposition de règlement mais avec un champ d'application élargi. Le responsable du traitement doit être tenu de communiquer à chaque destinataire auquel les données ont été divulguées toute rectification, tout effacement ou toute modification des données, effectués ou non conformément à l'article 15 ou 16 de la proposition de directive, à moins que cela ne s'avère impossible ou n'implique un effort disproportionné. Des obligations comparables figurent déjà dans des instruments existants de l'UE dans le domaine répressif[73].

III.5.c. Limitations aux droits de la personne concernée (articles 11, 13, 15 et 16)

370. Il ne fait nul doute que certaines limitations aux droits de la personne concernée peuvent être nécessaires dans le domaine répressif, étant donné que des informations sur les enquêtes pénales peuvent nuire à l'enquête elle-même. Toutefois, étant donné que ces limitations constituent des exceptions à un droit fondamental, elles ne doivent s'appliquer que dans la mesure du nécessaire et être proportionnées dans chaque cas. En outre, les exceptions doivent être limitées et bien définies et, si possible, partielles et limitées dans le temps. Par ailleurs, toute limitation aux droits de la personne concernée devrait s'accompagner des garanties appropriées.

371. Les articles 11, paragraphe 4, et 13 énoncent les dérogations permettant une limitation partielle ou complète de l'obligation de transparence et du droit d'accès lorsqu'elles

[73] Voir, par exemple, l'article 16 de la décision du Conseil 2009/934/JAI du 30 novembre 2009 portant adoption des règles d'application régissant les relations d'Europol avec ses partenaires, notamment l'échange de données à caractère personnel et d'informations classifiées, JO L 325, 11.12.2009, p. 6. Voir également le principe 5, paragraphe 5, ii, de la recommandation du Conseil de l'Europe n° R(87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

constituent une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des intérêts légitimes de la personne concernée. Le CEPD accueille favorablement le fait que la proposition de directive harmonise les motifs et les conditions des éventuelles dérogations[74].

372. Toutefois, contrairement aux dispositions sur la transparence et le droit d'accès, les motifs et les conditions pour limiter le droit à la rectification (article 15) et le droit à l'effacement (article 16) ne sont pas mentionnés dans la proposition de directive. Dans les deux dispositions, il est uniquement mentionné que le responsable du traitement informe la personne concernée des motifs du refus, et des possibilités de s'adresser à l'autorité de contrôle ou de former un recours juridictionnel. Le CEPD recommande que les motifs et les conditions pour limiter ces deux droits soient également mentionnés.

373. En ce qui concerne les dispositions nationales, l'article 11, paragraphe 8, et l'article 13, paragraphe 2, prévoient que vu la nature spécifique du traitement de certaines catégories de données, les États membres peuvent déterminer des catégories de traitements de données susceptibles de faire l'objet, dans leur intégralité ou en partie, de dérogations. Toutefois, cela ne doit être permis que pour des situations limitées, dans lesquelles cette exemption catégorique est dûment justifiée[75]. Cela implique qu'il doit être évident que les motifs légitimes pour une exemption s'appliquent à toutes les données pertinentes dans toutes les circonstances. En principe, toute limitation partielle ou complète du droit d'information et/ou d'accès doit être soigneusement examinée par le responsable du traitement, au cas par cas, en relation avec le motif invoqué pour cette limitation.

374. Le CEPD recommande, afin de garantir le caractère exceptionnel de cette dérogation, d'ajouter une phrase à l'article 11, paragraphe 4, et à l'article 13, paragraphe 1, déclarant que le responsable du traitement doit être tenu de vérifier chaque cas spécifique, au moyen d'un examen concret et individuel afin de déterminer si des restrictions partielles ou complètes pour l'un des motifs s'appliquent.

375. En outre, une interprétation limitée du champ d'application de l'article 11, paragraphe 8, et de l'article 13, paragraphe 2, doit être assurée par un amendement apporté aux dispositions elles-mêmes.

376. Enfin, le CEPD recommande la suppression du mot «non-fourniture» à l'article 11, paragraphe 4, et au considérant 33, dans la mesure où il n'a pas de valeur ajoutée.

III.5.d. Garanties supplémentaires (articles 14 and 45, paragraphe 1, point c))

377. La proposition de directive contient plusieurs obligations et garanties supplémentaires qui accompagnent la limitation des droits exposée aux articles 13, 15 et 16, en prévoyant notamment une intervention par une autorité de contrôle.

378. Par exemple, en refusant ou en limitant l'accès, la rectification ou l'effacement, le responsable du traitement est tenu d'informer la personne concernée de la possibilité d'introduire une plainte auprès de l'autorité de contrôle et de former un recours juridictionnel (voir les articles 13, paragraphe 3, 15, paragraphe 2, et 16, paragraphe 4,).

[74] Les limitations aux droits de la personne concernée sont autorisées par des dispositions identiques en ce qui concerne tant le droit à l'information que le droit d'accès.

[75] L'article 109 de la convention de Schengen pourrait servir d'illustration. Conformément à cette disposition, les signalements aux fins de surveillance discrète ne sont dans tous les cas pas communiqués à la personne concernée.

En outre, conformément à l'article 14, la personne concernée a le droit de demander que l'autorité de contrôle vérifie la licéité du traitement.

379. Le CEPD accueille favorablement ces garanties supplémentaires concernant l'autorité de contrôle. Toutefois, leur efficacité est limitée au motif que ces autorités n'ont pas le pouvoir, en vertu de la proposition de directive d'ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes relatives aux droits des personnes concernées.

380. Le CEPD recommande dès lors d'ajouter ce pouvoir, ainsi qu'il sera discuté plus amplement dans la partie III.8.a du présent avis.

III.5.e. Droit à l'effacement (article 16)

381. Le CEPD note que le responsable du traitement peut, dans certains cas spécifiques, marquer les données au lieu de les supprimer. L'esprit de cette disposition est le même que celui de l'article 17, paragraphes 4 et 5, de la proposition de règlement. Toutefois, la proposition de règlement prévoit une possibilité de «limiter» le traitement lorsque les données ne sont pas supprimées, tandis que la proposition de directive prévoit simplement le «marquage» des données.

382. Par souci de cohérence et de clarté du concept de limitation du traitement dans les deux propositions, le CEPD recommande l'utilisation, à l'article 16, paragraphe 3, du libellé «limite le traitement» au lieu de «marque». Il recommande également de développer davantage la définition à l'article 3, paragraphe 4, de la proposition de directive, dans le sens de l'article 17, paragraphe 8, de la proposition de règlement. Comme déjà mentionné dans la partie II.3.c, nous recommandons au législateur d'inclure également la définition de «limitation du traitement» dans le règlement.

383. En outre, il recommande d'ajouter, à l'article 16 de la proposition de directive, l'obligation pour le responsable du traitement d'informer la personne concernée avant de lever toute limitation sur le traitement. Il n'y a aucune raison pour que la proposition de directive s'écarte des normes de l'article 17, paragraphe 6, de la proposition de règlement à cet égard.

III.6. Responsable du traitement and sous-traitant (chapitre IV)

384. Dans la partie II.6 de son avis, le CEPD a exprimé sa satisfaction à l'égard des importantes améliorations proposées en ce qui concerne les règles pour les responsables du traitement et les sous-traitants, telles que prévues par le chapitre IV du règlement. Toutefois, le CEPD est moins positif en ce qui concerne la façon dont les règles pour les responsables du traitement et les sous-traitants ont été élaborées au chapitre IV de la proposition de directive.

385. Le CEPD croit comprendre que certaines dispositions de la proposition de règlement ont été adaptées afin de tenir compte de la nature spécifique de l'instrument juridique (une directive) et de la nature spécifique du traitement dans le domaine de la coopération policière et judiciaire en matière pénale. Toutefois, les écarts par rapport aux règles générales dans l'actuelle proposition vont beaucoup trop loin. Par exemple, il n'y a absolument aucune justification à la suppression de l'analyse d'impact relative à la protection des données et à la simplification drastique d'autres dispositions, telles que celles concernant le délégué à la protection des données.

386. Ces différences sapent de façon significative l'objectif d'un cadre solide, cohérent et global relatif à la protection des données, énoncé par la Commission dans sa communication. Ainsi qu'il sera exposé plus en détail ci-dessous, le CEPD recommande dès lors d'aligner la proposition de directive sur les dispositions pertinentes de la proposition de règlement.

III.6.a. Protection des données dès la conception et protection des données par défaut (article 19)

387. Le CEPD note que l'article 19 est une version très simplifiée de la disposition sur la protection des données dès la conception et par défaut, prévue à l'article 23 de la proposition de règlement.

388. En particulier, l'article 19, paragraphe 1, ne fait pas référence au moment où les mesures et procédures pour la mise en œuvre des deux principes doivent être mises en vigueur. De même, l'article 19, paragraphe 2, déclare simplement que «le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules les données à caractère personnel nécessaires aux finalités du traitement seront traitées».

389. Le CEPD recommande que les recommandations ci-dessus, sur l'article 23 de la proposition de règlement, pour étayer davantage la notion de protection des données «par défaut» (voir la partie II.6.b), soient également prises en considération pour la proposition de directive.

III.6.b. Documentation et établissement de relevés des opérations de traitement (article 23)

390. Conformément à l'article 23, paragraphe 1, les responsables du traitement et les sous-traitants sont tenus de conserver une trace documentaire de tous les systèmes et procédures de traitement sous leur responsabilité. La liste des informations est fournie à l'article 23, paragraphe 2, tandis que l'article 23, paragraphe 3, établit que la documentation doit être mise à la disposition de l'autorité de contrôle, à la demande de celle-ci.

391. Comme mentionné, l'exigence relative à la documentation découle de l'obligation générale de pouvoir *démontrer* la conformité avec la directive. Tout comme pour la proposition de règlement, ce point doit être explicitement mentionné à l'article 4, point f), et à l'article 18 de la proposition de directive.

392. En outre, étant donné la nature spécifique du traitement couvert par la directive, l'article 24 établit que les relevés des principales opérations de traitement effectuées doivent être utilisés à des fins de vérification de la licéité du traitement des données, d'autocontrôle et de garantie de l'intégrité et de la sécurité des données.

393. Il y a lieu de noter que la liste à l'article 23, paragraphe 2, est moins détaillée que la liste comparable à l'article 28, paragraphe 2, de la proposition de règlement. Les observations formulées ci-dessus, dans la partie II.6.e, ne s'appliquent dès lors pas totalement en l'espèce. Il serait néanmoins souhaitable de mieux aligner les deux dispositions à la lumière de ces observations avant leur adoption finale. Cela concerne notamment le nom et les coordonnées du délégué à la protection des données, ainsi que les mécanismes mis en œuvre afin de vérifier l'efficacité des mesures mises en place pour garantir la conformité.

394. En outre, l'obligation de mettre la documentation à la disposition de l'autorité de contrôle devrait également être complétée d'une obligation supplémentaire d'informer l'autorité de contrôle sur d'autres points pertinents, tels que les catégories de personnes concernées et les catégories des données à caractère personnel, ainsi qu'une indication générale des délais pour l'effacement.

395. En outre, les informations à conserver sur les transferts vers des pays tiers sont trop limitées (voir l'article 23, paragraphe 2, point d)). En ce qui concerne les transferts vers les pays tiers, le CEPD recommande en outre d'inclure l'exigence de conserver les informations sur le motif légal pour lequel les données sont transférées, avec des explications substantielles, notamment si un transfert est fondé sur l'article 35 ou 36.

396. L'article 24 traite de l'établissement des relevés des opérations de traitement. Le CEPD accueille favorablement cette disposition et recommande d'inclure spécifiquement l'identité des destinataires des données. En outre, le CEPD recommande de disposer, à l'article 24, tout comme à l'article 23, que l'autorité de contrôle a accès à ces informations à sa demande.

III.6.c. Sécurité des données (articles 27 à 29)

397. Le CEPD est heureux de constater que l'obligation de notifier une violation des données à caractère personnel à l'autorité de contrôle et à la personne concernée est également proposée dans la directive.

III.6.d. Analyse d'impact relative à la protection des données

398. Dans ses observations sur la proposition de règlement, le CEPD accueille favorablement l'introduction du principe d'une analyse d'impact relative à la protection des données à l'article 33 de la proposition de règlement étant donné qu'elle constitue un mécanisme important pour assurer la responsabilité du responsable du traitement (voir la partie II.6.h). En outre, elle contribue à la mise en œuvre pratique des principes de «protection des données dès la conception» et de «protection des données par défaut».

399. L'analyse d'impact relative à la protection des données n'apparaît pas du tout dans la proposition de directive. Il n'y a pas non plus de disposition pour une analyse d'impact préliminaire lorsque des données biométriques sont traitées, comme suggéré par le Conseil[76]. Si cette omission est fondée sur l'idée que les autorités publiques sont exemptées de l'analyse d'impact relative à la protection des données obligatoire dans le cadre du règlement, le CEPD souhaiterait rappeler l'observation formulée dans la partie II.6.h ci-dessus, selon laquelle la dérogation ne doit s'appliquer que si une évaluation spécifique, égale à une analyse d'impact relative à la protection des données, a déjà été effectuée durant le processus législatif.

400. Le CEPD ne voit pas de justification au fait que l'analyse d'impact relative à la protection des données ne doive pas être incluse dans la proposition de directive, accompagnée de la clause d'exception discutée ci-dessus. La nature spécifique des opérations de traitement effectuées par les autorités répressives rend d'autant plus nécessaire la réalisation de ces analyses d'impact.

[76] Voir les conclusions du Conseil de la 3071e session du Conseil Justice et affaires intérieures des 24 et 25 février 2011.

401. Le CEPD invite dès lors le législateur à insérer, dans la proposition de directive, une disposition exigeant des autorités compétentes qu'elles procèdent à une AIPD, à moins qu'une analyse spécifique, équivalente à une AIPD, ait déjà été réalisée durant le processus législatif.

III.6.e. Consultation préalable (article 26)

402. Aux termes de l'article 26, paragraphe 1, les États membres veillent à ce que le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle avant le traitement de données à caractère personnel qui feront partie d'un nouveau fichier à créer si le traitement vise des catégories particulières de données et si l'utilisation des technologies, des mécanismes ou des procédures est susceptible de présenter des risques spécifiques. Conformément à l'article 26, paragraphe 2, les États membres peuvent prévoir que l'autorité de contrôle établit une liste des traitements devant faire l'objet d'une consultation préalable conformément au paragraphe 1.

403. Le CEPD considère que le champ d'application de la procédure de consultation est trop limité et recommande d'aligner plus étroitement la disposition sur les procédures développées à l'article 34, paragraphe 2, de la proposition de règlement. Ces procédures sont fondées sur l'existence de l'analyse d'impact relative à la protection des données. Si la proposition de directive demeure telle qu'elle se présente actuellement, l'absence de toute analyse d'impact relative à la protection des données rendrait très difficile l'identification des risques potentiels pour les droits fondamentaux et la liberté des personnes concernées.

404. Dans ces circonstances, le responsable du traitement ou le sous-traitant devrait être obligé de consulter systématiquement l'autorité de contrôle lorsqu'une nouvelle opération de traitement est introduite dans un système de fichiers existant. Ce n'est que si l'obligation d'une analyse d'impact relative à la protection des données est introduite dans la proposition de directive que le champ d'application de la procédure de consultation pourrait être limité aux cas présentant des risques spécifiques, étant donné qu'il y aurait alors une garantie réelle que ces risques seraient détectés au préalable.

III.6.f. Délégué à la protection des données

405. Le CEPD a souligné, dans le contexte de la proposition de règlement, l'importance de la fonction de délégué à la protection des données pour veiller à la conformité, au niveau interne, des règles relatives à la protection des données. Il soutient dès lors vivement l'introduction, à l'article 30, paragraphe 1, de la proposition de directive, d'une disposition prévoyant l'obligation pour le responsable du traitement ou le sous-traitant de nommer un délégué à la protection des données.

406. Le CEPD déplore que la proposition n'ait pas établi certaines exigences fondamentales pour la désignation et la position du délégué à la protection des données. Le CEPD recommande dès lors que la proposition soit alignée sur la proposition de règlement et prévoie des garanties supplémentaires: premièrement, l'article 30 doit traiter de la question du conflit d'intérêts et établir un mandat minimum de deux ans et, ensuite, l'article 31 doit prévoir un rattachement administratif approprié en tenant dûment compte du rôle indépendant du délégué à la protection des données et en vue notamment d'éviter d'éventuelles relations inégales ou d'influence par des responsables du traitement de haut rang.

III.7. Transferts vers les pays tiers (chapitre V)

407. Dans un monde de plus en plus interconnecté, une coopération policière et judiciaire efficace à l'intérieur des frontières de l'UE dépend de plus en plus de la coopération avec les pays tiers et les organisations internationales. Le développement de cette coopération internationale étant susceptible de dépendre fortement des échanges des données à caractère personnel, il est d'autant plus important pour l'Union de développer ces échanges dans le plein respect des droits de l'homme, y compris la protection des données.

III.7.a. Principes généraux applicables aux transferts (article 33)

408. Conformément à l'article 33, les transferts des données à caractère personnel vers un pays tiers ou une organisation internationale, y compris le transfert ultérieur vers un autre pays ou une autre organisation internationale, peuvent avoir lieu lorsque le transfert est nécessaire à des fins répressives, dans les conditions exposées au chapitre V de la proposition de directive.

409. Les instruments juridiques existants dans le domaine de la coopération policière et judiciaire exigent que le responsable du traitement dans le pays tiers ou l'organisation internationale soit une autorité compétente aux fins répressives[77]. L'article 33 de la proposition de directive n'inclut pas cette exigence, qui n'est mentionné qu'à son considérant 45. Cela n'est manifestement pas suffisant. Le CEPD s'oppose vivement à toute possibilité de transfert et de traitement ultérieur des données à caractère personnel par des pays tiers hors du cadre fixé par la directive.

410. Le CEPD recommande dès lors vivement de compléter l'article 33 de la proposition de directive par une exigence selon laquelle le transfert ne pourra avoir lieu que si le responsable du traitement dans le pays tiers ou l'organisation internationale est une autorité compétente au sens de la proposition de directive.

III.7.b. Transferts assortis d'une décision constatant le caractère adéquat du niveau de protection (article 34)

411. En règle générale, un transfert peut avoir lieu lorsque la Commission, sur la base de l'article 41 de la proposition de règlement ou de l'article 34 de la proposition de directive, a décidé que le pays tiers ou l'organisation internationale offre un niveau de protection adéquat. Le principe du «niveau de protection adéquat» est consacré dans le protocole additionnel à la Convention 108[78]. Ce principe a également été mis en œuvre et spécifié dans plusieurs instruments juridiques de l'Union européenne, non seulement dans la directive 95/46/CE, mais aussi dans des instruments juridiques dans le domaine de la coopération policière et judiciaire, tels que les instruments juridiques établissant Europol et Eurojust. Le CEPD accueille favorablement cette référence aux décisions constatant le caractère adéquat à l'article 34 de la proposition de directive et le mécanisme connexe.

[77] Voir l'article 17, paragraphe 1, de la décision du Conseil 2009/934/JAI, citée à la note de bas de page 73, et l'article 13, paragraphe 1, point b), sur la décision-cadre du Conseil 2008/977/JAI.

[78] Le protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données énonce le principe général — assorti de certaines dérogations — selon lequel le transfert de données à caractère personnel n'est autorisé que si cette partie «assure un niveau de protection adéquat pour le transfert considéré».

III.7.c. Transferts non assortis d'une décision constatant le caractère adéquat (articles 35 et 36)

412. En l'absence de décision de la Commission constatant le caractère adéquat, des transferts peuvent avoir lieu lorsque i) des garanties appropriées ont été offertes dans un instrument juridiquement contraignant ou ii) le responsable du traitement a conclu, après avoir évalué toutes les circonstances entourant le transfert des données à caractère personnel, qu'il existe des garanties appropriées (article 35).

413. Toutefois, une évaluation par le seul responsable du traitement ne peut être considérée comme une garantie appropriée et suffisante pour autoriser les transferts vers un pays tiers ou une organisation internationale sur une base systématique ou structurelle, étant donné qu'elle n'offre manifestement pas une protection suffisante pour les personnes concernées.

414. Le CEPD note également que, hormis l'exigence d'une documentation spécifique – qui est une garantie supplémentaire, mais insuffisante en soi -, la proposition de directive ne prévoit aucune garantie pour ces transferts. Par contre, l'article 42, paragraphe 8, de la proposition de règlement prévoit, en pareils cas, une autorisation de l'autorité de contrôle.

415. Le CEPD recommande dès lors vivement la suppression de l'article 35, paragraphe 1, point b), ou, à tout le moins, l'ajout de l'exigence d'une autorisation préalable de l'autorité de contrôle.

416. Lorsqu'il n'y a ni décision constatant le caractère adéquat, ni garanties appropriées en vertu de l'article 35, un transfert peut encore avoir lieu en vertu de l'article 36 lorsqu'il est nécessaire i) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne, ii) à la sauvegarde des intérêts légitimes de la personne concernée, iii) pour prévenir une menace grave et immédiate pour la sécurité publique, iv) dans des cas particuliers, à des fins répressives et v) dans des cas particuliers, à la constatation, à l'exercice ou à la défense d'un droit en justice lié à des finalités répressives

417. Le CEPD souligne que toute dérogation utilisée pour justifier un transfert doit être interprétée de manière restrictive et ne doit pas permettre un transfert fréquent, massif et structurel des données à caractère personnel. Si l'article 36, points d) et e), prévoit que la dérogation s'applique à des cas individuels, il doit être clair que même un cas individuel ne doit pas permettre des transferts massifs de données et doit être limité aux données strictement nécessaires. Ceci s'applique également à tout transfert justifié par une menace grave pour la sécurité publique, comme mentionné à l'article 36, point c). Le CEPD recommande que ce point soit précisé dans un considérant.

418. En outre, le CEPD recommande que des garanties supplémentaires telles qu'une obligation de documenter spécifiquement ces transferts (par exemple, les données transférées, le moment du transfert, les données concernant le destinataire, le motif du transfert et le destinataire, etc.) soient ajoutées à l'article 36.

III.7.d. Transferts assortis d'une décision constatant le caractère inadéquat

419. Les conditions permettant un transfert vers un pays tiers ou une organisation internationale qui n'offre pas un niveau de protection adéquat ne sont pas claires. En effet, si l'article 34, paragraphe 6, et le considérant 48 de la proposition de directive permettent des transferts vers ces pays ou organisations lorsqu'ils sont fondés sur des garanties appropriées (article 35) ou des dérogations (article 36), l'article 35, paragraphe 1, qui traite des garanties appropriées, fait référence à des situations où la Commission n'a pas rendu de décision.

420. Une observation similaire a été formulée dans la partie II.7.b en ce qui concerne le règlement. Le CEPD suggère dès lors que l'article 35, paragraphe 1, soit modifié pour assurer la cohérence entre ces dispositions. Néanmoins, lorsqu'il existe une décision constatant le caractère inadéquat, les possibilités de continuer à transférer des données à caractère personnel doivent être très limitées dans ce domaine particulier. Le CEPD recommande que tout transfert dans cette situation soit dès lors uniquement fondé sur:
    - l'article 35, paragraphe 1, point a), s'il existe un accord international juridiquement contraignant autorisant le transfert sous certaines conditions spécifiques garantissant une protection adéquate,
    - l'article 36, point a) ou c), à savoir pour la sauvegarde des intérêts vitaux de la personne concernée ou en cas de menace grave et immédiate pour la sécurité publique.

III.8. Mécanismes de contrôle (chapitres VI, VII et VIII)

421. Le CEPD note que les dispositions sur les mécanismes de contrôle par des autorités de contrôle indépendantes, ainsi que les mécanismes de coopération entre ces autorités, diffèrent à certains égards des dispositions correspondantes dans la proposition de règlement.

422. Dans cette partie, le CEPD analysera ces différences, leur justification ainsi que les conséquences éventuelles pour l'organisation des autorités de contrôle. Dans la plupart des États membres, les mêmes autorités auront vraisemblablement été affectées au contrôle du règlement ainsi qu'aux dispositions législatives nationales transposant la directive.

III.8.a. Pouvoirs des autorités de contrôle

423. Selon le CEPD, dans le cadre d'une approche globale, il n'est pas nécessaire de différencier les pouvoirs des autorités de contrôle entre le règlement et la directive. En effet, la proposition de règlement prévoit également le contrôle des autorités publiques par des autorités de contrôle.

424. En ce qui concerne le champ d'application, les autorités compétentes auxquelles la proposition de directive est supposée s'appliquer en vertu de son article 1, paragraphe 1, sont, d'une part, les autorités policières au sens de l'article 87, paragraphe 1, TFUE, et, d'autre part, les autorités judiciaires. Selon le CEPD, une distinction pourrait se justifier dans une certaine mesure entre le contrôle de la police par des autorités de contrôle et le contrôle du pouvoir judiciaire par des autorités de contrôle. Dans le cas de la police, des spécificités ne sont pas nécessaires; au contraire, au vu des pouvoirs de la police, un contrôle fort pourrait être encore plus important que dans d'autres branches du gouvernement.

425. Si les personnes concernées ont besoin d'une pleine protection dans le domaine judiciaire également, en vertu de la primauté du droit, certaines activités du pouvoir judiciaire peuvent être (partiellement) exemptées d'une supervision par d'autres organismes publics tels que des autorités de contrôle. Ce point est reconnu par l'article 51, paragraphe 3, de la proposition de règlement et l'article 44, paragraphe 2, de la proposition de directive en ce qui concerne les tribunaux dans l'exercice de leurs fonctions juridictionnelles.

426. Le CEPD recommande de donner davantage d'orientations, dans un considérant, sur ce qui est destiné à être couvert par «l'exercice des fonctions juridictionnelles». Il croit comprendre que l'exception s'adresse plus particulièrement au traitement des données à caractère personnel dans les procédures judiciaires sur des affaires individuelles. Par ailleurs, les principes de protection des données – y compris le contrôle – doivent rester applicables, par exemple, au traitement des données à caractère personnel par l'enregistrement, la publication de rapports publics de procédures et la publication de décisions judiciaires.

427. Si une certaine exception limitée[79] se justifie en ce qui concerne les tribunaux dans l'exercice de leurs fonctions juridictionnelles, le CEPD ne voit aucune raison de limiter les pouvoirs des autorités de contrôle en dehors de ce contexte spécifique. Le CEPD recommande dès lors que les pouvoirs des autorités de contrôle vis-à-vis des autorités policières nationales soient pleinement alignés sur les pouvoirs visés dans le cadre de la proposition de règlement.

428. Toutefois, la différence la plus évidente entre la proposition de règlement et la proposition de directive ne concerne pas le champ d'application mais le contenu des pouvoirs des autorités de contrôle. Si l'article 53 de la proposition de règlement énumère une longue liste de pouvoirs, l'article 46 de la proposition de directive est plus limité. Plusieurs pouvoirs des autorités de contrôle ont été supprimés sans justification, par rapport à la proposition de règlement. Le CEPD fait notamment référence au pouvoir des autorités de contrôle d'ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes relatives aux droits des personnes concernées et au pouvoir de suspension des flux de données vers un destinataire dans un pays tiers ou une organisation internationale[80]. En outre, le pouvoir d'obtenir du responsable du traitement ou du sous-traitant un accès à toutes les données à caractère personnel ou à l'un de ses locaux a été substantiellement réduit et remplacé par le pouvoir de «collecter toutes les informations nécessaires»[81].

429. Le CEPD recommande la mise en équation du libellé de l'article 46, point a), avec le libellé de l'article 53 de la proposition de règlement.

430. Comme mentionné, le CEPD ne voit aucun élément qui justifierait une différenciation entre le règlement et la directive en ce qui concerne les pouvoirs des autorités de contrôle. Toutefois, il reconnaît que les pouvoirs effectifs, en vertu de l'article 46,

[79] Le champ d'application et la finalité de cette exception demeurent problématiques. Il existe un éventail de pratiques parmi les États membres, bien que la plupart des déclarations des parties contractantes à la convention 108 ne mentionnent pas l'exception. Dans la mesure où les autorités nationales en charge de la protection des données sont concernées, elles semblent trouver des solutions satisfaisantes dans la pratique. Une plus ample réflexion sur le sujet est dès lors nécessaire.

[80] Voir l'article 53, paragraphe 1, points b) et h), de la proposition de règlement.

[81] Comparer l'article 53, paragraphe 2, de la proposition de règlement avec l'article 46, point a), de la proposition de directive.

point b), de la proposition de directive sont potentiellement forts, à condition de veiller à ce que tous les États membres *doivent* doter les autorités de contrôle sur leurs territoires de *tous* les pouvoirs énoncés. Il conseille dès lors, en tant qu'option minimale, de remplacer le libellé «tels que» à l'article 46, points a) et b), par «y compris».

431. Le CEPD note également une différence importante concernant le rapport annuel sur l'activité des autorités de contrôle. Conformément à l'article 54 de la proposition de règlement, ce rapport doit non seulement être mis à la disposition de la Commission et du comité européen de protection des données, mais aussi être présenté au parlement national et rendu public. L'article 47 de la proposition de directive mentionne seulement que le rapport est mis à la disposition de la Commission et du comité. Le CEPD ne voit aucune justification à cette différence, du moins en ce qui concerne le parlement national. À cet égard, la Cour de justice, dans l'arrêt *Commission/Allemagne*, mentionne explicitement la présentation de rapports par l'autorité de contrôle au parlement national comme un outil de conformité au principe de démocratie[82].

III.8.b. Coopération et cohérence

432. La proposition de règlement prévoit un régime élaboré pour une assistance mutuelle entre les autorités de contrôle et encourage également les opérations conjointes. Les dispositions de la directive sont beaucoup plus limitées. Il existe bien sûr des raisons en faveur d'une approche plus limitée dans la directive, ne serait-ce que des raisons de souveraineté nationale. Il serait difficile d'imaginer que les membres du personnel d'une autorité de contrôle dans un État membre mènent des enquêtes dans les locaux de la police d'autres États membres.

433. Toutefois, la proposition de directive reconnaît qu'une étroite coopération entre les autorités de contrôle est logique dans le domaine de la coopération policière et judiciaire. Le considérant 58 rappelle qu'une application cohérente doit être assurée par un mécanisme d'assistance (mutuelle) des autorités de contrôle. La croissance exponentielle des échanges d'informations entre les autorités policières et judiciaires nationales exige des approches harmonisées ainsi que des garanties que les mesures d'application des autorités de contrôle dans un État membre ne seront pas contournées si des mesures appropriées ne sont pas prises dans les autres États membres où les mêmes données sont disponibles. Enfin, une étroite coopération des autorités de contrôle pourrait faciliter l'utilisation des données à caractère personnel dans les procédures judiciaires avec un élément transfrontalier.

434. De façon plus générale, le CEPD n'est pas convaincu que des dispositions spécifiques en matière d'assistance mutuelle, aux termes de la proposition de règlement, ne puissent être incluses dans la proposition de directive. Par exemple, l'article 55 de la proposition de règlement contient plusieurs dispositions détaillées visant à garantir une coopération rapide, efficace et obligatoire entre les autorités de contrôle.

435. Le CEPD recommande dès lors d'inclure, en tout état de cause, les dispositions de l'article 55, paragraphes 2 à 7, dans la proposition de directive.

[82] Voir l'arrêt *Commission/Allemagne* de la CJUE, cité à la note de bas de page 50, point 55. Voir également l'arrêt de la CJUE du 20 mai 2003, *Österreichischer Rundfunk*, C-465/00, C-138/01 et C-139/01, Recueil 2003, p. I-4989, dans lequel la Cour a donné une orientation sur la proportionnalité concernant la question de savoir si les données salariales doivent être communiquées au public ainsi qu'au Parlement.

436. Il n'est pas convaincu non plus qu'un mécanisme spécifique de coopération renforcée, inspiré du mécanisme de contrôle de la cohérence prévu aux articles 57 à 63 de la proposition de règlement ne puisse être inclus dans la directive, éventuellement avec des missions plus limitées. La création de ce mécanisme vise notamment à garantir que le droit de l'UE en matière de protection des données soit interprété de façon uniforme sur tout le territoire de l'Union, afin d'assurer à tous les résidents de l'UE une protection égale de leur droit fondamental, dans les affaires présentant des éléments transfrontaliers. Cette raison s'applique pleinement au domaine de la coopération policière et judiciaire en matière pénale.

437. Si, par exemple, des données à caractère personnel d'une personne spécifique sont échangées entre les autorités compétentes dans différents États membres, ce ne serait pas utile si cette personne ne pouvait pas bénéficier du même niveau de protection dans l'État expéditeur et l'État destinataire.

438. Le CEPD conseille au législateur de réexaminer la nécessité d'un mécanisme de coopération accrue, dans le champ d'application de la proposition de directive également.

CHAPITRE IV - CONCLUSIONS ET RECOMMANDATIONS

439. Le CEPD accueille favorablement la proposition de règlement car elle constitue un grand pas en avant pour le droit à la protection des données en Europe. Les règles proposées renforceront les droits des individus et responsabiliseront davantage les responsables du traitement quant à la manière de traiter les données personnelles. En outre, le rôle et les pouvoirs des autorités nationales de contrôle (séparément et conjointement) se verront réellement renforcés.

440. Le CEPD est particulièrement heureux de voir que l'instrument proposé est un *règlement* pour les règles générales sur la protection des données. La proposition de règlement sera directement applicable dans les États membres et mettra fin à de nombreuses complexités et incohérences découlant des différentes mesures d'exécution des États membres actuellement en place.

441. Le CEPD est cependant extrêmement déçu par la proposition de directive pour la protection des données en matière pénale. Le CEPD regrette que la Commission ait choisi de réglementer la question dans un instrument autonome qui offre un niveau de protection inadéquat, très inférieur à la proposition de règlement.

442. Un élément positif de la proposition de directive est le fait qu'elle couvre le traitement national et a dès lors un champ d'application plus large que l'actuelle décision-cadre. Toutefois, cet élargissement n'offre de plus-value que si la directive renforce substantiellement le niveau de protection des données dans ce domaine, ce qui n'est pas le cas.

443. La principale faiblesse de l'ensemble du paquet tient au fait qu'il ne remédie pas à l'absence d'une approche globale des règles de l'UE en matière de protection des données. Il ne produit aucun effet sur de nombreux instruments de l'UE en matière de protection des données, tels que les règles de protection des données pour les institutions et organes de l'UE, mais aussi tous les instruments spécifiques adoptés dans le domaine de la coopération policière et judiciaire en matière pénale, tels que la décision de Prüm et les règles relatives à Europol et Eurojust. En outre, les deux instruments proposés

considérés conjointement ne traitent pas complètement des situations de fait qui relèvent des deux domaines de politique, telles que l'utilisation des données PNR ou de télécommunications à des fins répressives.

444. Dans le présent avis, le CEPD a exposé des observations et des recommandations détaillées sur les deux propositions législatives. Toutes les recommandations sont énumérées ci-dessous de façon concise.

En ce qui concerne l'ensemble du processus de réforme (partie I.2)

- Annoncer publiquement le calendrier portant sur la deuxième phase du processus de réforme dans les plus brefs délais;
- incorporer les règles pour les institutions et organes européens dans la proposition de règlement ou, à tout le moins, veiller à ce que les règles soient en adéquation avec, et entrent en vigueur lors de l'application de la proposition de règlement;
- présenter dans les plus brefs délais une proposition pour des règles communes pour la politique étrangère et de sécurité commune, fondées sur l'article 39 du traité UE.

Recommandations sur la proposition de règlement

Questions horizontales

- Ajouter une disposition clarifiant le champ d'application territorial du droit national en vertu du règlement;
- Reconsidérer la délégation de pouvoir aux articles 31, paragraphes 5 et 6, 32, paragraphes 5 et 6, 33 paragraphes 6 et 7, 34, paragraphe 2, point a) et 44, paragraphe 1, points 1 et 7;
- Prévoir des mesures appropriées et spécifiques pour les MPMEs uniquement dans des actes d'exécution et pas dans des actes délégués aux articles 8, paragraphe 3, 14, paragraphe 7, 22, paragraphe 4 et 33, paragraphe 6.
- Affiner la notion d' 'intérêt public' dans chaque disposition qui l'utilise. L'intérêt public spécifique devrait être clairement identifié en rapport avec le contexte du traitement envisagé dans chaque disposition pertinente de la proposition (voir en particulier le considérant 87, les articles 17, paragraphe 5, 44, paragraphe 1, point d) et 81, paragraphe 1, points b) et c). Des exigences supplémentaires pourraient inclure que le motif ne puisse être invoqué que dans des circonstances spécifiquement pressantes ou pour des raisons impérieuses prévues par la loi. peut seulement être invoqué

Chapitre I – Dispositions générales (partie II.3)

- Article 2, paragraphe 2, point d): insérer un critère pour différencier les activités publiques et domestiques fondé sur le nombre *indéfini* des personnes pouvant accéder aux informations.
- Article 2, paragraphe 2, point e): prévoir que l'exception s'applique aux autorités *publiques* compétentes. Le considérant 16 doit être rendu cohérent avec l'article 2, paragraphe 2, point e).
- Article 4, paragraphe 1, paragraphe 2: ajourer une explication plus claire dans un considérant, en insistant sur le fait que dès qu'il existe une relation étroite entre un identifiant et une personne, cela générera habituellement l'application des principes relatifs à la protection des données.
- Article 4, paragraphe 13: affiner les critères pour identifier l'établissement principal du responsable du traitement pertinent, en tenant compte de l'«influence dominante» d'un établissement sur d'autres, en lien étroit avec le pouvoir de mettre en œuvre les règles relatives à la protection des données à caractère personnel ou les règles pertinentes pour la

protection des données. À titre alternatif, la définition pourrait se concentrer sur l'établissement principal de l'ensemble du groupe.
- Ajouter de nouvelles définitions concernant le «transfert» et la «limitation du traitement».

Chapitre II –Principes fondamentaux (partie II.4)
- Article 6: ajouter un considérant pour préciser ce que recouvre une mission effectuée «dans l'intérêt général ou relevant de l'exercice de l'autorité publique» à l'article 6, paragraphe 1, point e).
- Article 6, paragraphe 4: supprimer la disposition ou, à tout le moins, limiter son champ d'application au traitement ultérieur des données pour des finalités incompatibles aux motifs contenus à l'article 6, paragraphe 1, point a) et à l'article 6, paragraphe 1, point d). Cela nécessiterait également une modification du considérant 40.
- Ajouter une nouvelle disposition sur la représentation de toutes les personnes ne disposant pas d'une capacité (juridique) suffisante ou qui ne sont pas autrement pas en mesure d'agir.
- Article 9: inclure les infractions et questions n'ayant pas donné lieu à des condamnations dans les catégories particulières de données. Étendre l'exigence de contrôle de l'autorité officielle à tous les motifs indiqués à l'article 9, paragraphe 2, point j).
- Article 10: rendre plus explicite, au considérant 45, le fait que le responsable du traitement des données ne doit pas être en mesure d'invoquer une éventuelle absence d'informations pour rejeter une demande d'accès, lorsque ces informations peuvent être fournies par la personne concernée pour permettre cet accès.

Chapitre III – Droits de la personne concernée (partie II.5)
- Article 14: inclure les informations sur l'existence de certaines opérations de traitement qui exercent un impact particulier sur les personnes ainsi que les conséquences de ce traitement sur les personnes.
- Article 17: développer davantage la disposition pour assurer son efficacité dans la réalité. Supprimer l'article 17, paragraphe 3, point d).
- Article 18: préciser que l'exercice du droit est sans préjudice de l'obligation visé à l'article 5, point e), lorsqu'elles ne sont plus nécessaires. Veiller à ce que l'article 18, paragraphe 2, ne soit pas seulement limité aux données qui ont été fournies par la personne concernée sur la base d'un consentement ou d'un contrat.
- Article 19: préciser ce que le responsable du traitement est supposé faire des données en cas de désaccord avec la personne concernée et mettre en équation avec l'article 17, paragraphe 1, point c). Expliquer dans un considérant ce qui peut être qualifié de «raisons impérieuses et légitimes».
- Article 20: inclure le droit des personnes de soumettre leur point de vue, à l'article 20, paragraphe 2, point a), tel qu'il est actuellement prévu à l'article 15 de la directive 95/46/CE.
- Article 21: introduire des garanties détaillées selon lesquelles le droit national doit spécifier les objectifs poursuivis par le traitement, les catégories de données à caractère personnel à traiter, les finalités et moyens spécifiques du traitement, le responsable du traitement, les catégories de personnes autorisées à traiter les données, la procédure à suivre pour le traitement et les garanties contre toute interférence arbitraire de la part des autorités publiques. Inclure en tant que garanties supplémentaires l'information des personnes concernées d'une limitation et de leur droit de saisir l'autorité de contrôle afin d'obtenir un accès indirect. Ajouter à l'article 21 que la possibilité d'appliquer des limitations au traitement effectué par des responsables du traitement privés à des fins répressives ne doit pas les forcer à conserver des données en plus de celles qui sont strictement nécessaires pour la finalité originale poursuivie, ni à modifier leur architecture informatique. Supprimer le motif contenu à l'article 21, paragraphe 1, point e).

Chapitre IV – Responsable du traitement et sous-traitant (partie II.6)

- Article 22: faire explicitement référence au principe de responsabilité, en tout état de cause au considérant 60. Fusionner l'article 22, paragraphes 1 et 3, et mentionner explicitement que les mesures doivent être *appropriées* et *efficaces*. Inclure une disposition générale précédant les obligations spécifiques à l'article 22, paragraphe 2, et développer davantage le concept du «contrôle de la gestion», en incluant la répartition des responsabilités, la formation du personnel et les instructions adéquates et en exigeant que le responsable du traitement ait au moins une vue d'ensemble et un inventaire général des opérations de traitement qui entrent dans le champ de ses responsabilités. Ajouter un nouveau paragraphe disposant que le responsable du traitement décide ou est obligé de publier un rapport régulier de ses activités. Ce rapport doit également contenir une description des politiques et mesures visées à l'article 22, paragraphe 1.
- Article 23: faire référence, à l'article 23, paragraphe 2, et au considérant 61, au fait que la personne concernée doit en principe avoir le choix d'autoriser une utilisation de ses données à caractère personnel de façon plus large.
- Article 25, paragraphe 2, point a): supprimer l'exception pour les pays tiers adéquats.
- Article 26: ajouter l'obligation pour le sous-traitant de tenir compte du principe de protection des données dès la conception dans la liste des spécifications contenues à l'article 26, paragraphe 2.
- Article 28: reconsidérer ou supprimer les dérogations de l'article 28, paragraphe 4.
- Article 30: préciser l'article 30 pour garantir la responsabilité globale du responsable du traitement et ajouter l'obligation pour le responsable du traitement d'adopter une approche de gestion de la sécurité des informations au sein de l'organisation, incluant, le cas échéant, la mise en œuvre d'une politique de sécurité des informations spécifique au traitement des données réalisé. Inclure une référence explicite à l'analyse d'impact relative à la protection des données à l'article 30.
- Articles 31 et 32: spécifier les critères et les exigences pour établir une violation des données et les circonstances dans lesquelles elle doit être notifiée. Modifier le délai de 24 heures à l'article 31 en le remplaçant par un délai de 72 heures au plus tard.
- Article 33: la liste des opérations de traitement contenue à l'article 33, paragraphe 2, points b), c) et d), ne doit pas se limiter au traitement à grande échelle. Aligner l'article 33, paragraphe 8, sur le considérant 73. Limiter l'article 33, paragraphe 6, aux éléments non essentiels. Préciser que la taille d'une entreprise ne devrait jamais supprimer l'obligation d'effectuer une analyse d'impact relative à la protection des données en ce qui concerne les opérations de traitement qui présentent des risques spécifiques.
- Article 34: déplacer l'article 34, paragraphe 1, au chapitre V de la proposition de règlement.
- Articles 35 à 37: abaisser le seuil de 250 salariés à l'article 35, paragraphe 1, et préciser le champ d'application de l'article 35, paragraphe 1, point c). Ajouter des garanties, notamment des conditions plus strictes pour le renvoi du délégué à la protection des données et veiller, à l'article 36, paragraphe 1, à ce que le délégué à la protection des données ait accès à toutes les informations pertinentes et aux locaux tels que nécessaires pour l'exécution de ses devoirs. Inclure à l'article 37, paragraphe 1, point a), le rôle du délégué à la protection des données en matière de sensibilisation.

Chapitre V – Transfert vers des pays tiers (partie II.7)

- Déclarer au considérant 79 que la non-applicabilité du règlement aux accords internationaux est limitée dans le temps et uniquement aux accords internationaux déjà existants.
- Insérer une clause transitoire prévoyant l'examen de ces accords internationaux dans un délai fixé afin de les mettre en équation avec le règlement.

- Article 41 (et considérant 82): préciser qu'en cas de décision constatant le caractère inadéquat, les transferts ne seraient permis que sous réserve de garanties appropriées ou en vertu des dérogations exposées à l'article 44.
- Article 42: veiller à ce que la possibilité de recourir à des instruments qui ne soient pas juridiquement contraignants pour offrir des garanties appropriées soit clairement justifiée et limitée uniquement aux cas où la nécessité de se fier à ce type de mesure non contraignante a été démontrée.
- Article 44 (et considérant 87): ajouter que la possibilité de transférer des données ne doit concerner que des transferts occasionnels et être fondée sur une analyse soigneuse de toutes les circonstances du transfert, au cas par cas. Remplacer ou préciser la référence aux «garanties appropriées» à l'article 44, paragraphe 1, point h), et à l'article 44, paragraphe 3.
- Considérant 90: modifier le considérant en une disposition de fond. Mettre en place des garanties appropriées, impliquant des garanties judiciaires ainsi que des garanties relatives à la protection des données.

Chapitres VI et VII – Autorités de contrôle indépendantes, coopération et cohérence (parties II.8 et II.9)

- Article 48: inclure un rôle pour les parlements nationaux dans la procédure de désignation des membres des autorités de contrôle.
- Article 52, paragraphe 1: inclure le devoir d'élaborer des lignes directrices sur l'utilisation des différents pouvoirs d'exécution, si nécessaire coordonnées au niveau de l'UE au sein du comité. Ce point pourrait éventuellement être inclus également à l'article 66.
- Article 58: remplacer le terme anglais «immediately» *[immédiatement]* à l'article 58, paragraphe 6, par «without delay» *[sans délai]* et étendre le délai d'un mois visé à l'article 58, paragraphe 7, à deux mois/huit semaines.
- Article 58: accorder plus de poids à la règle de la majorité en veillant à ce qu'une requête d'une autorité puisse être soumise au vote dans le cas où la question en jeu ne se rapporte pas à l'une des principales mesures décrites à l'article 58, paragraphe 2.
- Articles 59 et 60: limiter le pouvoir de la Commission en supprimant la possibilité d'annuler la décision d'une autorité de contrôle nationale sur une question spécifique en adoptant un acte d'exécution. Veiller à ce que le rôle de la Commission consiste, dans une phase initiale, en le pouvoir de saisir le comité, comme prévu à l'article 58, paragraphe 4, et, dans une phase ultérieure, le pouvoir d'adopter des avis. Insérer une référence à une procédure ultérieure devant la Cour de justice, dans le contexte d'une procédure d'infraction ou une demande de mesures provisoires telles qu'une ordonnance de suspension.
- Article 66: ajouter que le comité doit être consulté dans le contexte des analyses du caractère adéquat.
- Reconsidérer l'actuelle analyse d'impact du secrétariat du comité européen de protection des données en termes de ressources financières et humaines (voir l'annexe au présent avis, disponible sur le site web du CEPD).

Chapitre VIII – Recours, responsabilité et sanctions (partie II.10)

- Articles 73 et 76: préciser la nature du mandat que l'organisation doit obtenir des personnes concernées et le degré de formalité requis. Inclure une disposition plus large sur des actions collectives.
- Article 74, paragraphe 4: préciser le type de «préoccupation» d'une personne concernée qui pourrait déclencher la procédure et de la limiter à un risque plus précis d'impact sur les droits de la personne concernée.
- Article 75, paragraphe 2: spécifier que la dérogation ne s'applique pas à une autorité publique d'un pays tiers.

- Article 76, paragraphes 3 et 4: insérer une procédure d'information plus systématique au niveau des tribunaux.
- Préciser l'interaction avec le règlement Bruxelles-I.
- Préciser la compatibilité de l'utilisation des informations collectées auprès d'un responsable du traitement des données (sur la base de l'article 53) avec le droit général de ne pas contribuer à sa propre incrimination.
- Article 77: ajouter qu'une personne concernée doit toujours avoir la possibilité de s'adresser au responsable du traitement, indépendamment du lieu et de la façon dont le dommage est survenu en ce qui concerne le règlement du dommage. Insérer le règlement ultérieur du dommage entre le responsable du traitement et le sous-traitant, une fois que le partage des responsabilités entre eux a été clarifié. Ajouter que cela doit également s'appliquer à la compensation pour les dommages immatériels ou le préjudice moral.
- Introduire une disposition utilisant le concept d'une entité économique unique ou d'une entreprise unique afin de pouvoir tenir un groupe pour responsable des violations commises par une filiale.
- Article 79: insérer une liberté d'appréciation pour les autorités de contrôle en ce qui concerne les sanctions administratives. Ajouter des spécifications mettant en lumière les circonstances dans lesquelles une sanction administrative est infligée. Veiller à ce que la non-conformité à un ordre spécifique entraîne normalement une sanction administrative plus lourde qu'une seule violation de la même disposition générale.

Chapitre IX – Situations de traitement spécifique des données (partie II.11)

- Article 80: reformuler l'article 80 et déclarer que les États membres prévoient des exemptions ou des dérogations des dispositions incluses dans le règlement (comme déjà indiqué dans le texte actuel) *si cela s'avère nécessaire* pour concilier le droit à la protection des données avec le droit à la liberté d'expression. Ajouter, dans la disposition ou dans un considérant, que lors de la conciliation des deux droits fondamentaux, il ne doit pas être porté atteinte au contenu essentiel des deux droits.
- Ajouter une disposition de fond sur l'accès public aux documents, déclarant que les données à caractère personnel dans les documents détenus par les autorités et organismes publics peuvent être divulguées publiquement si cela est 1) prévu par le droit de l'UE ou le droit national, 2) nécessaire pour concilier le droit à la protection des données avec le droit d'accès du public aux documents administratifs et 3) constitue un juste équilibre entre les divers intérêts concernés.
- Remplacer aux articles 81, 82, 83 et 84 le libellé «Dans les limites du présent règlement» par «Sans préjudice du présent règlement».
- Article 81: aligner les articles 81, paragraphes 1 et 3, et 9, paragraphe 3, et préciser le champ d'application et la nature de l'article 81. Une nouvelle orientation devrait être donnée sur l'exigence du consentement, la détermination des responsabilités et les exigences en matière de sécurité.
- Article 83: inclure des garanties supplémentaires si des catégories particulières de données sont traitées. Préciser à l'article 83, paragraphe 1, que le point de départ pour le traitement des données à des fins de recherche doit être que ce traitement est effectué en utilisant des données rendues anonymes. Préciser ce que signifie le mot «séparément» et veiller à ce que cette conservation séparée protège réellement les personnes concernées. Faire référence, à l'article 83, paragraphe 1, point b), aux «données qui permettent de relier certaines informations à une personne concernée» plutôt qu'aux «données permettant de rattacher des informations à une personne concernée identifiée ou identifiable». Exclure la limitation aux droits des personnes via des actes délégués.

Recommandations sur la proposition de directive

Questions horizontales (partie III.2)

- Article 59: les actes dans le domaine de la coopération policière et judiciaire en matière pénale doivent être modifiés au plus tard au moment où la directive entre en vigueur.
- Ajouter une nouvelle disposition introduisant un mécanisme d'évaluation pour des évaluations régulières basées sur la preuve que les activités de traitement des données d'une certaines envergure constituent réellement nécessaire et proportionnée à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière.
- Ajouter une nouvelle disposition pour veiller à ce que le transfert des données à caractère personnel des autorités répressives vers d'autres organismes publics ou des parties privées n'est permis que sous certaines conditions spécifiques et strictes.
- Ajouter une nouvelle disposition sur des garanties spécifiques en relation avec le traitement des données des enfants.

Chapitres I et II – Dispositions générales et principes (parties III.3 et III.4)

- Article 3, paragraphe 4: étayer davantage, dans le sens de l'article 17, paragraphe 8, de la proposition de règlement.
- Article 4, point b): inclure une précision dans un considérant, déclarant que la notion de «compatibilité d'utilisation» doit être interprétée de manière restrictive.
- Article 4, point f): aligner sur l'article 5, point f), de la proposition de règlement et modifier les articles 18 et 23 en conséquence.
- Article 5: inclure les personnes non suspectes en tant que catégorie distincte. Supprimer le libellé «dans la mesure du possible» et spécifier les conséquences de la catégorisation.
- Article 6: supprimer «dans la mesure du possible» aux paragraphes 1 et 2.
- Article 7, point a): modifier en une disposition autonome, garantissant, de manière générale, que toutes les opérations de traitement des données sont prévues par la loi, satisfaisant ainsi aux exigences de la Charte des droits fondamentaux et de la CEDH.
- Article 7, points b) à d): remplacer par une disposition supplémentaire, séparée, qui énonce de façon exhaustive les motifs d'intérêt général pour lesquels une dérogation au principe de limitation de la finalité peut être accordée.
- Ajouter une nouvelle disposition sur le traitement des données à caractère personnel à des fins de recherche historique, statistique et scientifique.
- Ajouter une obligation pour l'autorité compétente de mettre en place des mécanismes pour garantir que des délais sont établis pour l'effacement des données à caractère personnel et pour une révision périodique de la nécessité de conservation des données, y compris la fixation de délais de conservation pour les différentes catégories des données à caractère personnel ainsi que des vérifications régulières de leur qualité.
- Article 8: inclure le libellé strict du considérant 26 à l'article 8. Inclure ce qui est visé par des mesures adéquates qui vont au-delà des garanties ordinaires.

Chapitre III – Droits de la personne concernée (partie III.5)

- Article 10: supprimer la référence à «toutes les mesures raisonnables» à l'article 10, paragraphes 1 et 2. Intégrer un délai explicite à l'article 10, paragraphe 4, et déclarer que les informations doivent être communiquées à la personne concernée. Remplacer le libellé «abusives» à l'article 10, paragraphe 8, par «au caractère manifestement excessif». Donner de plus amples indications sur cette notion dans un considérant.
- Ajouter une nouvelle disposition exigeant du responsable du traitement qu'il communique à chaque destinataire auquel les données ont été divulguées, toute rectification, tout effacement ou toute modification des données, effectués ou non conformément à l'article 15 ou 16, à moins que cela ne s'avère impossible ou n'implique un effort disproportionné.

- Articles 11 et 13: ajouter une phrase à l'article 11, paragraphe 4, et à l'article 13, paragraphe 1, déclarant que le responsable du traitement doit être tenu de vérifier chaque cas spécifique, au moyen d'un examen concret et individuel, afin de déterminer si des restrictions partielles ou complètes pour l'un des motifs s'appliquent. Assurer une interprétation limitée du champ d'application de l'article 11, paragraphe 8, et de l'article 13, paragraphe 2. Supprimer le mot «non-fourniture» à l'article 11, paragraphe 4, et au considérant 33.
- Articles 15 et 16: ajouter les motifs et les conditions pour limiter le droit de rectification et le droit à l'effacement.
- Article 16: utiliser le libellé «limite le traitement» au lieu de «marque» à l'article 16, paragraphe 3. Inclure à l'article 16 l'obligation pour le responsable du traitement d'informer la personne concernée avant de lever toute limitation sur le traitement.

Chapitre V – Responsable du traitement et sous-traitant (partie III.6)
- Article 18: mentionner, à l'article 4, point f) également, que l'exigence relative à la documentation découle de l'obligation générale de pouvoir *démontrer* la conformité avec la directive. Inclure l'exigence de conserver les informations sur le motif légal pour lequel les données sont transférées, avec des explications substantielles, notamment si un transfert est fondé sur l'article 35 ou 36.
- Article 19: étayer la notion de protection des données «par défaut».
- Article 23, paragraphe 2: aligner avec l'article 28, paragraphe 2, de la proposition de règlement.
- Article 24: inclure l'identité des destinataires des données.
- Insérer une nouvelle disposition, exigeant des autorités compétentes qu'elles procèdent à une analyse d'impact relative à la protection des données, à moins qu'une analyse spécifique, équivalente à une analyse d'impact relative à la protection des données, ait déjà été réalisée durant le processus législatif.
- Article 26: aligner plus étroitement avec les procédures développées à l'article 34, paragraphe 2, de la proposition de règlement.
- Article 30: traiter de la question du conflit d'intérêts et établir un mandat minimum de deux ans.
- Article 31: prévoir un rattachement administratif approprié en tenant dûment compte du rôle indépendant du délégué à la protection des données et en vue notamment d'éviter d'éventuelles relations inégales ou d'influence par des responsables du traitement de haut rang.

Chapitre V – Transfert vers les pays tiers (partie III.7)
- Article 33: ajouter l'exigence selon laquelle le transfert ne pourra avoir lieu que si le responsable du traitement dans le pays tiers ou l'organisation internationale est une autorité compétente au sens de la proposition de directive.
- Article 35: supprimer l'article 35, paragraphe 1, point b), ou inclure au minimum l'exigence d'une autorisation préalable de l'autorité de contrôle.
- Article 36: préciser dans un considérant que toute dérogation utilisée pour justifier un transfert doit être interprétée de manière restrictive et ne doit pas permettre un transfert fréquent, massif et structurel des données à caractère personnel; même un cas individuel ne doit pas permettre de transferts massifs de données et doit être limité aux données strictement nécessaires. Ajouter des garanties supplémentaires telles qu'une obligation de documenter spécifiquement ces transferts.
- Articles 35 et 36: ajouter qu'en cas de décision constatant le caractère inadéquat, les transferts doivent être fondés i) sur l'article 35, paragraphe 1, point a), s'il existe un accord international juridiquement contraignant autorisant le transfert sous certaines

conditions spécifiques garantissant une protection adéquate, ou ii) sur les dérogations visées à l'article 36, point a) ou c).

Chapitre VI et VII – Mécanismes de surveillance (partie III.8)

- Article 44: donner une plus grande orientation dans un considérant sur ce qui est destiné à être couvert par «l'exercice des fonctions juridictionnelles».
- Article 46: aligner les pouvoirs des autorités de contrôle vis-à-vis des autorités policières nationales visés dans le cadre de la proposition de règlement. Aligner l'article 46, point a), sur l'article 53 de la proposition de règlement et remplacer le libellé «tels que» à l'article 46, points a) et b), par «y compris».
- Article 47: inclure que le rapport annuel sur l'activité des autorités de contrôle doit être présenté au parlement national et rendu public.
- Article 48: inclure les dispositions de l'article 55, paragraphes 2 à 7, de la proposition de règlement à l'article 48.
- Examiner la nécessité d'un mécanisme de coopération accrue, dans le champ d'application de la proposition de directive également.

Fait à Bruxelles, le 7 mars 2012

(**signé**)

Peter HUSTINX
Contrôleur européen de la protection des données