OBSERVATIONS COMPLÉMENTAIRES DU CEPD SUR LE PAQUET DE MESURES POUR UNE RÉFORME DE LA PROTECTION DES DONNÉES

I. ANONYMISATION ET PSEUDONYMISATION

1. Concepts

1. De nombreux amendements ont été proposés en vue de définir l'anonymisation et la pseudonymisation, et de fournir des règles particulières concernant les données traitées de cette façon[1]. Si des mesures réfléchies *sont susceptibles de* créer des incitations à utiliser ces techniques dans l'optique d'améliorer la protection des données, des dérogations trop générales pourraient entraîner l'érosion du concept bien établi de données à caractère personnel tel que défini dans la directive 95/46/CE. **De l'avis du CEPD, il convient de s'assurer que les amendements relatifs à la définition des données anonymes et des données pseudonymes soient pleinement compatibles avec la définition des données à caractère personnel et qu'ils n'entraînent pas la suppression indue de certaines catégories de données du champ d'application du règlement, notamment dans les cas où il n'est pas certain que les données aient effectivement été rendues entièrement anonymes. Dans ce cas, les données ne devraient pas être exclues du champ d'application du règlement.**

2. En particulier, certaines catégories de données qui ne sont pas *rendues anonymes* de façon irréversible ne doivent pas être exclues du champ d'application du règlement, ni de certains de ses principes. Le CEPD met également en garde contre les amendements qui confondent pseudonymisation et anonymisation et, ce faisant, suppriment les données *pseudonymisées* du champ d'application du règlement ou de certains de ses principes fondamentaux. Plus précisément:
    - les amendements LIBE 729 et 730, ainsi que d'autres amendements au libellé similaire proposant une définition des données «pseudonymes» ou «pseudonymisées» pourraient être acceptés moyennant quelques modifications d'ordre rédactionnel, conformément à nos commentaires énoncés au point 2 ci-dessous,
    - le CEPD met en garde contre les amendements LIBE AM 726 et 728,
    - les amendements qui feraient de la pseudonymisation une raison suffisante de rendre légitime le traitement des données, tels que les amendements LIBE AM 887, 897, 898 et 900, ou qui autoriseraient le profilage à partir de

[1] Dans certains cas, le chiffrement des données est lui aussi perçu de la même façon, bien qu'il s'agisse d'une mesure technique totalement différente ayant un effet limité principalement au niveau de la sécurité des données.

Adresse postale: rue Wiertz 60 - B-1047 Brussels
Bureaux: rue Montoyer 30
E-mail: edps@edps.europa.eu - Site Internet: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

telles données, tels que les amendements LIBE AM 1568 et 1585, doivent être **rejetés**.

2. Définitions

3. La définition des données à caractère personnel a été énoncée à l'article 2, point a), de la directive 95/46/CE (lu en combinaison avec le considérant 26). De plus, le groupe de travail «Article 29» a fourni des orientations quant à la notion de données à caractère personnel[2], identifiant un certain nombre de critères contribuant à déterminer si la définition est applicable. Le critère principal est l'**identifiabilité** de la personne. Ce critère contient deux éléments:

   (a) si la personne peut être identifiée, *directement ou indirectement*, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale [article 2, point a), de la directive], et

   (b) *par rapport à qui*: le responsable du traitement, le sous-traitant et tout tiers mettant en œuvre des moyens raisonnables pour identifier cette personne (considérant 26 de la directive).

4. Il convient en outre de faire remarquer que les moyens que le responsable du traitement ou tout tiers pourrait mettre en œuvre pour identifier une personne sont plus étendus qu'en 1995 du fait des progrès technologiques réalisés. Or, cette tendance devrait se poursuivre à l'avenir.

5. L'**anonymisation** des données à caractère personnel consiste à changer un ensemble de données de telle sorte qu'il devienne impossible au responsable du traitement ou à quiconque d'autre d'identifier, directement ou indirectement, la personne à laquelle les données ont trait. **Les données anonymes ne sont pas des données à caractère personnel et ne relèvent pas du champ d'application de la législation en matière de protection des données.** L'anonymisation nécessite d'effacer de l'ensemble de données non seulement tous les attributs d'identification directe (tels que les noms, numéros des registres d'état civil, numéros de téléphone, données biométriques), mais également, en règle générale, les données qui, combinées, font ressortir des caractéristiques uniques et toute autre modification[3], afin d'empêcher la réidentifiabilité. Certains types de données à caractère personnel, tels que les données biométriques, suffisent à eux seuls à identifier les personnes concernées et ne sauraient dès lors faire partie d'un quelconque ensemble de données rendues anonymes du fait de leur nature même (tel que par exemple les photographies faciales et les empreintes digitales). Les recherches récentes semblent indiquer que les données de localisation fines peuvent également suffire à elles seules à identifier la personne à laquelle elles se rapportent. Le concept d'identification comprend également l'aptitude à distinguer une personne de toutes

[2] Avis 4/2007 du groupe de travail «Article 29» sur le concept de données à caractère personnel, WP 136, 20.06.2007.

[3] Si les ensembles de données contiennent un nombre suffisant d'attributs, il est fort probable que les personnes se caractérisent par une combinaison de valeurs unique et puissent être identifiées. Les recherches ont montré que même des ensembles de données statistiques peuvent être réidentifiés si aucune mesure spécifique n'est prise pour éviter que tel soit le cas. Voir par exemple: http://www.census.gov/srd/papers/pdf/rrs2012-13.pdf

les autres («singularisation»), même en l'absence des identifiants couramment utilisés.

6. Par contre, **les données pseudonymisées** sont, par définition, des données relatives à une personne identifiable, en ce que le lien entre le pseudonyme et les données d'identification (telles que par exemple le nom, le prénom, l'adresse, etc.) est connu du responsable du traitement ou d'un tiers. Même si le pseudonyme et sa corrélation avec l'identité sont exclusivement connus d'une partie donnée (qu'il s'agisse du responsable du traitement ou d'un tiers) et ne sont partagés avec quiconque, **les données pseudonymisées restent des données à caractère personnel**[4]. **Les données pseudonymisées relèvent donc du champ d'application du règlement**[5].

7. Compte tenu de ces considérations, le CEPD suggère que toute définition d'«un pseudonyme» s'appuie sur les éléments suivants:

   - les «données pseudonymisées» font référence aux informations relatives à une personne physique qui peut être identifiée, directement ou indirectement (à savoir, elles continuent de relever des «données à caractère personnel»),
   - les moyens qui peuvent être mis en œuvre pour identifier la personne sont séparés efficacement des données concernées,
   - l'identification par des personnes non autorisées est prévenue de manière efficace.

3. Conséquences au niveau d'autres parties de la proposition

8. Étant donné que les **données pseudonymes restent des données à caractère personnel**, le CEPD met en garde contre des amendements qui dispensent d'un traitement des données pseudonymes des principes essentiels régissant la protection des données, tels que la transparence, la licéité du traitement et les droits des personnes concernées. Dans le même temps, le règlement pourrait inclure des mesures incitant les responsables du traitement ou sous-traitants à utiliser de bonne foi les données pseudonymes, sous réserve que le traitement soit soumis à des conditions strictes (par exemple en termes de sécurité et de confidentialité). Cela

[4] Les données enregistrées qui ne contiennent pas d'attributs d'identification communs (tels que le nom et l'adresse) mais des valeurs uniques utilisées dans le cadre de transactions avec de nombreuses parties (telles que les adresses IP ou les numéros de cookies) ne peuvent pas même être considérés comme des pseudonymes dans la mesure où de nombreux tiers ont connaissance de ces attributs et pourraient être capables d'identifier la personne concernée. Dans ce cas, ces données sont des données à caractère personnel dans la mesure où elles sont identifiables «par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne...».

[5] Une autre technique totalement différente est le chiffrage, un procédé technique consistant à brouiller temporairement les données sous forme illisible ou inintelligible à des fins de confidentialité ou d'intégrité de telle sorte que des personnes se livrant à des écoutes clandestines ou des pirates informatiques ne puissent ni les lire ni les modifier, mais que les parties autorisées puissent ce faire. Les données à caractère personnel chiffrées ne devraient pas être considérées comme des données rendues anonymes dans la mesure où le brouillage est uniquement temporaire, où toute personne détenant la clé de chiffrement peut facilement retrouver les données, et où il est possible de percer à jour le chiffrement sans être en possession de la clé si l'on dispose de ressources suffisantes. Un chiffrement renforcé et à la pointe du progrès peut néanmoins réduire considérablement le risque de violations des données (et les conséquences de celles-ci) et devrait par conséquent être considéré comme une mesure de sécurité importante et, à ce titre, être encouragé (par exemple à l'article 30) lorsqu'il est utilisé comme il se doit.

pourrait être par exemple opéré au niveau des dispositions relatives aux violations de données à caractère personnel (articles 31 et 32), selon que les données concernées par la violation ont fait l'objet ou non d'une protection adéquate empêchant l'identification, ou au niveau des dispositions relatives à la recherche et aux statistiques (article 83). Cela pourrait également être envisagé pour la conception de nouveaux systèmes informatiques (article 23 sur la protection des données dès la conception).

II. CHAMP D'APPLICATION DU RÈGLEMENT

1. Champ d'application matériel

9. En ce qui concerne le champ d'application matériel du règlement, le CEPD constate avec inquiétude une tendance qui se dégage des nombreux amendements de l'**article 2** proposés, lesquels limiteraient le champ d'application du futur règlement en créant des exceptions pour des secteurs ou situations de traitement donnés (tels que le secteur financier ou le contexte de l'emploi). S'il reconnaît que, dans certains cas, des dispositions particulières sont justifiées, le CEPD remarque que bon nombre de celles-ci sont déjà couvertes au chapitre IX relatif aux situations particulières de traitement des données. Qui plus est, un certain nombre d'exceptions concernant des finalités particulières sont définies à l'article 21, lequel énonce les conditions que toute limitation des droits et des obligations prévus au règlement doit remplir. L'ajout d'exceptions supplémentaires à l'article 2 non seulement entraînerait des lacunes importantes au niveau de la protection des droits fondamentaux des citoyens européens, mais irait également à l'encontre de l'idée même d'un cadre pour la protection des données commun (aussi global et uniforme que possible) à toute l'Europe. Ce faisant, le CEPD déconseille l'adoption de ces exceptions.

(a) Institutions et organes de l'UE

10. Le CEPD relève toute une série d'amendements (tels que LIBE AM 666) qui suppriment la dérogation pour les institutions de l'UE à l'article 2, incluant ainsi les institutions, organes et organismes de l'UE dans le champ d'application du futur règlement.

11. Ces amendements sont conformes aux recommandations[6] antérieures du CEPD et devraient, en théorie, être soutenus. Dans le même temps, il convient toutefois de souligner qu'**il faudra plus qu'une simple suppression de la dérogation prévue à l'article 2** pour créer un cadre juridique cohérent et une sécurité juridique suffisante pour tous les acteurs concernés, compte tenu du cadre juridique et institutionnel particulier dans lequel ils évoluent. En effet, le règlement (CE) nº 45/2001 qui s'applique à l'heure actuelle aux institutions et organes de l'UE couvre certaines questions qui sont spécifiques au contexte institutionnel de l'UE et qui, aux termes de la proposition de règlement général, continueraient d'échapper à la réglementation. Elles incluent: i) les transferts de données à caractère personnel entre institutions de l'UE, ainsi qu'entre celles-ci et d'autres destinataires; ii) les règles applicables au traitement des données au sein des réseaux internes de

[6] Voir l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, points 29 à 31.

télécommunications[7]; iii) les règles régissant la nomination du contrôleur européen de la protection des données et du contrôleur adjoint; et iv) un catalogue détaillé des fonctions et des pouvoirs du CEPD qui ne recoupent pas entièrement ceux des autorités nationales de contrôle, et qui ne peuvent pas entièrement les recouper dans la mesure, par exemple, où ils ont trait à la relation entre le CEPD et la Cour de justice de l'UE.

12. Ce faisant, le CEPD déconseille de simplement supprimer la dérogation prévue à l'article 2 sans qu'un autre texte ne traite des points susmentionnés, et serait au moins très favorable à l'ajout d'un considérant soulignant la nécessité d'aligner pleinement sur le règlement le cadre pour la protection des données concernant les institutions et organes de l'UE avant que le règlement ne soit applicable[8].

(b) Tribunaux dans l'exercice de leurs fonctions juridictionnelles

13. Parmi les amendements relatifs au champ d'application des pouvoirs de contrôle des autorités nationales de protection des données (article 51 de la proposition de règlement), le CEPD accueille favorablement ceux qui permettraient aux États membres d'étendre ces pouvoirs également aux traitements effectués par les tribunaux dans l'exercice de leurs fonctions juridictionnelles (LIBE AM 2595). Cela est conforme non seulement à la convention 108 et à son protocole concernant le contrôle indépendant, mais aussi à la tradition de plusieurs États membres, et devrait, à ce titre, être soutenu. Cette conclusion repose également sur le fait que la limitation figurant actuellement dans la proposition de la Commission ne s'applique pas non plus aux ministères publics.

2. Limitation *rationae temporis*

14. Le CEPD estime que la limitation de l'application du règlement dans le temps (comme par exemple dans LIBE AM 664 et 665) n'est pas nécessaire, étant donné que la période de *vacatio legis* proposée (deux ans) semble suffisante pour mettre tous les traitements existants en conformité avec les nouvelles règles. Le CEPD déconseille l'adoption de ces amendements.

3. Champ d'application territorial

15. Concernant le champ d'application territorial, des amendements de l'article 3, paragraphe 1, ont été proposés aux termes desquels les personnes concernées qui seront couvertes par le règlement seront confinées à celles **«ayant leur résidence sur le territoire de l'Union»** (LIBE AM 700, LIBE AM 701, LIBE AM 703).

16. S'ils sont acceptés, ces amendements viseraient à priver de protection de vastes groupes de personnes concernées qui sont pour l'heure protégés par la directive 95/46/CE. Tel serait par exemple le cas des touristes, ainsi que des activités de traitement menées au sein de l'UE concernant des personnes concernées ayant leur résidence à l'étranger, créant ainsi une justice à deux vitesses au sein de l'Union. En outre, il convient de souligner que cette limitation au niveau du droit dérivé est contraire au droit originaire, à savoir l'article 16 du TFUE et l'article 8 de la Charte

[7] Ces règles sont approximativement équivalentes à celles figurant dans la directive 97/66/CE, laquelle a ultérieurement été révisée et remplacée par la directive 2002/58/CE relative à la vie privée et aux communications électroniques.
[8] Voir l'article 91, paragraphe 1, de la proposition de la Commission.

des droits fondamentaux de l'UE, lesquels accordent explicitement le droit à la protection des données à caractère personnel à «toute personne», à savoir à toute personne qui relève du champ d'application du droit de l'UE, indépendamment de son lieu de résidence. Cela a également été un important point de départ des discussions avec les pays tiers. Étant donné que la proposition de règlement limite le champ d'application des droits subjectifs de manière appropriée, l**e CEPD déconseille l'adoption de ces amendements.**

III. LIMITATION DE LA FINALITÉ ET LICÉITÉ DU TRAITEMENT

1. Limitation de la finalité

17. Le CEPD accueille particulièrement favorablement l'amendement LIBE AM 103 qui propose **de supprimer l'article 6, paragraphe 4** tel que proposé par la Commission. **L'article 6, paragraphe 4** ouvre des possibilités de traitement des données pour des finalités incompatibles pour autant que le traitement trouve sa base juridique dans l'article 6, paragraphe 1, points a) à e). Ce texte signifierait de fait qu'il serait toujours possible de remédier à l'incompatibilité en identifiant simplement un nouveau fondement juridique du traitement. Toutefois, le CEPD souligne[9] que l'interdiction de l'incompatibilité d'utilisation et l'exigence de la licéité sont deux conditions cumulatives. L'exigence de la compatibilité ne peut être levée en se référant simplement à une condition de licéité du traitement. Cela serait en outre contraire à l'article 5 de la convention 108 du Conseil de l'Europe, laquelle est contraignante pour tous les États membres.

18. À l'heure actuelle, la logique de la directive 95/46/CE veut que l'utilisation incompatible ne soit autorisée que sous réserve des conditions de l'article 13 pour certaines raisons d'intérêt général (voir l'article 21 de la proposition de règlement). Dès lors, **le CEPD est favorable à la suppression de l'article 6, paragraphe 4**, laquelle permettrait de maintenir la logique de la directive 95/46/CE (alors qu'un changement de finalité serait possible dans des conditions strictes conformément à l'article 21). La question de la compatibilité est l'un des principaux sujets à propos duquel le groupe de travail «Article 29» adoptera un avis dans les semaines à venir. Cet avis fournira des orientations et critères concrets pour une interprétation commune de la notion de «compatibilité».

19. Le CEPD déconseille les amendements qui suggèrent qu'un traitement ultérieur de données à des fins liées à la santé ne devrait pas être considéré comme incompatible (LIBE AM 821) dans la mesure où le traitement ultérieur de données aussi sensibles pourrait avoir une incidence importante sur la protection de la vie privée des personnes. Aux termes du droit actuel, les possibilités de traitement ultérieur dépendent de critères tels que ceux qui viennent d'être mentionnés.

2. Licéité du traitement

20. Le projet de rapport de la commission LIBE propose de longues listes normatives pour l'**article 6, paragraphe 1, point b) et l'article 6, paragraphe 1, point c)** qui décriraient les situations dans lesquelles les intérêts légitimes des responsables du traitement l'emportent sur les droits et intérêts des personnes concernées et vice

[9] Voir aussi l'avis du CEPD du 7 mars 2012, points 115 à 124.

versa (LIBE AM 99-102). **De l'avis du CEPD, ces listes normatives sont contre-productives et devraient être rejetées**.

21. Le CEPD conseille de remplacer ces listes par une disposition plus concise, tenant compte du fait qu'il existe de nombreuses situations qui ne peuvent pas être prévues à l'avance et qui doivent être examinées *in concreto* au cas par cas. En outre, **un considérant** pourrait énumérer les facteurs pertinents les plus fréquents dont il faudrait tenir compte afin d'équilibrer les intérêts et droits fondamentaux en jeu. Si nécessaire, certains exemples de ce qui pourrait constituer des «intérêts légitimes» peuvent également être fournis.

22. En revanche, le CEPD accueille favorablement la proposition d'amendement de **l'article 6, paragraphe 1, point a)** (LIBE AM 100), qui vise plus de transparence quant aux «motifs qu'il a de croire que ses intérêts prévalent sur les intérêts ou les libertés et les droits fondamentaux de la personne concernée.» Cela favoriserait une responsabilité accrue quant à la façon d'atteindre un équilibre acceptable entre les divers intérêts.

23. Enfin, le CEPD insiste sur le fait que le concept de **consentement explicite** tel que défini à l'heure actuelle dans la proposition de la Commission [notamment à l'article 4, paragraphe 8, à l'article 6, paragraphe 1, point a) et à l'article 7] **devrait être maintenu**. Il permet un certain degré de flexibilité quant à la façon dont il est exprimé (soit en une déclaration soit en un acte non équivoque) et s'appuie sur la nécessité de consentement «indubitable» qui constitue une composante essentielle de l'équilibre général de la protection des données depuis 1995. Selon la jurisprudence constante des instances de l'UE chargées de la protection des données, l'exigence de l'article 7, point a), de la directive 95/46/CE, lue conjointement avec l'article 2, point h), selon laquelle le consentement doit être «indubitable» signifie qu'un tel consentement doit être «explicite»[10] (de sorte que, par exemple, l'absence d'action ou le silence ne saurait être considéré comme indubitable). Dès lors, le CEPD recommande le **rejet** des amendements tels que ITRE AM 83, IMCO AM 63, et les propositions d'amendement LIBE AM 757, 758, 760, 764 à 766, etc.

IV. RÔLES, OBLIGATIONS ET RESPONSABILITÉ RESPECTIVES DU RESPONSABLE DU TRAITEMENT ET DU SOUS-TRAITANT

24. Les amendements relatifs aux fonctions du responsable du traitement/sous-traitant touchent de nombreuses parties du texte, y compris les définitions. Plusieurs amendements supprimeraient la notion selon laquelle le responsable du traitement détermine **non seulement les finalités mais aussi «les conditions et les moyens»** du traitement, tel que défini à l'article 4, paragraphe 5, de la proposition (par exemple ITRE AM 81; IMCO AM 62; LIBE AM 746, 747 et 748). Les critères selon lesquels le responsable du traitement détermine les «finalités et les moyens» du traitement ont été établis dans la directive 95/46/CE et développés dans l'avis 1/2010 du groupe de travail «Article 29» sur les concepts de «responsable du traitement» et de «sous-traitant». **Ces critères ont contribué efficacement à la**

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

compréhension et à la délimitation des rôles des responsables du traitement et des sous-traitants et, dès lors, ne devraient pas être supprimés.

25. De nombreux amendements visent à réduire la responsabilité des sous-traitants prévue dans la proposition, par exemple en supprimant ou en réduisant les obligations pour le sous-traitant de tenir à jour la documentation, d'effectuer une analyse de l'impact sur la protection des données ou d'aider le responsable du traitement à se conformer aux obligations en matière de sécurité (à savoir ITRE AM 43, 229, 233, 238 et 260; LIBE AM 1829, 1832, 1834, 1836, 1837 et 2024). Toutefois, l'extension de certaines obligations aux sous-traitants reflète le rôle actuel croissant que jouent les sous-traitants au niveau de la détermination de certaines conditions essentielles du traitement (par exemple dans le contexte de l'informatique dématérialisée, où ils décident souvent des transferts et du sous-traitement). **Dans ce contexte, les sous-traitants devraient également être responsables de leur traitement.** La clarification expliquant que les sous-traitants qui ne suivent pas les instructions ou vont au-delà de celles-ci deviennent responsables du traitement (article 26, paragraphe 4) devrait être conservée. Le CEPD déconseille donc d'appliquer les suggestions présentées dans les amendements ITRE AM 231 ainsi que LIBE AM 1808 à 1810.

26. Les **trois composantes de la responsabilité devraient demeurer: garantir la conformité**, **en apporter la preuve** et **la vérifier**. Plusieurs amendements émanant de diverses commissions et visant la suppression de tout ou partie de ces aspects de la responsabilité, dans l'optique de réduire la charge pesant sur les responsables du traitement (tels que ITRE AM 199, 204, 207; LIBE AM 1658, 1661, 1687, 1688, 1834, 1836), devraient être rejetés. En outre, les amendements suggérant la suppression de l'article 28 relatif à la documentation (LIBE AM 1825, 1826, 1830) devraient être rejetés.

27. Afin de réduire la charge administrative, Albrecht AM 188 propose que la documentation à conserver aux termes de l'article 28 reprenne sensiblement les informations à fournir à la personne concernée aux termes de l'article 14. Bien que cela s'apparente à une simplification, il est improbable que la documentation énumérée à l'article 14 (même telle qu'étendue selon les amendements Albrecht AM 125 à 133) suffise pour vérifier la conformité dans la mesure où la liste de l'article 28 coïncide dans une certaine mesure avec la liste d'informations à fournir aux personnes concernées de l'article 14. De l'avis du CEPD, les informations à conserver au titre de documentation devraient contenir des informations suffisantes pour permettre la vérification, à la demande des autorités de contrôle, des deux aspects suivants des traitements:

    i) elles devraient consigner les éléments justifiant de la façon dont le système de contrôle des traitements est structuré, et

    ii) elles devraient consigner les éléments justifiant des performances des deux (par exemple sur la base des fichiers journaux).

28. Enfin, le CEPD salue les amendements qui décrivent de façon plus détaillée les mesures que les organisations devraient mettre en œuvre en interne pour aider à garantir la responsabilité (telles que les politiques et procédures internes, la formation du personnel, la preuve de la mobilisation de la haute direction, les

analyses de l'efficacité à des intervalles réguliers, suggérées dans les amendements ITRE AM 205, 210, 212 et 213; LIBE AM 1684 et 1698).

V. FLEXIBILITÉ, APPROCHE FONDÉE SUR L'ANALYSE DES RISQUES ET MPME

29. Plusieurs amendements tendent à introduire une approche fondée sur l'analyse des risques et assortie d'une liste détaillée de ce qui constituerait des traitements présentant des risques. **Le CEPD met en garde contre tout amendement qui pourrait avoir pour effet que la protection ne s'applique qu'aux traitements présentant le plus de risques.** La protection complète prévue au règlement devrait s'appliquer à tous les traitements et pas uniquement à ceux qui présentent le plus de risques (par exemple, le principe de protection des données dès la conception ne devrait pas s'appliquer uniquement «lorsque nécessaire» ou suite à l'approche fondée sur les risques, comme le suggèrent les amendements IMCO AM 138 et 140 ainsi que ITRE 216). Il y a lieu de tenir compte du fait que le risque est inhérent à tout traitement de données. Par ailleurs, le CEPD recommande de rejeter les amendements qui modifient l'équilibre entre le risque et les mesures, par exemple en liaison avec l'article 30 sur la sécurité (ITRE AM 243 ainsi que LIBE AM 1922, 1923, 1924, 1925 et 1926). La gestion des risques nécessaire garantira la proportionnalité de l'effort et du risque.

30. Par contre, **le CEPD remarque de nombreux éléments positifs au niveau de l'approche progressive fondée sur l'analyse des risques que suit le Conseil**[11]. Cette approche suggère que des obligations plus détaillées devraient être applicables lorsque le risque est supérieur alors que, lorsque le risque est inférieur, le caractère normatif devrait être réduit. Une clause sur le risque horizontal serait introduite à l'article 22 et de nombreuses dispositions du chapitre IV du règlement seraient remaniées dans l'optique d'accorder davantage d'importance **au principe de responsabilité**. Des mesures incitatives sont recherchées en vue d'alléger les obligations des responsables du traitement au sein des organisations ayant mis en place des mesures contribuant à la responsabilité.

31. À cet égard, plusieurs amendements ont également été présentés au Parlement en vue de mettre davantage l'accent sur la notion de responsabilité et d'alléger plusieurs obligations du responsable du traitement, notamment concernant les notifications à l'autorité de contrôle (en particulier concernant les articles 22 à 29, 33 et 34). **Le CEPD accueille favorablement les amendements qui renforcent les effets du principe de responsabilité,** dans la mesure où il reconnaît la nécessité d'introduire davantage de souplesse concernant les organisations ayant mis en place des mécanismes de responsabilité, tels que la nomination d'un délégué à la protection des données ou la mise en œuvre de mécanismes de certification reconnus.

32. Par contre, l'allègement de certaines obligations du responsable du traitement dans ce contexte ne devrait pas entraîner la suppression d'obligations importantes relatives au traitement présentant des risques. En particulier, le CEPD déconseille les amendements qui dispenseraient les responsables du traitement de l'obligation

[11] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/135901.pdf.

de réaliser une analyse d'impact relative à la protection des données s'ils ont nommé un délégué à la protection des données, s'ils font l'objet d'un mécanisme de certification (amendement AM 297 proposé par la commission JURI) ou si le traitement est fondé sur le consentement ou une obligation légale (LIBE AM 2020). Dans tous ces cas, les traitements qui présentent particulièrement des risques devraient toujours nécessiter la réalisation d'une analyse d'impact relative à la protection des données afin d'analyser les risques et donc de les atténuer. De plus, le CEPD déconseille les amendements qui supprimeraient l'obligation imposant au responsable du traitement de consulter l'autorité de contrôle avant d'entreprendre des traitements présentant des risques (tels que les amendements ITRE AM 207, 208 et 272, ainsi que LIBE AM 2108). **La nécessité de notification à l'autorité de contrôle en cas de traitement présentant des risques devrait être maintenue, bien que les modalités de la procédure auprès de l'autorité de contrôle puissent pour leur part être allégées.** Par exemple, des mesures incitatives pourraient être mises en place concernant les organisations qui mettent en œuvre des mécanismes de responsabilité particuliers de telle sorte que, dans ce cas, la notification soit gérée dans le cadre d'une procédure rapide et simplifiée de consultation préalable, uniquement dans le but de s'assurer du respect de bonnes pratiques.

33. À cet égard, le CEPD estime qu'**il devrait y avoir davantage de mesures incitatives concernant l'utilisation de délégués à la protection des données.** Par exemple, si certaines obligations devraient rester applicables au responsable du traitement concernant les traitements présentant des risques, telles que la nécessité de notifier l'autorité de contrôle du traitement à des fins de consultation préalable, un allègement des procédures pourrait être envisagé lorsqu'un délégué à la protection des données a été nommé, allègement dans le cadre duquel le traitement pourrait commencer dès la date de notification, sans qu'il soit nécessaire d'attendre la réponse de l'autorité de contrôle. Par ailleurs, au-delà de la question consistant à décider si la nomination d'un délégué à la protection des données devrait être rendue obligatoire ou facultative, il y a lieu de reconnaître que toutes les organisations doivent avoir mis en place des mécanismes permettant de se conformer aux obligations relatives à la protection des données. Cela nécessite de s'en remettre à plusieurs personnes en interne (faisant par exemple partie des départements informatique, juridique, GRH et conformité) afin de s'assurer que les traitements de l'organisation sont conformes à ces obligations. Dans la plupart des cas, il peut s'avérer non seulement bénéfique mais aussi utile que l'organisation confie à une autre personne encore la responsabilité générale des questions relevant de la protection des données au niveau interdépartemental.

34. Plusieurs amendements visant à introduire de nouvelles exceptions pour les micro, petites et moyennes entreprises («MPME») devraient être rejetés dans la mesure où ils les dispenseraient des principes généraux du règlement, plutôt qu'uniquement des dispositions spécifiques. Par exemple, ils visent à supprimer du champ d'application du règlement le traitement réalisé par les MPME à des «fins internes» (LIBE AM 678 à 680) ou à dispenser les MPME de l'obligation de tenir à jour la documentation prévue à l'article 28 (par exemple ITRE AM 235) ou de celle de réaliser une analyse d'impact relative à la protection des données notamment lorsque le traitement est au cœur de leurs activités (ITRE AM 160). Des exceptions

ou limitations relatives à des dispositions particulières pourraient être envisagées uniquement lorsque cela est approprié[12].

VI. TRANSFERTS, Y COMPRIS LES PROPOSITIONS D'ARTICLES 43bis ET 44bis

35. Les amendements visant à clarifier le principe du **«caractère adéquat»** et à y ajouter des éléments devraient être **rejetés** en ce qu'ils risquent uniquement de porter à confusion (JURI AM 53 et LIBE AM 2383 à 2386).

36. Le caractère adéquat devrait rester possible pour les **secteurs,** comme tel est actuellement le cas pour certaines décisions relatives au caractère adéquat, comme par exemple la sphère de sécurité américaine (*US Safe Harbor* - uniquement applicable à certaines parties du secteur privé) ou le Canada (couvrant uniquement le secteur privé). Certains amendements de l'article 41, paragraphe 1, suppriment cette possibilité (LIBE AM 241). Or, cela serait contraire à la reconnaissance du «principe du caractère adéquat» comme «concept fonctionnel», afin de permettre un véritable échange de données avec les pays tiers (ou un secteur de traitement au sein d'un pays tiers). **Le CEPD déconseille ces amendements.**

37. Par contre, s'agissant des transferts vers des pays tiers qui ont été déclarés inadéquats, la proposition de la commission manquait de clarté quant à savoir si l'article 41, paragraphe 5 interdit totalement le transfert vers ces pays ou si les transferts seraient possibles sous certaines conditions (contradiction entre le considérant 82 et l'article 41, paragraphe 5). Au vu de cela, le CEPD estime que des amendements positifs de l'article 42, paragraphe 1, ont été inclus et clarifient le fait que des garanties appropriées peuvent être adoptées dans les cas pour lesquels la Commission a adopté une décision de caractère non adéquat aux termes de l'article 41, paragraphe 5 (LIBE AM 2415, ITRE AM 305 première partie de l'amendement, JURI AM 55). **Il convient donc de soutenir ces amendements.**

38. Le CEPD est favorable aux amendements qui **élargissent le champ d'application des règles d'entreprise contraignantes** [article 43, paragraphe 1, point a)] de sorte qu'elles s'appliquent également **à leurs sous-traitants externes** (LIBE 2470 to 2479). Cet élargissement pourrait renforcer la protection et contribuer à la sécurité juridique dans des domaines tels que l'informatique dématérialisée, lesquels se caractérisent par une multitude de relations avec des sous-traitants.

39. Certains amendements ont introduit un nouvel **article 43bis sur les transferts qui ne sont pas autorisés par le droit de l'UE** (Albrecht AM 259, LIBE AM 2490, ainsi que JURI AM 354). Le CEPD soutient ces amendements qui, par exemple, traitent des cas où une demande émanant d'un juge étranger (pays tiers) exige d'un responsable du traitement ou d'un sous-traitant lié par le droit de l'UE relatif à la protection des données qu'il transfère des données à caractère personnel (par exemple les cas d'administration de la preuve électronique).

[12] Voir l'avis du CEPD du 7 mars 2012, points 79 et 80.

40. Un autre amendement propose d'ajouter **un nouvel article 44bis** (LIBE AM 2531) sur les transferts vers des services informatiques dématérialisés relevant de la juridiction d'un pays tiers. Il y a en effet lieu de saluer une plus grande transparence en la matière. Toutefois, les risques que cet amendement envisage de traiter en imposant certaines obligations ne sont pas spécifiques à l'informatique dématérialisée; il s'agit des risques typiques des transferts internationaux. Il est vrai que, dans le domaine de l'informatique dématérialisée, ces risques sont plus évidents et que les droits des personnes concernées sont plus incertains, dans la mesure où il n'est pas toujours possible de savoir où les données à caractère personnel se trouvent, ni quels sont les éventuels risques inhérents au pays (ou aux pays) destinataire. Cependant, la création de nouvelles obligations ne devrait pas se faire d'une façon qui n'est pas neutre sur le plan technologique. **Le CEPD déconseillerait donc cet amendement.**

VII. COOPÉRATION, COHÉRENCE, POUVOIRS CONTRAIGNANTS DU COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES

41. De façon générale, le CEPD accueille favorablement tout mécanisme qui fournit un «guichet unique» aux responsables du traitement mais qui n'attribue pas une compétence *exclusive* à l'«autorité chef de file» et, ce faisant, permet aux personnes concernées de s'adresser à l'autorité de contrôle de leur propre pays de résidence (rapport Albrecht AM 277 introduisant un nouvel article 54bis).

42. Le CEPD accueille favorablement les amendements (dans le projet de rapport Albrecht) qui suppriment la possibilité que la Commission puisse intervenir à diverses occasions dans le cadre du mécanisme de contrôle de la cohérence et annuler la décision d'une autorité de contrôle nationale sur une question spécifique en adoptant un acte d'exécution [telle que prévue aux articles 58, 59, 60, paragraphe 1, et 62, paragraphe 1, point a), de la proposition de règlement]. Comme cela est souligné dans son avis du 7 mars 2012, ces pouvoirs de la Commission portent préjudice à l'indépendance des autorités de contrôle nationales, garantie au chapitre VI et seraient contraires au TFUE, à la Charte des droits fondamentaux de l'UE et à la jurisprudence de la Cour de justice de l'UE.

43. Parmi les options présentées, le CEPD préférerait celle proposée dans le projet de rapport Albrecht relativement aux chapitres VI et VII. Toutefois, le projet de rapport laisse certaines questions sans réponse en ce qui concerne l'architecture du système. Le CEPD estime qu'une réflexion plus approfondie s'impose quant au rôle du comité européen de la protection des données dans le mécanisme de contrôle de la cohérence, concernant des questions telles que s'il devrait ou non rendre des décisions contraignantes, et dans l'affirmative, selon quelles modalités. Cette réflexion devrait tenir particulièrement compte du besoin d'uniformité à travers l'UE ainsi que de la nécessité d'offrir une voie de recours juridique aux personnes physiques et organisations. Le point de départ de cette réflexion devrait être que les autorités de contrôle nationales restent les principaux responsables et comptables au niveau de leur système juridique national.

44. **Le CEPD recommande le rejet des amendements proposés dans l'avis de la commission ITRE**, lesquels édulcorent le mécanisme de contrôle de la cohérence et donneraient un rôle important aux lobbies puissants. Le CEPD déconseillerait également les amendements visant à permettre aux responsables du traitement, aux personnes concernées ou aux «parties prenantes» de déclencher le mécanisme de contrôle de la cohérence, dans la mesure où cela rendrait le système impraticable (voir par exemple IMCO AM 195 ou ITRE AM 352). Les personnes physiques devraient toujours être en mesure de demander réparation en justice auprès de leurs tribunaux nationaux.

45. Enfin, le CEPD estime que le comité européen de la protection des données pourrait tirer profit d'un outil informatique approprié soutenant les échanges d'informations entre autorités de contrôle, tel que le système d'information du marché intérieur (IMI)[13], et remarque que, si l'utilisation d'un outil informatique était envisagée, cela pourrait nécessiter l'ajout d'une base juridique dans le règlement.

VIII. SANCTIONS

46. Le CEPD rappelle que, dans son avis du 7 mars 2012, il préconisait le renforcement du nouveau droit pour les organisations ou associations qui défendent les droits des personnes concernées d'introduire une réclamation auprès d'une autorité de contrôle ou de saisir une juridiction (articles 73 et 76 de la proposition de règlement). Il estime donc que **les amendements qui affaibliraient une telle action collective** (voire même l'élimineraient totalement, comme LIBE AM 2777 et les amendements suivants) **ne devraient pas être soutenus.**

47. L'avis demandait également une plus grande flexibilité au niveau de l'application des sanctions pour violation du règlement. Une liberté d'appréciation pour les autorités de contrôle est un élément indispensable d'un système d'exécution cohérent et modulaire, en particulier au regard des différentes options dont disposeraient les autorités de contrôle afin d'imposer des sanctions *réparatrices* en cas de violation particulière du règlement [voir article 53, paragraphe 1, point a)]. De ce point de vue, l**e CEPD accueille favorablement les amendements qui accordent aux autorités de contrôle une plus grande liberté d'appréciation pour décider d'imposer ou non une sanction,** notamment concernant les cas de non-conformité qui n'étaient pas intentionnels (par exemple Albrecht AM 318). Dans le même temps, il estime que l'ajout de listes de facteurs «aggravants» ou «atténuants» (comme dans Albrecht AM 316 et 317, ITRE AM 371 et 372 et IMCO AM 206 et 207) nécessite d'être étudié plus avant afin de veiller à un juste équilibre entre, d'un côté, la sécurité juridique et, de l'autre, la nécessité pour les autorités de contrôle d'exercer leurs pouvoirs de façon suffisamment flexible.

[13] L'IMI a été officiellement créé par le règlement (UE) nº 1024/2012 du Parlement européen et du Conseil du 25 octobre 2012 concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur et abrogeant la décision 2008/49/CE de la Commission, JO L 316 du 14.11.2012.

48. Enfin, le CEPD accueille favorablement les tentatives visant à assurer la **cohérence** du système de sanctions au niveau de l'UE, par exemple grâce au comité européen de la protection des données (par exemple en ayant recours à des orientations et à un échange d'informations concernant les sanctions imposées).

IX. CONCLUSIONS PRÉLIMINAIRES RELATIVES À LA DIRECTIVE[14]

1. Champ d'application

49. Comme cela a été expliqué en section II.1(a) ci-dessus, le CEPD accueille en théorie favorablement le fait que la proposition de directive s'appliquerait également aux institutions et organes de l'UE (LIBE AM 270 à 272) bien qu'il souhaite souligner que, compte tenu du cadre juridique et institutionnel particulier dans lequel ils évoluent, des clarifications supplémentaires non étudiées dans les propositions actuellement à l'étude sont nécessaires.

2. Principes de protection des données

50. Le CEPD relève que plusieurs amendements tentent de traiter de la question du traitement ultérieur des données pour une «**utilisation incompatible**». Le CEPD rappelle que toute dérogation au principe d'«utilisation compatible» ne devrait être autorisée que pour les finalités qui sont définies de façon claire et exhaustive et sous réserve de garanties appropriées. Dans ce contexte, il remarque que les amendements LIBE 66, 347 et 350 contiennent plusieurs éléments positifs qui pourraient servir de bonne base à développer. Comme cela a été mentionné ci-dessus (voir section III.1), le CEPD souhaiterait attirer l'attention sur l'avis du groupe de travail «Article 29» sur la limitation de la finalité qui doit être adopté dans les semaines à venir. Cet avis fournira de plus amples orientations et davantage de critères afin de générer une interprétation commune de la notion d'«utilisation compatible».

51. Le CEPD accueille favorablement les amendements qui renforcent l'obligation de faire la distinction entre les différentes catégories de personnes concernées et les différents degrés de précision et de fiabilité des données à caractère personnel (tels que LIBE AM 60 et 318 à 319). Ces obligations - qui sont spécifiques au secteur répressif - sont importantes aussi bien pour les personnes concernées que pour les autorités répressives. Des obligations comparables sont également prévues dans la législation de l'UE pour la coopération policière[15]. Dans ce contexte, les amendements LIBE 314 à 317, lesquels suppriment l'obligation de faire la distinction entre les catégories de personnes concernées, ne sont pas acceptables.

52. Le CEPD se félicite des amendements créant l'obligation pour les États membres de fournir des règles spécifiques quant aux conséquences de la catégorisation des personnes concernées (LIBE AM 330 et 331). Il accueille également favorablement l'amendement LIBE AM 351, lequel introduit des garanties spécifiques concernant

[14] Ces conclusions préliminaires sont basées sur les propositions d'amendements LIBE.
[15] Voir par exemple l'article 14, paragraphe 1, de la décision Europol.

les personnes «non suspectées» conformément aux recommandations émises par le groupe de travail «Article 29» dans son avis du 26 février[16].

3. Échange d'informations avec les parties privées

53. Le CEPD accueille favorablement l'intention de réglementer les échanges d'informations entre le secteur répressif et les parties privées en vue de clarifier - dans une certaine mesure - l'insécurité juridique concernant les situations dans lesquelles les activités du secteur privé et du secteur répressif entrent en interaction (par exemple lorsque les données sont collectées à des fins commerciales et ultérieurement utilisées à des fins d'application de la loi mais également lorsque les informations sont transférées par une autorité répressive à des parties privées ou à des autorités non répressives).

54. En ce qui concerne l'**accès par les autorités répressives à des données traitées à l'origine à des fins autres que l'application de la loi**, le CEPD remarque avec satisfaction que les amendements LIBE AM 58 et 310 introduisent des conditions et des garanties spécifiques concernant l'accès à ces données. Il estime toutefois que l'amendement LIBE AM 310, lequel exige uniquement une base juridique valable veillant à ce que la personne concernée dispose d'assurances suffisantes, est trop général et ne fournit pas les garanties nécessaires. Seul, cet amendement ne devrait donc pas être accepté.

55. Concernant la transmission, par les autorités répressives, de données à d'autres parties (à savoir des autorités non répressives et parties privées), le CEPD accueille favorablement l'intention de traiter cette question et l'introduction de conditions spécifiques régissant cette transmission (par exemple LIBE AM 162). Il souhaite toutefois attirer l'attention en particulier sur les amendements qui visent à réglementer les transferts à des autorités non répressives et à des parties privées en dehors de l'UE (LIBE AM 589 et 590) dans la mesure où le libellé de ces amendements amoindrit le degré de protection (voir ci-dessous «transfert de données à des tiers»).

4. Rôles et obligations du responsable du traitement

56. Le CEPD accueille favorablement les amendements qui introduisent des éléments essentiels du principe de responsabilité qui sont absents de la proposition de la Commission. En particulier, le CEPD accueille favorablement l'obligation pour le responsable du traitement d'*apporter la preuve* de la conformité (par exemple LIBE AM 480), d'effectuer une analyse de l'impact sur la protection des données (par exemple LIBE AM 27 et 28, 110 et 113) et de consulter l'autorité de protection des données avant le traitement de données à caractère personnel (par exemple LIBE AM 541 à 543). Il relève également avec satisfaction plusieurs amendements dans la mesure où ils renforcent le rôle et le statut du délégué à la protection des données (par exemple LIBE AM 120 à 123, 570, 573, 575, 576 et 578).

[16] Avis 01/2013 du 26 février 2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale.

5. Transfert de données à des tiers

57. Le CEPD accueille favorablement l'obligation que le responsable du traitement dans le pays tiers ou l'organisation internationale soit une autorité compétente aux fins d'application de la loi (LIBE AM 126, 584) tel que prévu dans les instruments juridiques existants dans le domaine de la coopération policière et judiciaire. En outre, il accueille également favorablement, en substance, les conditions supplémentaires qu'introduisent les amendements LIBE 126 et 591.

58. Il rappelle que **tout transfert à des autorités non répressives ou parties privées devrait être strictement limité et sous réserve de solides garanties**. Cela est d'autant plus important lorsque ces destinataires sont en dehors de l'UE. Comme cela a déjà été mentionné ci-dessus, les amendements LIBE 589 et 590, lesquels envisagent un tel transfert, ne fournissent pas de garanties suffisantes. En outre, ces amendements posent de sérieux problèmes dans la mesure où, d'après leur libellé actuel, il serait plus facile de transférer des données à des autorités non répressives ou à des parties privées qu'à des autorités répressives.

59. Enfin, dans son avis du 7 mars 2012, le CEPD critiquait le fait que la seule évaluation du responsable du traitement constitue un motif légal permettant d'autoriser les transferts vers un pays tiers et, dès lors, accueille favorablement les amendements proposant de supprimer cette possibilité (LIBE AM 33 et 602).

6. Pouvoirs des autorités de contrôle

60. Dans son avis, le CEPD insistait sur le fait que bien que quelques exceptions restreintes puissent être justifiées **en ce qui concerne les tribunaux dans l'exercice de leurs fonctions juridictionnelles**, il n'existe selon lui aucune raison de limiter les pouvoirs des autorités de contrôle hors de ce contexte particulier. Il accueille donc favorablement les amendements qui alignent les pouvoirs des autorités de contrôle envers les autorités répressives avec les pouvoirs définis dans la proposition de règlement (par exemple LIBE AM 142 à 645). Il accueille également favorablement les amendements LIBE 645 et 649 dans la mesure où ils tiennent compte des inquiétudes soulevées par le groupe de travail «Article 29» quant à la nécessité i) de s'assurer que toutes les autorités aient accès aux mêmes informations et ii) d'identifier les informations dont l'accès est permis[17].

7. Actes dans le domaine de la coopération policière et judiciaire en matière pénale

61. Dans son avis, le CEPD regrettait que les actes dans le domaine de la coopération policière et judiciaire en matière pénale n'aient pas été modifiés. Il soulignait que la période de deux ans mentionnée à l'article 61, paragraphe 2, de la proposition de directive dont la Commission dispose pour réexaminer ces actes entraînerait une période d'une durée inacceptable, durant laquelle la mosaïque actuelle, largement critiquée, resterait en vigueur. Ce faisant, l'amendement LIBE 671 qui supprime l'obligation d'un tel réexamen est inacceptable.

Bruxelles, le 15 mars 2013

[17] Avis 01/2013 du 26 février 2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale.