Avis du Contrôleur européen de la protection des données sur

la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI

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 le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[2],

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008[3] relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale,

A ADOPTÉ LE PRÉSENT AVIS:

I. INTRODUCTION

I.1. Contexte de l'avis

1. Le 27 mars 2013, la Commission a adopté la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI (ci-après la «proposition»). Le jour même, la Commission a transmis cette proposition pour consultation au CEPD, qui l'a reçue le 4 avril 2013.

[1] JO 1995, L 281/31.
[2] JO L8 du 12.1.2001, p. 1.
[3] JO L350 du 30.12.2008, p. 60.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
Courriel: edps@edps.europa.eu – Site interne: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax : 02-283 19 50

2. Avant l'adoption de la proposition, le CEPD a eu l'occasion de soumettre des observations informelles. Le CEPD se félicite du fait que nombre de ces observations ont été prises en considération.

3. Le CEPD se réjouit du fait qu'il ait été consulté par la Commission et qu'une référence à cette consultation soit mentionnée dans le préambule de la proposition.

4. Le CEPD a également été consulté sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions sur la création d'un programme européen de formation des services répressifs, adoptée en même temps que la proposition[4]. Il s'abstiendra cependant d'émettre une réaction séparée sur cette communication, étant donné que ses observations à cet égard sont très limitées et qu'elles sont mentionnées dans la partie IV du présent avis.

I.2. Objectif de la proposition

5. Cette proposition est fondée sur l'article 88 et sur l'article 87, paragraphe 2, point b), du traité sur le fonctionnement de l'Union européenne (TFUE) et vise à[5]:
   - mettre Europol en conformité avec les exigences du traité de Lisbonne, en définissant son cadre juridique en vertu de la procédure législative ordinaire;
   - atteindre les objectifs du programme de Stockholm en faisant d'Europol une plate-forme d'échange d'informations entre les autorités répressives des États membres et en créant des programmes européens de formation et d'échange à l'intention de tous les professionnels participant à des activités répressives;
   - conférer à Europol de nouvelles responsabilités, en reprenant les fonctions du CEPOL et en octroyant une base juridique au Centre européen de lutte contre la cybercriminalité;
   - assurer la solidité du régime de protection des données, en particulier en renforçant la structure de contrôle;
   - améliorer la gouvernance d'Europol dans un souci de plus grande efficacité et en l'alignant sur les principes fixés dans l'approche commune sur les agences décentralisées de l'Union européenne.

   Le CEPD souligne que la proposition est essentielle du point de vue du traitement des données à caractère personnel. Le traitement d'informations, comprenant des données à caractère personnel, est une des raisons principales de l'existence d'Europol. En l'état actuel du développement de l'Union européenne, l'orientation policière opérationnelle continue à relever de la compétence des États membres. Cependant, cette tâche revêt une nature transfrontalière croissante, et le niveau de l'Union européenne procure un appui en fournissant, échangeant et examinant des informations.

I.3. Objectif de l'avis

6. Le présent avis sera axé sur les modifications les plus significatives du cadre juridique d'Europol du point de vue de la protection des données. Il analysera en

[4] COM(2013) 172 final.
[5] Exposé des motifs, partie 3.

premier lieu le contexte juridique, son évolution et ses conséquences pour Europol. Il détaillera ensuite les principales modifications, qui sont les suivantes:

- la nouvelle structure d'information d'Europol, qui engendre une fusion des différentes bases de données et ses conséquences pour le principe de limitation;
- le renforcement du contrôle de la protection des données;
- le transfert et l'échange de données à caractère personnel et d'autres informations, en accordant une attention particulière à l'échange de données à caractère personnel avec les pays tiers.

7. Cet avis abordera ensuite un certain nombre de dispositions spécifiques de la proposition, en particulier son chapitre VII (articles 34 à 48) sur les garanties en matière de protection des données.

II. ANALYSE DU CONTEXTE JURIDIQUE

8. L'Office européen de police («Europol») était initialement un organe intergouvernemental régi par une convention[6], conclue entre les États membres, qui est entrée en vigueur le 1er octobre 1998. En 2009, la convention Europol a été remplacée par une décision du Conseil adoptée le 6 avril 2009[7]. En vertu de cette décision, Europol est financé par le budget communautaire et soumis au règlement financier et au statut des fonctionnaires de la Commission européenne, alignant ainsi Europol sur les autres organes et agences de l'Union européenne. Ce nouveau cadre juridique est entré en vigueur le 1er janvier 2010 lorsqu'Europol est devenu une agence de l'Union européenne.

Traité de Lisbonne et Europol

9. Le traité de Lisbonne, qui est entré en vigueur le 1er décembre 2009, a aboli la «structure en piliers» de la législation de l'Union européenne et a engendré la création d'Europol en vertu de l'article 88 du TFUE. Par conséquent, la base juridique d'Europol s'est vue modifiée et est passée de la procédure de consultation, soumise à l'unanimité au Conseil après consultation du Parlement européen, à la procédure législative ordinaire, caractérisée par le vote à la majorité qualifiée au Conseil et par le statut de colégislateur à part entière du Parlement européen. Par ailleurs, le traité de Lisbonne a transformé le domaine de la coopération policière et judiciaire en matière pénale (l'ancien troisième pilier) pour en faire le principal domaine du droit de l'Union européenne, ce qui conduira, par exemple, à la pleine juridiction de la Cour de justice de l'Union européenne.

10. À cet égard, le protocole sur les dispositions transitoires annexé au traité de Lisbonne[8] impose une période de transition de cinq ans avant que les instruments existants du troisième pilier, y compris la décision du Conseil relative à Europol, ne soient traités de la même manière que les instruments communautaires. L'article 10 de ce protocole prévoit que les effets juridiques de tous les actes adoptés avant

[6] Convention sur la base de l'article K.3 du traité sur l'Union européenne, portant création d'un office européen de police («convention Europol»), JO C 316 du 27.11.1995, p. 1.
[7] Décision du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) (ci-après la «décision du Conseil relative à Europol»), JO L 121 du 15.5.2009, p. 37.
[8] Protocole (n° 36) sur les dispositions transitoires, JO C115 du 9.5.2008, p. 322.

l'entrée en vigueur du traité de Lisbonne sont préservés aussi longtemps que ces actes n'auront pas été abrogés, annulés ou modifiés. En outre, les compétences étendues de la Cour de justice et la possibilité pour la Commission d'ouvrir des procédures d'infraction ne s'appliqueront pas à ces actes, aussi longtemps qu'ils n'auront pas été modifiés ou qu'une période de cinq ans ne se sera pas écoulée depuis l'entrée en vigueur du traité.

11. Le CEPD se félicite de la proposition. Elle met Europol en conformité avec les exigences de l'article 88, paragraphe 2, du TFUE. Le renforcement du rôle du Parlement européen en tant que colégislateur, l'extension du principe de la majorité qualifiée au Conseil ainsi que la pleine juridiction de la Cour de justice auront une incidence positive sur la qualité et la cohérence du cadre juridique, y compris les aspects essentiels relatifs à la protection des données à caractère personnel. Les règles générales relatives à la protection des données ainsi que les règles spécifiques qui pourraient être nécessaires pour des échanges particuliers de données bénéficieront de la pleine participation de toutes les institutions concernées de l'Union européenne.

Traité de Lisbonne et protection des données

12. L'entrée en vigueur du traité de Lisbonne a marqué le début d'une nouvelle ère pour la protection des données. L'article 6 du traité sur l'Union européenne (TUE), tel que modifié, donne un effet juridique contraignant à la Charte des droits fondamentaux de l'Union européenne[9]. L'article 8 de la Charte consacre le droit de toute personne à la protection des données à caractère personnel et expose ses différents éléments. Ce droit fondamental est aussi mentionné à l'article 16, paragraphe 1, du TFUE. En outre, l'article 16, paragraphe 2, du TFUE constitue une base juridique spécifique en vue d'une protection des données solide au sein de l'Union européenne dans toutes les politiques européennes, y compris dans le domaine de la coopération policière et judiciaire en matière pénale.

13. À cet égard, le 25 janvier 2012, la Commission a adopté un ensemble de mesures en vue de réformer le cadre juridique européen de la protection des données. Cet ensemble est composé d'une communication[10] et de deux propositions législatives (ci-après les «propositions sur la protection des données»): un règlement général sur la protection des données[11] (ci-après la «proposition de règlement sur la protection des données») et une directive spécifique dans le domaine de la police et de la justice[12] (ci-après la «proposition de directive sur la protection des données»).

14. Le CEPD a accueilli très positivement les propositions sur la protection des données, en particulier la proposition de règlement sur la protection des données qui

[9] Charte des droits fondamentaux de l'Union européenne, JO C 83 du 30.3.2010, p. 389.
[10] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions 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» COM(2012) 9 final.
[11] 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, COM(2012)11 final.
[12] Proposition de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012)10.

représente un grand pas en avant vers une protection des données plus efficace et plus cohérente au sein de l'Union européenne. Le CEPD a toutefois averti que les propositions sur la protection des données sont encore loin de constituer un ensemble complet de règles relatives à la protection des données aux niveaux national et européen dans tous les domaines d'action de l'Union européenne[13].

15. La nécessité d'une approche globale à l'égard de la révision du cadre européen de la protection des données avait été annoncée par la Commission dans sa communication de novembre 2010 intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne»[14]. Cette communication 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 plein et entier en faveur d'une approche globale[15]. Dans ses conclusions des 24 et 25 février 2011, le Conseil a lui aussi fait référence à un nouveau cadre juridique sur la base de l'approche globale[16].

16. L'avis du CEPD du 14 janvier 2011 a souligné l'importance d'un instrument juridique global pour la protection des données comprenant la coopération policière et judiciaire en matière pénale. Ce caractère global a été mis en évidence comme étant une *condition sine qua non* pour une protection des données efficace à l'avenir[17]. Le CEPD a mis en évidence le fait qu'il n'y a pas de différence fondamentale entre les autorités policières et judiciaires et les autres autorités des États membres chargées de l'application de la loi (fiscalité, douanes, anti-fraude, immigration) couvertes par la directive 95/46/CE. Il a également rappelé que la plupart des États membres ont doté d'un champ d'application large leur législation nationale mettant en œuvre la directive 95/46/CE et la convention 108 du Conseil de l'Europe[18] et qu'ils les appliquent aussi à leurs autorités policières et judiciaires.

17. Le CEPD a aussi largement privilégié l'inclusion du traitement au niveau européen, par les institutions, organes, offices et agences de l'Union européenne dans cet instrument juridique général. Un texte unique permettrait d'éviter tout risque de disparités entre les dispositions, entre différents instruments, et serait particulièrement adéquat pour l'échange de données entre le niveau européen et les entités publiques et privées des États membres.

18. La Commission a cependant adopté une approche différente. Premièrement, elle a choisi de réglementer la protection des données dans le domaine de l'application de la loi dans un instrument autonome (la proposition de directive sur la protection des

[13] Voir l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, JO C 192 du 30.6.2012, p. 7, section 1.2. Le texte intégral de cet avis est disponible sur le site internet du CEPD: http://www.edps.europa.eu.

[14] Communication du 4 novembre 2010 de la Commission au Parlement européen, au Conseil, au Comité économique et social, au Comité des régions intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», COM(2010) 609 final.

[15] Voir la résolution du Parlement européen du 6 juillet 2011, 2011/2025(INI).

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

[17] Voir l'avis du CEPD du 14 janvier 2011 sur la communication de la Commission intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», JO C 181/01 du 22.06.2011, p. 1, point 3.2.5.

[18] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28.1.1981.

données), ce qui n'est pas pleinement conforme au niveau de protection de la proposition de règlement sur la protection des données[19]. Deuxièmement, les règles relatives à la protection des données concernant les institutions, les organes et les agences de l'Union européenne fixées dans le règlement (CE) n° 45/2001 sont restées inchangées, tout comme les mesures spécifiques dans le domaine de la coopération policière et judiciaire en matière pénale, et elles ont été reportées à une phase ultérieure.

Conséquences pour Europol

19. Au niveau de l'Union européenne, à la suite de l'entrée en vigueur du traité de Lisbonne, le règlement (CE) n° 45/2001 s'applique au traitement des données à caractère personnel par toutes les institutions, organes, offices et agences de l'Union européenne dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit européen, sauf si le droit européen a prévu clairement et précisément d'autres dispositions.

20. Il a été soutenu qu'en vertu du cadre juridique en vigueur, l'existence de règles spécifiques relatives à la protection des données aurait comme conséquence que le règlement (CE) n° 45/2001 ne s'appliquerait pas à Europol, en tout état de cause pas à ses principales activités. Dans le cadre du présent avis, il n'est pas nécessaire de mettre en question cet argument.

21. Cependant, malgré le fait que le régime spécifique en vigueur relatif à Europol semblerait ne se rapporter qu'aux activités principales d'Europol, le statut des données relatives au personnel administratif d'Europol fait débat. Le CEPD se félicite dès lors de la proposition visant à préciser le fait que le règlement (CE) n° 45/2001 devrait s'appliquer à ces données[20].

22. Le traitement des données à caractère personnel par Europol aux fins de ses activités principales (à savoir appuyer et renforcer l'action des États membres dans la lutte contre les crimes graves) est abordé différemment. Dans la proposition, la Commission a choisi d'opter pour un régime autonome relatif à la protection des données, fondé sur l'hypothèse selon laquelle le règlement (CE) n° 45/2001 ne s'applique pas à Europol. Le CEPD regrette le fait que la Commission n'ait pas choisi d'appliquer le règlement (CE) n° 45/2001 à Europol et de limiter la proposition à des règles spécifiques et des dérogations supplémentaires, qui tiennent dûment compte des spécificités du secteur des services répressifs.

23. Cependant, le CEPD note que le considérant 32 de la proposition mentionne expressément le fait que les règles relatives à la protection des données au niveau d'Europol devraient être renforcées et se fonder sur les principes du règlement (CE) n° 45/2001. Par conséquent, la proposition reprend la plupart des éléments essentiels du règlement (CE) n° 45/2001.

[19] Dans son avis du 7 mars 2012 (point 20), le CEPD a même indiqué que le niveau de protection fourni par la proposition de directive sur la protection des données est très inférieur à celui de la proposition de règlement (voir aussi les points 309 et 310).
[20] Le règlement (CE) n° 45/2001 s'applique déjà à toutes les activités du CEPOL.

24. Le considérant 32 précise aussi que les règles relatives à la protection des données au niveau d'Europol devraient être alignées sur les autres instruments pertinents de la protection des données applicables dans le domaine de la coopération policière au sein de l'Union, en particulier la convention 108 et la recommandation n° R(87)15 du Conseil de l'Europe[21] ainsi que la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[22]. Le CEPD rappelle que ni la convention 108, ni la décision-cadre du Conseil ne s'appliquent à Europol, mais qu'il soutient, bien entendu, l'intention de veiller à ce que la protection apportée par ces instruments dans les États membres soit respectée par Europol.

Réforme de la protection des données

25. Comme mentionné précédemment, le caractère complet est l'une des principales raisons et l'un des principaux buts de la réforme de la protection des données. Précédemment, le CEPD a demandé qu'un instrument unique complet incluant la police et la justice soit adopté. Un tel instrument pourrait permettre de se doter de règles spécifiques supplémentaires prenant dûment en considération les spécificités du domaine de la police et de la justice, conformément à la déclaration 21 annexée au traité de Lisbonne. Il convient d'éviter la prolifération de différents régimes s'appliquant, par exemple, à Europol, à Eurojust, au SIS et à Prüm.

26. Le CEPD recommande dès lors de préciser dans les considérants de la proposition que le nouveau cadre de la protection des données des institutions et des organes de l'Union européenne devrait s'appliquer à Europol dès son adoption. En outre, l'application à Europol du régime de protection des données des institutions et organes de l'Union européenne devrait être clarifiée dans l'instrument remplaçant le règlement (CE) n° 45/2001, comme annoncé pour la première fois en 2010, dans le cadre de la révision du train de mesures sur la protection des données[23].

27. Le considérant 32 de la proposition mentionne que les règles relatives à la protection des données d'Europol devraient être autonomes et alignées sur les autres instruments pertinents relatifs à la protection des données applicables dans le domaine de la coopération policière au sein de l'Union, y compris la décision-cadre 2008/977/JAI, et précise que cette décision sera remplacée par la directive pertinente en vigueur lors de son adoption. Le CEPD attire l'attention sur le fait que la décision du Conseil relative à Europol fournit un régime solide de protection des données et considère que ce niveau ne devrait pas être abaissé, indépendamment des discussions sur la proposition de directive relative à la protection des données. Il convient de préciser ces points dans le préambule.

28. Enfin, au plus tard à partir de l'application du nouveau cadre général, les principaux nouveaux éléments de la réforme de la protection des données (à savoir le principe

[21] Recommandation n° R(87) 15 du Comité des ministres du Conseil de l'Europe aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, du 17.9.1987.

[22] Décision-cadre 2008/977/JAI 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 L 350 du 30.8.2008, p. 60.

[23] Communication de la Commission intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», COM(2010)609 final, p. 18 et 19.

de responsabilité, l'analyse d'impact relative à la protection des données, la prise en compte du respect de la vie privée dès la conception et la protection de la vie privée par défaut et la notification de violation de données à caractère personnel) devraient aussi s'appliquer à Europol. Il convient de mentionner également ce point dans le préambule. Comme nous le développerons ci-dessous, ces éléments sont actuellement absents de la proposition ou ne sont pas suffisamment pris en considération.

III. ANALYSE DE LA PROPOSITION

OBSERVATIONS GÉNÉRALES

29. Le rôle d'Europol est d'appuyer les autorités répressives nationales et leur coopération mutuelle dans la prévention de la criminalité organisée, du terrorisme et d'autres formes graves de criminalité affectant deux États membres ou plus et dans la lutte contre ces phénomènes[24]. L'assistance offerte par Europol aux autorités répressives nationales englobe la facilitation des échanges d'informations, la fourniture d'analyses criminelles ainsi que l'aide et la coordination en matière d'opérations transfrontalières. Afin de remplir ces tâches, les activités principales d'Europol consistent à rassembler, analyser et diffuser les informations, y compris, dans une large mesure, les données à caractère personnel.

30. Un cadre solide de la protection des données n'est pas seulement important pour les personnes concernées, mais il contribue aussi au succès de la coopération policière et judiciaire en elle-même. Un tel cadre est à la base de la confiance des États membres qui fournissent les informations en matière policière et judiciaire. Les données à caractère personnel concernées sont très souvent sensibles et ont été obtenues par les autorités policières et judiciaires à la suite d'une enquête menée sur des personnes. L'un des problèmes soulevés dans l'analyse d'impact est que les États membres ne fournissent pas suffisamment d'informations à Europol. Cette tendance à ne pas partager les informations s'explique, entre autres, par la culture policière qui encourage les agents des services répressifs à être prudents à cet égard. Un régime solide de protection des données devrait contribuer à améliorer la confiance entre États membres, condition d'un échange d'informations fructueux. Des objectifs clairs, accompagnés de règles spécifiques et strictes, permettraient de faire accepter plus facilement aux États membres les échanges d'informations à caractère personnel. Enfin, veiller au respect des principes de la protection des données permettrait d'assurer ultérieurement qu'Europol opère en respectant l'état de droit, ce qui renforcera la confiance dans son comportement et favorisera dès lors un sentiment de confiance diffus dans les institutions de l'Union européenne.

31. La Commission a, à plusieurs reprises, souligné l'importance qu'il y a de renforcer la protection des données dans le contexte de la répression et de la prévention de la criminalité, dans lequel l'échange et l'utilisation des informations à caractère personnel augmentent considérablement[25]. En outre, le programme de Stockholm, approuvé par le Conseil européen, présente un dispositif renforcé de protection des

[24] Article 3 de la décision du Conseil relative à Europol.

[25] Voir la communication du 20.7.2010 de la Commission au Parlement européen et au Conseil – «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice», COM(2010) 385 final.

données comme étant la condition essentielle à la stratégie européenne en matière de gestion de l'information dans ce domaine[26].

32. Il est dès lors extrêmement important que la proposition garantisse un niveau élevé de protection des données, du moins aussi élevé que celui qui résulte du cadre en vigueur.

a) Europol: une nouvelle structure des informations

33. La décision du Conseil relative à Europol contient des dispositions détaillées sur la protection des données, qui sont complétées par un ensemble de règles d'application comme les actes du Conseil sur les règles applicables aux fichiers de travail à des fins d'analyse[27], les règles régissant les relations d'Europol avec ses partenaires[28], les règles relatives à la confidentialité[29] et les conditions relatives au traitement des données afin de déterminer si celles-ci sont utiles aux missions d'Europol[30].

34. En vertu de la décision du Conseil relative à Europol, Europol traite des informations, y compris des données à caractère personnel, principalement dans deux systèmes: le système d'information Europol («SIE») et les fichiers de travail à des fins d'analyse[31]. Ces systèmes sont techniquement et juridiquement distincts et caractérisés par des règles spécifiques quant à leurs objectifs et à leurs droits d'accès. Par conséquent, Europol n'est autorisé ni à relier ni à analyser des données réparties dans les différentes bases de données de ces systèmes. Par ailleurs, il n'est pas possible pour Europol de s'écarter de l'architecture spécifique prédéfinie.

35. La proposition vise à accroître la flexibilité, à autoriser Europol à concevoir graduellement une architecture qui s'adapterait aux besoins futurs nécessitant l'établissement de solutions innovantes de traitement des données. À cette fin, la proposition supprime les règles générales régissant les différents systèmes et est axée sur les finalités pour lesquelles les données ont été fournies plutôt que sur les fichiers prédéfinis[32].

36. En vertu de l'article 24 de la proposition, Europol est autorisé à traiter des informations aux fins suivantes: a) vérification croisée visant à identifier les connexions entre les informations; b) analyse de nature stratégique ou thématique; et

[26] Le programme de Stockholm - Une Europe ouverte et sûre qui sert et protège les citoyens (2010/C115/01), JO C 115, p. 1.
[27] Décision 2009/936/JAI du Conseil du 30 novembre 2009 portant adoption des règles d'application relatives aux fichiers de travail à des fins d'analyse Europol, JO L 325 du 11.12.2009, p. 14.
[28] Décision 2009/934/JAI du Conseil 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 du 11.12.2009, p. 6. Voir aussi la décision 2009/935/JAI du Conseil du 30 novembre 2009 établissant la liste des États et organisations tiers avec lesquels Europol conclut des accords, JO L 325,du 11.12.2009, p. 12.
[29] Décision 2009/968/JAI du 30 novembre 2009 portant adoption des règles relatives à la confidentialité des informations d'Europol, JO L 332 du 17.12.2009, p. 17.
[30] Décision du conseil d'administration d'Europol du 4 juin 2009 sur les conditions relatives au traitement des données sur la base de l'article 10, paragraphe 4, de la décision Europol, JO L 348 du 29.12.2009, p. 1.
[31] Article 10 de la décision du Conseil relative à Europol.
[32] Voir le considérant 20 de la proposition. Voir également les p. 23 et 24 de l'analyse d'impact.

c) analyse opérationnelle dans des cas spécifiques. Ni la proposition ni aucun des documents d'accompagnement ne précisent ces fins.

L'architecture actuelle des informations

37. Afin que les modifications soient compréhensibles, le CEPD décrira brièvement ci-dessous les principaux éléments du système actuel ainsi que son fonctionnement concret. Cette description montrera que la décision du Conseil relative à Europol fournit déjà une flexibilité significative.

38. Le SIE est une base de données de référence utilisée à des fins de vérification croisée: il permet aux États membres de partager et de rechercher des informations relatives à des personnes, des événements et des dispositifs liés à une affaire pénale. Les données stockées dans le SIE sont relatives aux personnes soupçonnées, aux personnes condamnées ou aux personnes pour lesquelles il existe des indices concrets ou des bonnes raisons de croire qu'elles ont commis ou commettront des infractions relevant de la compétence d'Europol. La décision du Conseil relative à Europol comporte une liste exhaustive des types de données qui sont susceptibles d'être stockées dans le SIE, les délais de conservation et les règles relatives à l'accès aux données stockées dans le SIE et à leur utilisation[33].

39. Contrairement au SIE, les fichiers de travail à des fins d'analyse visent à analyser des formes spécifiques de criminalité. Les données stockées dans les fichiers de travail à des fins d'analyse peuvent avoir trait aux suspects, mais aussi aux témoins, aux victimes, aux personnes servant de contacts ou d'accompagnateurs et aux informateurs[34]. Les catégories de données pouvant être stockées dans les fichiers de travail à des fins d'analyse sont plus larges qu'en ce qui concerne le SIE[35]. Cependant, des règles supplémentaires relatives à la protection des données s'appliquent aux fichiers de travail à des fins d'analyse. Avant d'être créé, chaque fichier de travail à des fins d'analyse fait l'objet d'une instruction de création. L'instruction de création doit préciser l'objet du fichier, les personnes sur lesquelles des données peuvent être stockées et le type de données. En vertu de l'article 16, paragraphe 1, de la décision du Conseil relative à Europol, l'instruction de création doit aussi décrire le contexte général donnant lieu à la décision de créer le fichier, les conditions et les procédures relatives à la communication des données à certains destinataires ainsi que la durée pendant laquelle elles sont stockées[36].

[33] Voir les articles 12, 13 et 20.

[34] Article 14 de la décision du Conseil relative à Europol. Voir aussi la décision 2009/936/JAI du Conseil du 30 novembre 2009 portant adoption des règles d'application relatives aux fichiers de travail à des fins d'analyse Europol, JO L 325 du 11.12.2009, p. 14.

[35] Article 6 de la décision 2009/936/JAI du Conseil du 30 novembre 2009 portant adoption des règles d'application relatives aux fichiers de travail à des fins d'analyse Europol, JO L 325 du 11.12.2009, p. 14.

[36] Pour être complet, l'article 10, paragraphe 2, de la décision du Conseil relative à Europol autorise aussi Europol à créer de nouveaux systèmes traitant des données à caractère personnel. Cependant, ces nouveaux systèmes ne peuvent pas traiter des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, ni les données à caractère personnel concernant la santé ou la sexualité. Toutefois, la possibilité de créer de nouveaux systèmes n'a pas été utilisée, et ce pour les deux raisons principales suivantes: l'absence de besoin opérationnel et les restrictions relatives au stockage d'informations sensibles à caractère personnel (voir, sur ce point, *Evaluation of the Implementation of the Europol Council Decision*

40. Jusqu'en 2010, il existait 23 fichiers de travail à des fins d'analyse, ce qui signifiait qu'il existait 23 bases de données différentes non reliées entre elles, traitant chacune d'un type spécifique de criminalité organisée. Fin 2010, le système des fichiers de travail à des fins d'analyse a été réorganisé et rendu plus flexible. Il permet désormais aux analystes d'Europol d'avoir accès aux informations pertinentes traitées dans les autres fichiers de travail à des fins d'analyse. Les 23 fichiers de travail à des fins d'analyse existants ont été fusionnés en deux fichiers de travail à des fins d'analyse. Le premier traite des crimes graves et de la criminalité organisée; l'autre de la lutte contre le terrorisme. En conséquence de cette fusion, les finalités des deux fichiers de travail à des fins d'analyse sont larges et suscitent des préoccupations en ce qui concerne les principes de finalité requis par l'article 16, paragraphe 2, point d), de la décision du Conseil relative à Europol. Dès lors, au sein de chacun des deux fichiers de travail à des fins d'analyse, des points de référence[37] et/ou des groupes cibles[38] ont été créés, chacun définissant une finalité spécifique pour les données qu'il traitera. La finalité spécifique, ainsi que le type de données et les personnes sur lesquelles des données peuvent être stockées au niveau du point de référence ou du groupe cible, sont précisés dans les annexes de l'instruction de création du fichier de travail à des fins d'analyse.

41. En vertu de ce nouveau concept lié aux fichiers de travail à des fins d'analyse, les groupes d'analystes d'Europol ont accès à toutes les informations traitées dans les fichiers de travail à des fins d'analyse qui leur sont confiés. Ils peuvent utiliser les autres informations auxquelles ils ont accès uniquement à condition i) d'établir un lien clair avec la finalité du point de référence ou du groupe cible dont ils sont en charge; et que ii) seules les données nécessaires soient ensuite traitées au sein du point de référence ou du groupe cible.

42. Cette flexibilité permettrait, par exemple, de détecter des liens entre des enquêtes et des *modus operandi* communs parmi différentes organisations criminelles[39]. La criminalité organisée aujourd'hui est très différente de ce qu'elle était à l'époque où Europol a été créé. Le développement du marché intérieur, l'abolition postérieure des frontières, ainsi que les avantages offerts par la mondialisation et les innovations technologiques ont ouvert des perspectives d'engendrer de nouveaux profits pour les organisations criminelles existantes et émergentes. Les organisations criminelles sont plus sophistiquées et dynamiques. Elles ne sont plus axées sur des crimes spécifiques, mais commettent des infractions variées et en plein essor, passant d'une activité à une autre, et ajoutant de nouvelles activités à celles dans lesquelles elles sont déjà spécialisées. Par ailleurs, les organisations criminelles ne sont plus confinées à des zones géographiques et coopèrent très souvent avec d'autres organisations différentes de la criminalité organisée. La diversité tant des infractions pénales que de la composition des organisations criminelles exige une approche différente.

---

and of Europol activities, rapport technique, p. 80 et 81, disponible (en anglais) sur le site internet d'Europol).

[37] À savoir, un domaine qui se concentre sur un phénomène particulier, du point de vue d'un produit ou d'un angle thématique ou régional (par exemple, l'exploitation des enfants, le trafic de drogues dans les Balkans occidentaux, etc. Analyse d'impact, p. 33.

[38] À savoir un projet opérationnel doté d'une équipe d'Europol en vue d'appuyer une enquête pénale internationale ou une opération de renseignements en matière pénale contre une cible spécifique (par exemple, un groupe identifié de criminels; une organisation criminelle originaire du Kosovo, etc.). Analyse d'impact, p. 33.

[39] Voir l'analyse d'impact, p. 14 («Aspect 1 du problème»).

Évaluation du CEPD

43. Le CEPD comprend la nécessité de la flexibilité en raison de l'évolution du contexte, ainsi qu'à la lumière des rôles accrus d'Europol, qui se développera davantage en tant que plate-forme pour l'échange d'information entre les autorités répressives des États membres, et qui se verra aussi attribuer des tâches indépendantes en matière de traitement des informations. Dans cette perspective, Europol doit être en mesure de remplir ses rôles de la manière la plus efficace. L'architecture existante en matière d'information ne constitue pas nécessairement la référence pour l'avenir. Le CEPD évaluera dès lors le nouveau système en fonction de ses propres avantages et non en fonction de la nécessité de modifier le système en vigueur.

44. Le CEPD tient à souligner que c'est aux législateurs de fixer les principaux éléments de la structure d'information d'Europol. Dans son rôle en tant que conseiller auprès des législateurs, il se concentre sur la question de savoir dans quelle mesure le choix des législateurs est limité par – et le cas échéant selon – les principes de la protection des données. Dans ce contexte, cela signifie une évaluation du niveau de protection accordé à la personne concernée à la lumière du principe de la limitation des finalités, tel qu'appliqué dans le domaine de la coopération policière. Sur la base de cette évaluation, le CEPD proposera d'introduire des garanties supplémentaires à l'approche de l'article 24 de la proposition.

Limitation des finalités

45. Le CEPD rappelle que la limitation des finalités est un principe clé de la protection des données, reconnu par l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Il s'agit à la fois d'une condition essentielle du traitement et d'une condition préalable pour les autres exigences relatives à la qualité des données. La limitation des finalités contribue à la transparence, à la sécurité juridique et à la prévisibilité. Ce principe vise à protéger les personnes concernées, grâce à la fixation de limites relatives à la manière dont les responsables du traitement peuvent utiliser leurs données. Cela est d'autant plus important dans le domaine de la coopération policière et judiciaire en matière pénale, car les personnes concernées ne savent habituellement pas quand a lieu le traitement des données les concernant.

46. Une finalité spécifiée signifie que les traitements inclus et non inclus dans la finalité sont fixés, de manière précise et complète[40]. Elle déterminera les données pertinentes à collecter, les périodes de conservation ainsi que tous les autres aspects clés de la manière dont les données à caractère personnel seront traitées en vue de la(des) finalité(s) choisie(s).

Conséquences pour l'article 24

[40] Voir l'avis 03/2013 du 2.4.2013 du groupe de travail «Article 29» sur la protection des données sur la limitation des finalités, 39 Section II.2.1., disponible (en anglais) sur le site internet du groupe de travail article 29 à l'adresse suivante:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

47. Le CEPD formule les observations suivantes sur l'article 24 de la proposition, à la lumière du principe de la limitation des finalités:

- l'article 24, paragraphe 1, point a), autorise la vérification croisée des données visant à identifier les liens entre les informations. Le CEPD se félicite du fait que l'article 24, paragraphe 2, et l'annexe 2 limitent la vérification croisée aux données relatives aux i) personnes qui sont soupçonnées d'avoir commis une infraction ou participé à une infraction relevant de la compétence d'Europol, ou qui ont été condamnées pour une telle infraction, et aux ii) personnes pour lesquelles il existe des indices concrets ou de bonnes raisons de croire qu'elles commettront des infractions;

- en vertu de l'article 24, paragraphe 1, point b), les données à caractère personnel relatives aux personnes soupçonnées, mais aussi aux témoins, aux victimes, aux personnes servant de contacts ou d'accompagnateurs pourraient être traitées aux fins de l'analyse stratégique ou thématique. Si l'article 24, paragraphe 1, point b), vise à mentionner l'analyse actuelle des tendances générales et l'évaluation de la menace que représente la criminalité organisée,[41] le CEPD estime que les données à caractère personnel ne sont pas requises. Il recommande de définir dans la proposition les notions d'analyse stratégique, thématique et opérationnelle et de supprimer la possibilité de traiter les données à caractère personnel aux fins de l'analyse stratégique ou thématique, à moins qu'une justification solide soit donnée;

- l'article 24, paragraphe 1, point c), de la proposition prévoit qu'Europol peut traiter des informations aux fins de l'analyse opérationnelle dans des cas spécifiques. Cette disposition n'exige pas la définition d'une finalité spécifique pour ces cas ni n'exige de ne traiter que les données à caractère personnel pertinentes pour chacune des finalités spécifiques. Or, l'article 16 de la décision du Conseil relative à Europol prévoit que, pour chaque fichier de travail à des fins d'analyse, une finalité spécifique et les catégories des données à traiter sont décrites dans l'instruction de création. Le principe de finalité a été mis en œuvre par l'intermédiaire des concepts de points de référence et de groupes cibles. Le CEPD recommande dès lors d'inclure une limitation des finalités fondée sur l'expérience de la présente décision du Conseil relative à Europol. Il recommande fortement de définir clairement une finalité spécifique pour chaque cas d'analyse opérationnelle et d'exiger que seules les données à caractère personnel pertinentes soient traitées conformément à la finalité spécifique définie. L'article 24, paragraphe 1, point c), doit être modifié en conséquence.

48. En outre, en ce qui concerne l'article 24, paragraphe 1, point c), de la proposition, le CEPD comprend qu'en raison des activités principales d'Europol (à savoir accroître le volume d'informations fournies par les États membres afin de fournir des connaissances supplémentaires sur les activités criminelles), la diversité des infractions pénales et la composition des organisations criminelles[42], il est nécessaire qu'Europol effectue une vérification croisée des données reçues dans le cadre de l'analyse opérationnelle. Le CEPD rappelle qu'en vertu du principe de finalité, les données à caractère personnel ne peuvent être traitées d'une manière

[41] Voir le compte-rendu d'Europol, Rapport général sur les activités d'Europol, disponible sur le site internet d'Europol.
[42] Voir le point 42 plus haut.

incompatible avec les finalités pour lesquelles elles ont été collectées (article 34, point b), de la proposition). Il convient d'examiner la compatibilité au cas par cas en tenant compte de toutes les circonstances pertinentes, y compris la relation entre les finalités, le contexte de la collecte et les garanties appliquées par le responsable du traitement[43].

49. Il convient d'ajouter que, dans le domaine de la répression, le traitement ultérieur de données à des fins considérées incompatibles avec la finalité initiale pourrait être autorisé lorsqu'il est strictement nécessaire, dans un cas spécifique. Étant donné que ce traitement pourrait porter atteinte à la vie privée, il convient d'assortir ce type de traitements de conditions très strictes.[44]

50. Le CEPD considère dès lors que la vérification croisée des données collectées à des fins différentes par les analystes d'Europol exige des garanties spécifiques. Il recommande donc d'ajouter dans la proposition les éléments suivants: i) toutes les opérations de vérification croisée par les analystes d'Europol sont expressément motivées; ii) l'extraction de données à la suite d'une consultation est limitée au strict minimum requis et est expressément motivée; iii) la traçabilité de toutes les opérations liées aux vérifications croisées est garantie; et iv) seul le personnel autorisé responsable de la finalité pour laquelle les données ont initialement été collectées peut modifier ces données. Ces éléments seraient conformes à la pratique actuelle au sein d'Europol.

51. Le CEPD considère que les recommandations ci-dessus sont essentielles en vue de garantir un niveau de protection des données au moins aussi élevé que celui figurant dans la décision du Conseil relative à Europol.

b) Renforcement du contrôle de la protection des données

Remarques préliminaires

52. Le CEPD salue les dispositions relatives au contrôle qui prévoient une architecture solide en matière de contrôle sur le traitement des données. Ces dispositions prennent dûment en considération les responsabilités au niveau national et au niveau de l'Union européenne et établissent un système en vue de coordonner toutes les autorités participant à la protection des données, sur la base de l'expérience et des mécanismes existants et éprouvés. Dans cette partie, les observations du CEPD visent à renforcer davantage ces mécanismes.

53. Le renforcement des mécanismes de contrôle est nécessaire à la lumière des rôles accrus d'Europol. Les pouvoirs étendus d'Europol prévoient une évolution claire des activités de traitement des données, y compris les informations traitées au niveau de l'Union européenne qui ne proviennent pas directement des autorités

[43] Voir l'avis 03/2013 du 2.4.2013 du groupe de travail article 29 sur la protection des données sur la limitation des finalités, 39 Section II.2.1., disponible (en anglais) sur le site internet du groupe de travail «Article 29» à l'adresse suivante:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion.

[44] Avis du CEPD du 19 décembre 2005 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 (COM (2005)475 final), JO C 47 du 25.2.2006, p. 27.

nationales. En outre, Europol est désormais un organe de l'Union européenne: il devra être pleinement aligné sur les autres agences de l'Union européenne et ses activités relèveront de la juridiction de la Cour de justice de l'Union européenne.

54. Dans ce contexte, le CEPD salue la reconnaissance, dans la proposition, de son rôle en tant qu'autorité créée pour contrôler toutes les institutions et tous les organes de l'Union européenne. Par conséquent, l'article 46 attribue au CEPD la responsabilité de contrôler Europol, y compris le rôle de conseiller d'Europol et des personnes concernées sur toutes les questions relatives au traitement des données. Cette responsabilité garantira une approche cohérente et efficace du contrôle au niveau de l'Union européenne.

55. À cet égard, l'article 45 de la proposition reconnaît que le contrôle des traitements prévu dans la proposition est une tâche qui nécessite aussi la participation active des autorités nationales de protection des données[45]. La coopération entre le CEPD et les autorités nationales de contrôle est essentielle en vue du contrôle efficace dans ce domaine. L'article 47 s'appuie dès lors sur la structure existante de coopération dans les domaines pertinents du droit européen, comme le système d'information Schengen (2e génération), Eurodac et le système d'information sur les visas. L'expérience montre que ces structures sont efficaces parce qu'elles encouragent une coopération étroite entre les autorités nationales de contrôle et le CEPD. Cette coopération sera même plus importante dans le cas présent parce que le contrôle du traitement par le CEPD ne sera pas uniquement axé sur l'infrastructure technique[46], mais aussi sur la substance des données.

56. En effet, le CEPD estime que les dispositions sur le contrôle et la coopération lors du contrôle pourraient bien constituer un modèle pour la proposition de la Commission sur la protection des données au niveau de l'Union européenne annoncée dans la réforme sur la protection des données[47].

57. Enfin, le CEPD salue l'article 48 de la proposition, qui prévoit que le règlement (CE) n° 45/2001, y compris les dispositions sur le contrôle, s'applique entièrement aux données administratives et concernant le personnel.

a) Contrôle efficace d'Europol

58. Étant donné ses activités, Europol a besoin d'un contrôle efficace en matière d'indépendance, d'expertise et d'outils répressifs.

59. Un contrôle indépendant et efficace est un élément essentiel de la protection des personnes en ce qui concerne le traitement des données à caractère personnel aux niveaux national et européen, consacré à l'article 8 de la Charte des droits fondamentaux et à l'article 16 du TFUE. La Cour de justice a reconnu que le CEPD remplit tous les critères d'indépendance établis par la Cour en ce qui concerne les

[45] Voir aussi la résolution n° 4 de la conférence de printemps des autorités européennes de protection des données (Lisbonne, 16 et 17 mai 2013).
[46] C'est le cas pour les systèmes d'information mentionnés ci-dessus.
[47] Voir la communication de la Commission intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», COM(2010)609 final, p. 18 et 19, et le point 15 ci-dessus.

autorités de contrôle de la protection des données et a en effet cité le CEPD comme référence à cet égard[48].

60. Par ailleurs, après le terme de la période transitoire en vertu de l'article 10 du protocole n° 36 du traité de Lisbonne[49], toute personne physique ou morale pourra intenter un recours juridictionnel devant la Cour de justice contre des actes d'Europol, y compris en matière de protection des données[50]. Le même cadre judiciaire devrait s'appliquer à toute décision adoptée par l'autorité de contrôle d'Europol, comme c'est également le cas pour le CEPD[51].

61. La proposition accorde de larges pouvoirs d'enquête et d'exécution au CEPD, allant de la fourniture de conseils à la formulation d'avertissements et à l'imposition d'interdictions du traitement (voir les points 68 et 69 ci-dessous), ce qui garantira un contrôle renforcé et efficace d'Europol[52].

b) Rôle des autorités nationales de protection des données

62. Le CEPD salue l'article 45 de la proposition. Cet article indique que le traitement de données par les autorités nationales ainsi que la manière dont elles interagissent avec Europol sont soumis à un contrôle au niveau national, ce qui reflète dès lors le rôle clé des autorités nationales de contrôle. Il salue également l'accent mis sur l'étroite coopération, ainsi que l'exigence selon laquelle les autorités nationales de contrôle devraient tenir le CEPD informé de toute action prise à l'égard d'Europol.

c) Une protection des données rationnelle et cohérente au niveau de l'Union européenne

63. À la suite de l'entrée en vigueur du traité de Lisbonne, le domaine de la coopération policière et judiciaire a perdu son statut intergouvernemental distinct et s'est inscrit dans le cadre de la méthode communautaire. Europol, en tant qu'un des «organes de l'ancien troisième pilier», est devenu une agence de l'Union européenne. Dès lors, en ce qui concerne le contrôle de la protection des données, Europol devrait être traité de la même manière que les autres entités de l'Union européenne, dont certaines traitent aussi des données relatives à la répression (OLAF, Frontex et EU Lisa, la nouvelle agence IT jouant un rôle clé dans la gestion des systèmes d'information à grande échelle).

---

[48] Voir l'affaire 518/07, Commission contre Allemagne, point 30: «(...) *les autorités de contrôle* (...) *doivent jouir d'une indépendance qui leur permette d'exercer leurs missions sans influence extérieure*. *Cette indépendance exclut non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte, qui pourraient remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel*»), et l'affaire 614/10, Commission contre Autriche (point 43: «*l'indépendance requise* (...) *vise à exclure non seulement l'influence directe, sous forme d'instructions, mais également,* (...) *toute forme d'influence indirecte susceptible d'orienter les décisions de l'autorité de contrôle*»).

[49] Au 1er décembre 2014.

[50] Voir le considérant 46 et l'article 52 de la proposition. Voir l'exposé des motifs, p. 9.

[51] Voir l'article 32, paragraphe 3, du règlement (CE) n° 45/2001 et l'article 50 de la proposition.

[52] Voir également l'exposé des motifs, p. 8.

64. Par ailleurs, la nature du traitement effectué par Europol est significative. Europol ne se contente pas de stocker des données provenant des États membres, mais traite aussi activement des données dont la finalité est la réalisation de ses propres activités et utilise d'autres données qui ne proviennent pas des autorités nationales, mais d'autres sources interagissant directement avec Europol (autres organes de l'Union européenne, tiers en dehors de l'Union européenne, etc.). Le traitement effectué par Europol lui-même au niveau de l'Union européenne devrait dès lors être contrôlé invariablement au niveau de l'Union européenne.

65. Enfin, compte tenu du fait qu'Europol échange des données avec les autres organes de l'Union européenne, il est nécessaire de garantir la cohérence et un niveau de protection égal du traitement des données par ces autres organes. Il convient dès lors que ces entités de l'Union européenne soient soumises au même système harmonisé et cohérent de contrôle global.

4) Contrôle par le CEPD

66. À la lumière de ce qui précède, l'article 46 prévoit un contrôle rationnel et cohérent de la protection des données au niveau européen par le CEPD. Le CEPD contrôle la soixantaine d'autres institutions, organes et agences actifs dans l'ensemble des politiques de l'Union européenne et possède une solide expérience dans le contrôle des organes et agences de l'Union européenne qui traitent des données dans le domaine de la répression, comme Frontex et l'OLAF.

67. Le CEPD salue le considérant 32 de la proposition, qui indique que les règles relatives à la protection des données au niveau d'Europol devraient être renforcées et se fonder sur les principes du règlement (CE) n° 45/2001, et l'article 46 de la proposition, qui accorde au CEPD des obligations et des pouvoirs similaires à ceux qui lui sont accordés par le règlement (CE) n° 45/2001.

68. À cet égard, le CEPD exerce son rôle de contrôle au moyen de différents outils, comme les contrôles préalables, les consultations, les traitements des réclamations, les visites et les inspections[53]. Le CEPD a le pouvoir d'obtenir l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à ses enquêtes et d'obtenir l'accès à tout local dans lequel l'organe de l'Union européenne mène ses activités[54]. Si nécessaire, le CEPD peut avoir recours à un certain nombre de mesures formelles d'exécution. Il jouit en particulier de pouvoirs en vue d'ordonner la rectification, le blocage, l'effacement ou la destruction de données qui seraient traitées en violation de la proposition[55]; d'avertir ou de réprimander le responsable du traitement-l'organe de l'Union européenne[56]; d'imposer une interdiction

[53] Ces outils de contrôle, ces pouvoirs d'enquête et d'exécution sont décrits dans le document stratégique du CEPD intitulé « Contrôler et garantir le respect du règlement (CE) n° 45/2011» du 13 décembre 2010, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_FR.pdf).
[54] Article 47, paragraphe 4, de la proposition.
[55] Article 46, paragraphe 3, point e), de la proposition.
[56] Article 46, paragraphe 3, point d), de la proposition.

temporaire ou définitive de traitement[57]; et de saisir la Cour de justice de l'Union européenne[58].

69. Certains de ces pouvoirs, comme le pouvoir prévu par l'article 46, paragraphe 3, point f), d'imposer une interdiction temporaire ou définitive de traitement, sont considérés comme une sanction définitive et ne seront pas imposés à la légère, en particulier en raison de leurs répercussions éventuelles sur les tâches d'Europol. Cependant, un système efficace de contrôle a besoin d'outils répressifs solides afin d'avoir un effet préventif fort. En outre, l'utilisation de ces pouvoirs par l'autorité de contrôle de l'Union européenne sera toujours soumise au contrôle juridictionnel de la Cour de justice.

e) Coopération entre le CEPD et les autorités nationales

70. La proposition veille à ce que toutes les entités de l'Union européenne, y compris Europol, soient soumises à un contrôle cohérent et complet. En outre, elle tient compte de la relation étroite entre l'Union européenne et les États membres dans le cadre des tâches d'Europol et du fait que nombre des données traitées par Europol proviennent des États membres. Cela exige que le cadre juridique fournisse les dispositions nécessaires en vue d'approches coordonnées afin de garantir qu'à tous les niveaux, les activités de contrôle sont coordonnées efficacement via de solides mécanismes de coopération.

71. À cet égard, le cadre juridique d'Europol devrait définir clairement les responsabilités des différentes autorités de contrôle en ce qui concerne les différents éléments du système, pour garantir la pleine responsabilité et la sécurité juridique.

72. Le résultat devrait être une approche pleinement cohérente à tous les niveaux. La cohérence nécessite une coopération appropriée, et le cas échéant étroite, entre le CEPD et les autorités nationales de contrôle, de même qu'une approche cohérente entre les traitements aux niveaux européen et national.

73. Le CEPD salue dès lors l'article 47 sur la coopération et la coordination avec les autorités nationales de contrôle, qui sont essentielles pour assurer l'application cohérente de la proposition au sein de l'Union européenne, comme souligné au considérant 42[59].

74. Cette coopération et cette coordination comportent des avantages supplémentaires, à savoir l'utilisation optimale des ressources et le bénéfice de l'expertise accumulée. Le contrôle cohérent permettra au CEPD de s'appuyer sur l'expérience acquise grâce au contrôle coordonné et peut tirer profit de l'ensemble des connaissances accumulées tant au niveau national qu'au niveau européen. Ce résultat peut être atteint grâce aux échanges de membres du personnel, au détachement d'experts nationaux auprès du CEPD et à la participation d'experts nationaux aux contrôles du

[57] Article 46, paragraphe 3, point f), de la proposition.
[58] Article 46, paragraphe 3, point h), de la proposition.
[59] Le considérant 42 prévoit que: «*Le contrôleur européen de la protection des données et les autorités nationales de contrôle coopèrent entre eux sur des questions spécifiques nécessitant la participation du niveau national et en vue de garantir l'application cohérente de ce règlement au sein de l'Union*». Voir l'exposé des motifs, p. 9.

CEPD. À cet égard, le CEPD salue la disposition de l'article 47, paragraphe 2, concernant l'échange d'informations pertinentes, l'assistance mutuelle en vue de mener des audits et des contrôles, l'étude des problèmes liés à l'exercice du contrôle indépendant ou à l'exercice des droits des personnes concernées, la conception de propositions harmonisées en vue de solutions conjointes à tout problème et la promotion de la sensibilisation quant aux droits en matière de protection des données.

75. L'article 47, paragraphe 3, régit les réunions de coordination entre les autorités nationales de contrôle et le CEPD. Le CEPD salue cette disposition et le fait qu'elle suppose que la coopération est fondée sur les besoins. La formulation actuelle permet une flexibilité suffisante. Par exemple, elle prévoit tant des réunions avec toutes les autorités nationales que, lorsqu'elles sont plus appropriées et plus rentables, des réunions supplémentaires avec un public plus restreint et plus ciblé. Cette approche sera plus amplement développée dans le règlement mentionné dans cette disposition.

76. Afin de garantir une coopération efficace, le CEPD propose de préciser dans l'article 47 que la coopération envisagée inclut tant la coopération bilatérale que la coopération collective. En outre, un considérant devrait souligner l'importance de la coopération entre les différentes autorités de contrôle et fournir des exemples de la manière dont cette coopération pourrait être améliorée.

c) Transfert de données à caractère personnel

Définition

77. La proposition (article 2, point l)) définit le transfert de données à caractère personnel comme étant «la communication de données à caractère personnel, rendues disponibles, entre un nombre limité de parties identifiées, l'expéditeur souhaitant donner accès aux données à caractère personnel au destinataire».

78. La proposition autorise Europol à échanger un volume considérable de données à caractère personnel avec les autorités compétentes aux niveaux national, européen et international, ce qui peut inclure l'accès direct aux données par Eurojust, l'OLAF et les États membres. Le CEPD se félicite de l'ajout d'une définition de la notion de «transfert»[60], qui couvre non seulement les transferts délibérés de données à caractère personnel (système de type «push»), mais aussi l'accès aux données fournies au destinataire (système de type «pull»). Il attire également l'attention du législateur européen sur le fait qu'en ce qui concerne la définition du transfert, il convient d'assurer la cohérence avec le futur règlement général sur la protection des données[61].

Accès direct et indirect par les États membres, l'OLAF et Eurojust

[60] Voir les points 108 et 109 de l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données du 7 mars 2012.

[61] La proposition de règlement sur la protection des données ne contient pas de définition de la notion de «transfert». Une définition de cette notion est insérée sous la forme de l'amendement 86 dans le projet de rapport de la commission LIBE du Parlement européen concernant cette proposition, et dont la formulation est similaire à celle de l'article 2, point l), de la proposition.

79. L'article 26 de la proposition prévoit que les États membres aient i) un accès direct aux informations stockées par Europol aux fins de la vérification croisée en vue de déterminer les connexions entre les informations et aux d'analyse de la nature stratégique ou thématique; et ii) un accès indirect aux mêmes informations sur la base d'un système «hit - no hit» aux fins des analyses opérationnelles dans des cas spécifiques. En cas de «hit», Europol lance la procédure grâce à laquelle les informations ayant généré le hit peuvent être partagées. L'article 27 de la proposition prévoit des règles similaires concernant l'accès direct et indirect aux informations d'Europol par l'OLAF et Eurojust.

80. Eu égard au large accès accordé par la proposition aux États membres et à l'OLAF/Eurojust, il convient d'accorder une attention particulière à la qualité des données. Le CEPD recommande dès lors d'insérer une phrase à l'article 26, paragraphe 1, de la proposition indiquant que les autorités compétentes des États membres peuvent avoir accès aux informations et rechercher des informations sur la base du besoin d'en connaître et dans la mesure où cela est nécessaire en vue de la performance légitime de leurs tâches.

81. En outre, le CEPD recommande que les dispositions de l'article 26, paragraphe 2, exigent également qu'en cas de «hit», i) les autorités compétentes de l'État membre précisent de quelles données elles ont besoin; et que ii) Europol ne peut partager les données avec les autorités en question que dans la mesure où les données qui génèrent le «hit» sont nécessaires en vue de la performance légitime de leurs tâches. Il convient d'apporter des modifications similaires à l'article 27, paragraphe 1, et à l'article 27, paragraphe 2, en ce qui concerne l'accès par l'OLAF et Eurojust. De la même manière, une obligation de soumettre l'accès à une identification devrait être incluse.

82. L'article 26, paragraphe 2, indique qu'en cas de «hit», Europol lance la procédure grâce à laquelle les informations qui ont généré le «hit» peuvent être partagées, «conformément à la décision de l'État membre qui a fourni les informations à Europol». Cependant, tel que mentionné à l'article 26, paragraphe 1, de la proposition, les informations à partager peuvent provenir des États membres, d'organes de l'Union, de pays tiers ou d'organisations internationales. L'article 26, paragraphe 2, devrait dès lors être modifié en conséquence et aligné sur l'article 27, paragraphe 2, qui précise qu'Europol partage les informations conformément à la décision de l'État membre, l'organe de l'Union, du pays tiers ou de l'organisation internationale qui a fourni les informations à Europol.

Relations avec les partenaires

83. Comme mentionné précédemment, le traitement d'informations, y compris l'échange de données à caractère personnel, est l'une des principales raisons d'être d'Europol. Il est aussi évident que les données qu'Europol échange sont bien souvent d'une sensibilité extrême étant donné qu'elles traitent de l'(éventuelle) implication de personnes dans des actes criminels.

84. Le CEPD salue l'insertion du chapitre VI de la proposition sur les relations avec les partenaires et, en particulier, le fait qu'il inclut des dispositions régissant les

transferts vers les organes de l'Union, les pays tiers et les organisations internationales.

85. Dans un monde de plus en plus connecté, une coopération policière et judiciaire efficace au sein des frontières de l'Union européenne dépend de plus en plus de la coopération avec les pays tiers et les organisations internationales. Le développement d'une telle coopération internationale est susceptible de dépendre fortement des échanges de données à caractère personnel, ce qui est complexe en raison du fait que les informations seront aussi échangées avec des pays qui ne garantissent pas un niveau élevé de protection des données à caractère personnel. Il est dès lors d'autant plus important pour l'Union européenne de développer ces échanges dans le plein respect des droits de l'homme, y compris le respect de la vie privée et la protection des données. Un système pour l'échange des données à caractère personnel avec les pays tiers doit trouver un juste équilibre entre la nécessité de disposer de mesures répressives efficaces et la nécessité d'une protection solide des données à caractère personnel.

86. Le CEPD salue dès lors le fait qu'en principe, le transfert de données à caractère personnel vers des pays tiers et des organisations internationales ne peut avoir lieu que si ce transfert est adéquat ou si un accord contraignant fournit des garanties appropriées. Un accord contraignant devrait garantir la sécurité juridique ainsi que la responsabilité d'Europol en ce qui concerne le transfert. Quoi qu'il en soit, en principe, un accord contraignant doit toujours être utilisé en cas de transferts structurels, répétitifs et portant sur des volumes considérables[62].

87. De temps en temps, dans certaines situations, il ne sera pas possible d'obtenir un accord juridiquement contraignant. Ces situations devraient être exceptionnelles et fondées sur une réelle nécessité, dans des cas limités. Elles devraient également être fondées sur des garanties solides, aussi bien au niveau du fond qu'au niveau de la procédure.

Dispositions communes (article 29)

88. L'article 29 de la proposition prévoit des dispositions communes sur l'échange d'informations entre Europol, les organes de l'Union européenne, les pays tiers, les organisations internationales et les tiers. Lorsque les données à transférer ont été fournies par un État membre, Europol doit obtenir l'autorisation de ce dernier, sauf si:
    - l'autorisation peut être supposée lorsque l'État membre n'a pas expressément limité la possibilité de transferts ultérieurs;
    - l´État membre a accordé une autorisation préalable à ces transferts ultérieurs, de façon générale ou à des conditions spécifiques, tout en sachant que ces autorisations peuvent être retirées à tout moment[63].

89. Le CEPD considère que l'autorisation de l'État membre en vue du transfert de données à caractère personnel devrait être explicite et ne peut être «supposée»,

[62] Voir le document de travail du groupe de travail «Article 29» du 24 juillet 1998 intitulé «Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données» (groupe de travail 12).
[63] Article 29, paragraphe 4, de la proposition.

comme c'est actuellement le cas en vertu de l'article 29, paragraphe 4, point a), de la proposition. Les États membres devraient limiter le transfert au moment où ils fournissent les données à Europol. S'ils ne mentionnent aucune restriction à ce moment, ils devraient au moins avoir la possibilité de s'opposer ou de formuler des restrictions avant le transfert. Une autorisation à cette étape serait aussi utile pour garantir la qualité et la précision des données. Le CEPD recommande dès lors fortement de supprimer la possibilité pour Europol de supposer l'autorisation des États membres en supprimant l'article 29, paragraphe 4, point a). Le CEPD conseille également d'ajouter que l'autorisation devrait être accordée «avant le transfert», à la deuxième phrase de l'article 29, paragraphe 4.

90. Enfin, eu égard à la sensibilité des opérations de transfert et bien que l'article 29, paragraphe 5, de la proposition interdise tout transfert ultérieur sans l'autorisation explicite d'Europol, le CEPD recommande d'ajouter que les données ne sont transférées que si le destinataire, qu'il s'agisse d'un organe de l'Union européenne, d'un pays tiers ou d'une organisation internationale, s'engage à les utiliser exclusivement aux fins auxquelles elles ont été transmises[64]. Le CEPD recommande également d'ajouter à l'article 29 un paragraphe exigeant qu'Europol consigne de manière détaillée les transferts de données à caractère personnel ainsi que les raisons de ces transferts, conformément à l'article 44, paragraphe 2, point b), de la proposition (voir le point 148 ci-dessous).

Transferts vers des organes de l'Union européenne (autres qu'Eurojust et que l'OLAF) (article 30)

91. L'article 30 de la proposition autorise Europol à transférer directement des données à caractère personnel vers des organes de l'Union dans la mesure où ce transfert est nécessaire à la réalisation des tâches d'Europol ou de celles de l'organe de l'Union destinataire et à condition que les éventuelles restrictions prévues par l'État membre, l'organe de l'Union, le pays tiers ou l'organisation internationale ayant fourni les informations en question soient respectées.

92. Cette disposition, lue conjointement avec l'article 41, paragraphe 5, de la proposition, respecte l'article 7 du règlement (CE) n° 45/2001, qui traite des transferts de données au sein des organes de l'Union ou entre eux[65]. Etant donné que l'article 27 de la proposition traite déjà de l'OLAF et d'Eurojust[66], le CEPD recommande, pour des raisons de clarté, d'ajouter, à l'article 30, que ce dernier s'applique sans préjudice de l'article 27.

93. Enfin, pour des raisons de transparence, le CEPD recommande qu'Europol rende publique la liste des institutions et des organes de l'Union européenne avec lesquels il partage des informations, en la publiant sur son site internet et en la mettant régulièrement à jour. L'article 30 de la proposition devrait être modifié en conséquence.

Transfert vers des pays tiers et des organisations internationales (article 31)

[64] Cette exigence est mentionnée à l'article 24, paragraphe 2, de la décision du Conseil relative à Europol.
[65] Voir toutefois le point 143 ci-dessous sur l'article 41, paragraphe 5, de la proposition.
[66] Y compris l'accès (voir la définition de «transfert» à l'article 2, point l), de la proposition).

94. Le CEPD salue l'article 31, qui fixe des règles strictes concernant le transfert de données à caractère personnel vers des pays tiers et des organisations tierces.

95. En règle générale, l'article 31, paragraphe 1, de la proposition prévoit qu'un transfert ne peut avoir lieu que lorsque la Commission a décidé que le pays tiers ou l'organisation internationale garantit un niveau de protection adéquat. En l'absence de décision en ce sens, le transfert ne peut avoir lieu que sur la base d'un accord contraignant conclu entre l'Union européenne et le pays tiers ou l'organisation internationale. Cet accord doit apporter des garanties adéquates en ce qui concerne la protection de la vie privée ainsi que les libertés et droits fondamentaux des personnes.

96. Le CEPD salue l'insertion du principe d'adéquation en tant que base des transferts internationaux. Il salue également la référence à la nécessité d'adopter des garanties suffisantes contraignantes lorsqu'aucune décision en matière d'adéquation n'a été adoptée. Ces garanties suffisantes, en tant que garanties *ad hoc* en matière de protection des données, devraient inclure les éléments essentiels mentionnés par le groupe de travail «Article 29» sur la protection des données dans le cadre de l'évaluation de l'adéquation des pays tiers[67]. Le CEPD propose d'ajouter à l'article 31, paragraphe 1, qu'il devrait être consulté en temps utile pendant les négociations de tout accord international entre l'Union européenne et un pays tiers ou une organisation internationale, et en particulier avant l'adoption du mandat de négociation ainsi qu'avant la finalisation de l'accord.

97. Outre la conclusion des futurs accords internationaux, l'article 31, paragraphe 1, point c), de la proposition indique qu'Europol peut aussi transférer des données à caractère personnel vers des autorités de pays tiers ou des organisations internationales sur la base d'accords en vigueur en matière de coopération internationale conclus avec ces pays et ces organisations avant l'entrée en vigueur de la proposition. Le CEPD recommande d'ajouter à la proposition une disposition transitoire relative aux accords de coopération déjà existants et régissant les transferts de données à caractère personnel par Europol. Cette disposition devrait mentionner un délai raisonnable pour la révision de ces accords afin de les aligner sur les exigences de la proposition. Elle devrait être insérée dans les principales dispositions de la proposition, au plus tard deux ans après l'entrée en vigueur de la proposition[68].

98. Pour des raisons de transparence, le CEPD recommande aussi d'ajouter, à la fin de l'article 31, paragraphe 1, qu'Europol publie sur son site internet la liste, régulièrement mise à jour, de ses accords de coopération internationaux avec les pays tiers et les organisations internationales.

Dérogations et instruments ad hoc

[67] Voir le document de travail du groupe de travail «Article 29» du 24 juillet 1998 intitulé «Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données» (Groupe de travail 12). Une interprétation restrictive de la protection des données est aussi conforme à la jurisprudence de la CJUE. Voir également l'avis du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, points 224 et suivants, et point 417.

[68] Voir également le point 217 de l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données.

99. L'article 31, paragraphe 2, de la proposition prévoit, dans un certain nombre de circonstances spécifiques, des dérogations aux exigences de garanties d'adéquation de l'article 31, paragraphe 1. Dans ce contexte, le CEPD note que le considérant 29 mentionne erronément une dérogation supplémentaire (consentement de la personne concernée) qui n'est pas indiquée à l'article 31, paragraphe 2. Les termes «si la personne concernée a consenti» doivent dès lors être supprimés du considérant 29.

100. Le CEPD salue le fait que l'article 31, paragraphe 2, indique que ces dérogations, en tant que justifications pour le transfert sans autorisation préalable du CEPD, doivent être utilisées au cas par cas (voir cependant le point 102 ci-dessous). Le CEPD souhaite toutefois rappeler que l'utilisation de toute dérogation en tant que justification pour un transfert doit être interprétée de façon restrictive et ne s'appliquer qu'aux transferts occasionnels ne pouvant pas être qualifiés de fréquents, massifs ou structurels[69]. En vue d'éviter tout doute, le CEPD recommande d'ajouter expressément, à l'article 31, paragraphe 2, que les dérogations ne peuvent s'appliquer pour les transferts fréquents, massifs ou structurels, en d'autres termes aux ensembles de transferts (et pas uniquement aux transferts occasionnels).

101. En outre, la formulation actuelle des dérogations mentionnées à l'article 31, paragraphe 2, point a), à savoir les transferts nécessaires pour protéger les «intérêts essentiels» d'un État membre, et à l'article 31, paragraphe 2, point c), à savoir les transferts requis en raison d'«intérêts publics importants» est trop vague. L'article 31 devrait mentionner que cette exception ne peut être utilisée que si le transfert a de l'intérêt pour les autorités de l'Union européenne ou des États membres, et pas uniquement pour une ou plusieurs autorité(s) publique(s) dans le pays tiers ou pour une organisation internationale[70]. En ce qui concerne la dérogation relative à l'intérêt public, l'article 31 devrait au moins exiger que cet intérêt public soit reconnu par la législation européenne ou par la législation nationale d'un État membre de l'Union européenne.

102. Outre l'utilisation des dérogations au cas par cas, l'article 31, paragraphe 2, prévoit l'autorisation d'un «ensemble de transferts». Cette disposition ne respecte pas le principe selon lequel les dérogations/les exceptions doivent être limitées aux transferts occasionnels.

103. Il serait très peu souhaitable qu'Europol soit autorisé à procéder à des transferts significatifs vers un pays tiers ou une organisation internationale qui n'est pas reconnu comme veillant au respect de l'adéquation, sans fournir un cadre adéquat pour le transfert, par l'intermédiaire de l'adoption d'un instrument contraignant contenant des garanties suffisantes (voir le point 86 ci-dessus). Le CEPD reconnaît que, dans certains cas, il peut être impossible dans la pratique d'adopter des «garanties suffisantes» sous la forme d'un «instrument contraignant» entre l'Union

[69] Voir la page 7 du document de travail du groupe de travail «Article 29» du 25 novembre 2005 relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (WP114).
[70] Voir la page 15 du document de travail du groupe de travail «Article 29» du 25 novembre 2005 relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (WP114).

européenne et le pays tiers ou l'organisation internationale en question[71]. La proposition devrait limiter ces cas exceptionnels en l'absence d'adéquation et d'accord international en vigueur ou susceptible d'être conclu avec le pays ou l'organisation internationale de destination et lorsque les dérogations décrites ne peuvent pas s'appliquer parce que les transferts sont fréquents, massifs ou structurels (voir le point 100 ci-dessus).

104. Dans de tels cas, et uniquement lorsqu'il est impossible d'obtenir un accord contraignant, un autre type d'instrument de protection ad hoc devrait être considéré[72]. Cet instrument ad hoc devrait être adapté aux éléments spécifiques des transferts envisagés, comme la taille et le nombre de transferts de données envisagés, le type de données (qu'elles concernent des catégories spéciales de personnes concernées ou non) et la qualité du destinataire. Quels que soient le type d'instrument adopté et sa nature non contraignante, un instrument ad hoc doit inclure une description des principes relatifs à la protection des données qu'Europol et l'autorité importatrice-destinataire doivent respecter, ainsi que les moyens mis en place pour assurer le contrôle de la conformité et des mesures de répression (mécanismes nécessaires pour que cette protection soit efficace). Europol devrait être responsable du respect des exigences de protection des données de l'instrument en question. Dès lors, si une personne concernée au sein de l'Union européenne devait être lésée par des dommages en raison d'un transfert de données couvert par un instrument ad hoc, Europol devrait être le responsable final et supporter les coûts de tout dommage résultant des actes posés par le destinataire et des omissions commises par ce dernier. Enfin, l'utilisation d'un tel instrument non contraignant devrait toujours être soumise à une autorisation préalable du CEPD.[73]

105. À la lumière de ce qui précède, le CEPD recommande d'ajouter un paragraphe spécifique consacré aux transferts autorisés par le CEPD. Ce paragraphe, qui devrait logiquement précéder celui sur les dérogations (voir le point 99 ci-dessus), devrait prévoir que le CEPD peut autoriser un transfert ou un ensemble de transferts lorsqu'Europol apporte des garanties suffisantes quant à la protection de la vie privée et des libertés et droits fondamentaux des personnes, et quant à l'exercice des droits correspondants. En outre, cette autorisation peut être accordée avant le transfert/l'ensemble de transferts, pour une période ne dépassant pas un an, renouvelable.

106. En outre, si l'article 31, paragraphe 2, devait *in fine* rester dans le texte, le CEPD souhaite adresser deux recommandations à cet égard:

- les transferts sont autorisés à condition qu'Europol apporte des «garanties», lorsqu'Europol doit apporter des garanties suffisantes, comme indiqué au considérant 29 de la proposition;
- l'autorisation est délivrée par le conseil d'administration «en accord avec le CEPD», lorsque les autorisations doivent être délivrées (ou non) par le CEPD uniquement, agissant en tant qu'autorité de contrôle indépendante.

[71] En tant qu'agence de l'UE, Europol ne peut plus conclure d'accords internationaux contraignants, comme il le faisait avant l'entrée en vigueur du traité de Lisbonne.
[72] Voir aussi les points 222 et 223 de l'avis du Contrôleur européen de la protection des données sur le paquet de mesures pour une réforme de la protection des données, du 7 mars 2012, disponible à l'adresse:
[73] Voir l'article 9, paragraphe 7, du règlement (CE) n° 45/2001.

107. Enfin, l'article 31, paragraphe 3, de la proposition indique qu'Europol doit informer le CEPD lorsque l'article 31, paragraphe 2, est appliqué. À cet effet, le CEPD recommande que tout transfert fondé sur des dérogations soit expressément documenté (par exemple, les données transférées, l'époque du transfert, les données concernant le destinataire, la raison du transfert, etc.).

OBSERVATIONS SPÉCIFIQUES:

Définition des données administratives à caractère personnel (article 2)

108. L'article 2, point o), de la proposition définit les données «administratives à caractère personnel» comme étant «l'ensemble des données à caractère personnel traitées par Europol à l'exception de celles qui sont traitées en vue de remplir les objectifs fixés à l'article 3, paragraphes 1 et 2». Le CEPD salue cette définition dans la mesure où elle établit une distinction claire entre les données à caractère personnel traitées par Europol dans le cadre de ses tâches administratives («données administratives») et les données à caractère personnel traitées en vue d'effectuer ses tâches principales («données opérationnelles»). Cette disposition clarifie aussi la question relative au cadre juridique applicable au traitement de ces données (à savoir le règlement (CE) n° 45/2001 pour les données administratives à caractère personnel et la proposition pour les données opérationnelles)[74].

109. Considérant que la définition des données administratives à caractère personnel inclut des données relatives au personnel d'Europol, le CEPD propose, pour des raisons de clarté, de supprimer les références aux données relatives au personnel dans le titre et le corps de l'article 48.

Tâches liées à la formation des agents des services répressifs (articles 9 à 11)

110. L'article 9, paragraphe 1, indique que l'Institut Europol soutiendra, concevra, fournira et coordonnera une formation pour les agents des services répressifs, en particulier en vue de les sensibiliser et d'accroître leurs connaissances sur plusieurs points mentionnés dans cette disposition. Étant donné que le traitement des données à caractère personnel est une des activités principales des autorités répressives, le CEPD recommande d'inclure à l'article 9, point a), la protection des données en tant que l'un des points à traiter par la formation conçue par l'Institut Europol[75].

Fonctions du conseil d'administration et programme de travail (articles 14 et 15)

111. Le CEPD propose d'inclure à l'article 14 le fait que le délégué à la protection des données sera nommé par le conseil d'administration et de supprimer ce point de l'article 44, ce qui permettra de regrouper dans un seul article toutes les fonctions principales du conseil d'administration. Il propose, en outre, d'ajouter le CEPD en tant que destinataire du rapport d'activités annuel à l'article 14, paragraphe 1, point d), et à l'article 15. Le CEPD devrait recevoir un exemplaire du programme de travail annuel d'Europol une fois que ce dernier a été finalisé et approuvé par le conseil d'administration. Le CEPD propose en outre d'ajouter à l'article 14,

[74] Voir également les points 154 et 155 ci-dessous.
[75] Voir aussi les points 164 à 166 ci-dessous.

paragraphe 1, que le conseil d'administration veille au suivi adéquat des résultats et des recommandations découlant des contrôles effectués par le CEPD de la manière déjà décrite pour les rapports d'audit interne et externe, les évaluations et les enquêtes de l'OLAF à l'article 14, paragraphe 1, point o).

Sources d'information (article 23)

Accès aux systèmes d'informations nationaux, européens ou internationaux

112. L'article 23, paragraphe 3, de la proposition autorise Europol à accéder aux systèmes d'informations de nature nationale, européenne ou internationale, y compris via un accès informatisé direct, dans la mesure où cet accès est autorisé par les instruments juridiques européens, internationaux ou nationaux. Les dispositions applicables de ces instruments régissent l'accès et l'utilisation de ces informations dans la mesure où elles fournissent des règles plus strictes sur l'accès et l'utilisation que la proposition.

113. En ce qui concerne l'accès aux systèmes d'informations nationaux, l'article 7, paragraphe 5, de la proposition exige déjà que les États membres fournissent des informations et des renseignements à Europol[76]. Le CEPD considère dès lors que l'accès aux bases de données nationales n'est pas justifié. Par ailleurs, l'accès direct par Europol aux bases de données nationales soulève des inquiétudes quant à la protection des données et à la sécurité des données. La fourniture d'un accès direct aux données engendre un risque: que le responsable du traitement propriétaire des données perde le contrôle du transfert, en particulier en ce qui concerne les finalités du transfert, les catégories de données transférées ainsi que les conditions du transfert. Néanmoins, il reste responsable de la légalité du transfert et de la précision des données transmises. Le CEPD recommande dès lors de supprimer la possibilité pour Europol d'accéder directement aux bases de données nationales.

114. Lorsque l'accès concerne les systèmes d'informations européens – en particulier les bases de données dont les finalités initiales ne sont pas la répression –, il convient de démontrer la nécessité et la proportionnalité de cet accès[77]. Si les preuves sont suffisantes, la loi autorisant l'accès doit contenir des dispositions explicites et détaillées précisant au moins i) les objectifs du traitement, ii) les données à caractère personnel à traiter, iii) les finalités et les moyens du traitement, iv) la nomination du responsable du traitement, et v) la procédure à suivre pour le traitement des données à caractère personnel.

115. En outre, l'accès ne doit être accordé que sur la base du système «hit - no hit» (à savoir, une réponse positive ou négative). Toute information relative au «hit» doit être communiquée à Europol après l'approbation et l'autorisation explicites du transfert par l'État membre (si l'accès concerne des données fournies par un État membre), l'organe de l'Union européenne ou l'organisation internationale et doit être soumise à une évaluation, tel que mentionné à l'article 35 de la proposition. Le CEPD recommande de fixer ces conditions à l'article 23 de la proposition.

[76] Voir aussi l'analyse d'impact qui mentionne explicitement la précision juridique selon laquelle les États membres sont obligés de fournir des données à Europol (p. 21).
[77] Voir, par exemple, les avis du CEPD sur le système VIS, Eurodac et les données PNR.

Fixation des finalités (article 25)

116. En vertu de l'article 25 de la proposition, les États membres, les organes de l'Union, les pays tiers ou les organisations internationales doivent définir les finalités pour lesquelles les informations qu'ils fournissent peuvent être ultérieurement traitées. Si cela n'a déjà été fait, Europol doit déterminer l'importance de ces informations ainsi que les finalités auxquelles elles peuvent être traitées. D'après le CEPD, l'État membre, en tant que responsable du traitement des données, doit toujours assurer le respect, entre autres, du principe de la limitation des finalités et ne transmettre les données à caractère personnel que pour des finalités spécifiques et bien définies. À la lumière de ce qui précède, le CEPD recommande de supprimer la dernière phrase de l'article 25, selon laquelle Europol doit fixer la finalité des informations fournies par un État membre si ce dernier ne l'a pas fait.

Différents degrés de précision et de fiabilité (article 35)

117. Le CEPD souhaite souligner l'importance qu'il y a de faire la distinction entre les données en fonction de leur degré de précision et de fiabilité, tant pour les personnes concernées que pour les autorités répressives. Cette distinction est en particulier pertinente lorsque les données sont 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», des «renseignements non vérifiés». La personne concernée pourrait aussi être affectée de façon disproportionnée par l'éventuel manque de précision des données relatives aux soupçons pesant à son encontre[78].

118. À la lumière de ce qui précède, le CEPD considère que l'article 35 de la proposition devrait être consolidé en rendant obligatoire l'évaluation par l'État membre fournissant les informations. Il propose de supprimer, à l'article 35, paragraphes 1 et 2, la formulation «autant que possible» et de modifier l'article 36, paragraphe 4, en conséquence.

119. En vertu de l'article 35, paragraphe 6, de la proposition, Europol examine les informations provenant de sources à la disposition du grand public. Le CEPD indique que ces sources n'offrent pas de garanties quant à la qualité des données. À moins que, et aussi longtemps que, la précision des informations et la fiabilité de leurs sources n'ont pas été corroborées par d'autres sources fiables, Europol devrait attribuer à ces informations ou à ces données le code d'évaluation (X) et (4) mentionné aux paragraphes 1 et 2. Le CEPD recommande de modifier l'article 35, paragraphe 6, en conséquence.

Catégories particulières de données à caractère personnel et catégories de personnes concernées (article 36)

[78] Voir l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, points 355 à 358: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_FR.pdf

120. L'article 36 de la proposition fournit des garanties spécifiques en ce qui concerne le traitement des catégories particulières de données (c'est-à-dire les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou les croyances, l'appartenance syndicale et les données concernant la santé ou la sexualité) et des catégories de personnes concernées (c'est-à-dire les victimes d'infraction pénale, les témoins ou d'autres personnes pouvant fournir des informations sur l'infraction pénale et les personnes de moins de 18 ans).

121. Les catégories particulières de données à caractère personnel mentionnées à l'article 36, paragraphe 1, sont, de par leur nature, particulièrement sensibles et méritent une protection spécifique[79]. Les catégories de personnes concernées mentionnées à l'article 36, paragraphe 2, ne sont pas supposées faire partie du traitement normal et habituel effectué par Europol en vue de mener ses principales activités. Le CEPD salue dès lors le fait que la proposition prévoit des garanties supplémentaires pour le traitement des données sensibles et des données relatives à des catégories particulières de personnes concernées.

122. Le CEPD salue en particulier le fait que i) le traitement des données susmentionnées est interdit à moins qu'il ne soit strictement nécessaire (et, pour les données sensibles, qu'elles complètent d'autres données déjà traitées par Europol), et que ii) l'accès à ces données est restreint à un nombre limité de fonctionnaires d'Europol désignés par le directeur. Cependant, le CEPD considère que l'existence d'une nécessité stricte doit être dûment justifiée. Cette justification est importante en vue d'assurer un contrôle efficace et de permettre à Europol de prouver qu'il respecte les règles relatives à la protection des données conformément au principe de la responsabilité (voir les points 161 à 163 ci-dessous). Le CEPD recommande dès lors d'ajouter à l'article 36, paragraphes 1 et 2, les termes «et dûment justifiées».

123. En vertu de l'article 36, paragraphe 5, la transmission de données sensibles ou relatives à des catégories particulières de personnes concernées à des États membres, des organes de l'Union, des pays tiers ou des organisations internationales est interdite à moins qu'elle ne soit strictement nécessaire dans des affaires concernant des infractions qui relèvent des objectifs d'Europol. Le CEPD rappelle que ces transmissions doivent respecter les règles du chapitre VI de la proposition. Afin d'éviter tout doute, il recommande d'ajouter ce critère à l'article 36, paragraphe 5. En outre, parallèlement à son observation concernant l'article 36, paragraphes 1 et 2, il recommande d'ajouter à l'article 36, paragraphe 5, les termes «dument justifiée» après «strictement nécessaire».

124. Enfin, le CEPD fait remarquer qu'en vertu de l'article 36, paragraphe 6, de la proposition, Europol fournit au CEPD un aperçu des données sensibles tous les six mois. Tandis que le CEPD est autorisé, dans le cadre de son mandat, à avoir accès aux données à caractère personnel en cas de nécessité en vue de remplir ses tâches de contrôle[80], il ne doit pas nécessairement connaître les détails de toutes les données à caractère personnel qui ont été traitées. Le CEPD recommande de remplacer l'aperçu de toutes les données à caractère personnel mentionné à l'article 36, paragraphe 2, par les statistiques sur ces données pour chaque finalité.

[79] Voir la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28.1.1981, ainsi que la directive 95/46/CE.
[80] Article 47, paragraphe 2, du règlement n° 45/2001.

Étant donné que les catégories particulières de personnes concernées mentionnées à l'article 36, paragraphe 1, méritent aussi une attention spécifique, le CEPD propose d'inclure les statistiques relatives à ces données.

Délais de stockage et d'effacement des données à caractère personnel (article 37)

125. L'article 31, paragraphe 1, indique que les données à caractère personnel ne sont stockées par Europol qu'aussi longtemps que nécessaire en vue de «la réalisation de ses objectifs». Le CEPD considère que le critère choisi pour fixer le délai de conservation est trop large et doit être limité à la finalité pour laquelle les données sont traitées. Le CEPD recommande dès lors de remplacer les termes «en vue de la réalisation de ses objectifs» par «la finalité pour laquelle les données sont traitées».

126. Le CEPD salue la précision, à l'article 31, des délais de stockage et d'effacement des données à caractère personnel et d'une révision régulière des données stockées. En particulier, il note avec satisfaction que:

i) le stockage continu de données à caractère personnel doit être justifié et enregistré et, en l'absence d'une décision quant au stockage continu, les données doivent être effacées automatiquement;

ii) si des données sensibles et des données relatives à des catégories particulières de personnes concernées sont stockées pendant une période supérieure à cinq ans, le CEPD doit être informé en conséquence;

iii) les situations dans lesquelles les données à caractère personnel ne doivent pas être effacées afin de protéger l'intérêt des personnes concernées sont énumérées.

Sécurité du traitement (article 38)

127. Le CEPD salue les garanties mentionnées à l'article 38, lesquelles visent à assurer un niveau de sécurité suffisamment élevé pour protéger les données à caractère personnel des menaces. Cependant, uniquement sécuriser les données à caractère personnel de manière appropriée ne suffit pas: il se peut que des informations qui ne constituent pas des données à caractère personnel soient utilisées pour compromettre les structures de traitement automatisé des données, ce qui pourrait en fin de compte porter atteinte à la sécurité des données à caractère personnel. Par exemple, les résultats d'audits, les évaluations des risques, les rapports d'incident de sécurité, les rapports sur des faiblesses techniques etc. ne contiennent généralement pas de données à caractère personnel. Cependant, la connaissance de leur contenu a une valeur considérable pour les personnes malveillantes qui cherchent à compromettre des infrastructures ou à obtenir des informations complémentaires susceptibles d'inclure des données à caractère personnel.

128. En outre, le CEPD recommande de préciser à l'article 38, paragraphe 1, que la pratique en matière de gestion des informations sur les risques doit être utilisée afin de définir les mesures techniques et organisationnelles appropriées à mettre en œuvre afin de protéger toutes les données Europol, en tenant compte de tous les besoins en matière de protection des données. Il convient d'établir que les pratiques adéquates en matière de gestion des informations sur les risques sont utilisées sur la base i) de normes internationales reconnues et de révisions régulières de l'ensemble des analyses réalisées dans ce contexte, et ii) de contrôles et d'examens de toutes les

mesures techniques et organisationnelles mises en œuvre dans ce contexte. En outre, pour les raisons expliquées aux paragraphes précédents, les objectifs énumérés à l'article 38, paragraphe 2, devraient être revus afin de couvrir toutes les données.

129. Le CEPD salue la collaboration entre Europol et les États membres mentionnée à l'article 38, paragraphe 3, en vue d'aborder la question de la sécurité au-delà des frontières des systèmes d'information. Outre l'article 7, paragraphe 9, le CEPD souhaite que l'article 38, paragraphe 3, précise que la collaboration entre Europol et les États membres couvre la gestion des informations sur les risques.

Droits des personnes concernées (articles 39 et 40)

130. Premièrement, le CEPD souhaite souligner que la transparence est un point essentiel de la protection des données, non seulement en raison de sa valeur intrinsèque mais également parce qu'elle permet à d'autres principes de la protection des données d'être exercés. Les individus ne sont en mesure d'exercer leurs droits que s'ils savent que leurs données sont traitées. Cela est d'autant plus important dans le domaine de la répression, où l'utilisation des données à caractère personnel a inévitablement des conséquences énormes sur la vie et la liberté des individus. Le CEPD recommande dès lors d'inclure dans la proposition une exigence selon laquelle Europol doit adopter une politique transparente et facilement accessible expliquant son traitement des données à caractère personnel et les moyens disponibles pour l'exercice des droits des personnes concernées. Cette politique devrait prendre une forme intelligible et utiliser un langage clair et simple. Cette disposition devrait aussi indiquer que cette politique doit être facilement accessible sur le site internet d'Europol et sur les sites internet des autorités nationales de contrôle.

131. Les articles 39 et 40 de la proposition traitent des droits des personnes concernées en matière d'information, d'accès, de rectification et d'effacement. Le CEPD salue ces dispositions dans la mesure où elles prévoient un ensemble de droits pour les personnes concernées tout en tenant compte de la nature particulière du traitement par les autorités répressives et judiciaires.

132. L'article 39, paragraphe 1, de la proposition précise quelles sont les informations à communiquer aux personnes concernées. Le CEPD recommande d'ajouter les informations suivantes:

- la période pendant laquelle les données seront stockées;
- l'existence du droit de demander à Europol la rectification, l'effacement ou la restriction du traitement des données à caractère personnel concernant la personne concernée;
- toute autre information dans la mesure où elle est nécessaire pour assurer un traitement loyal à l'égard de la personne concernée, en tenant compte des circonstances spécifiques dans lesquelles les données à caractère personnel sont traitées.

133. En outre, afin d'assurer la cohérence avec les règles applicables relatives à la protection des données en vertu du règlement (CE) n° 45/2001 et avec les règles prévues dans le train de réformes, le CEPD propose d'ajouter le droit des personnes concernées à obtenir d'Europol une copie des données en cours de traitement.

134. La proposition prévoit que le droit d'accès est exercé au moyen d'une demande adressée à l'autorité désignée à cette fin dans l'État membre choisi par la personne concernée, qui transmettra ensuite la demande à Europol dans un délai d'un mois à compter de sa réception[81]. Europol doit répondre à la demande dans un délai de trois mois à compter de sa réception[82]. Afin d'éviter toute confusion concernant ces deux délais, le CEPD propose de mentionner expressément qu'Europol doit répondre à la demande dans un délai de trois mois à compter de sa réception par l'autorité nationale.

135. En vertu de l'article 39, paragraphe 2, de la proposition, toute personne concernée souhaitant exercer son droit d'accès peut formuler une demande en ce sens sans que cela n'engendre de coûts excessifs. En revanche, l'article 13 du règlement (CE) n° 45/2001 indique que la personne concernée doit être en mesure d'exercer son droit «sans contrainte» et «gratuitement». Pour des raisons de cohérence, le CEPD recommande de supprimer de cette disposition le fait qu'elle n'engendre pas de coûts excessifs.

136. La proposition prévoit qu'Europol doit consulter les autorités compétentes des États membres concernés par l'accès de la personne concernée à ces données, et si un État membre s'oppose à la proposition de réponse d'Europol, il doit notifier son opposition à Europol[83].

137. L'article 39, paragraphe 6, de la proposition mentionne que les informations relatives aux motifs factuels et juridiques sur lesquels la décision d'Europol sur le droit d'accès se fonde peuvent être omises lorsque la fourniture de ces informations priverait d'effet les motifs de restriction imposés par l'article 39, paragraphe 5. Dans ce cas, le CEPD recommande d'exiger d'Europol qu'il documente les motifs permettant d'omettre la communication des motifs factuels et juridiques sur lesquels la décision se fonde. De manière plus générale, si la fourniture d'informations en réponse à une demande d'accès est refusée, la proposition doit prévoir qu'Europol doit avertir la personne concernée qu'il a effectué des contrôles sans donner d'informations qui pourraient lui révéler si des données à caractère personne la concernant sont ou non traitées par Europol.

138. En ce qui concerne le droit de rectification, d'effacement et de verrouillage, l'article 40, paragraphe 4, indique que, si les données à rectifier, à effacer ou à verrouiller détenues par Europol lui ont été fournies par des pays tiers ou des organisations internationales ou si elles résultent d'analyses menées par Europol, ce dernier doit les rectifier, les effacer ou les verrouiller. Conformément au partage de responsabilités prévu à l'article 41 de la proposition, Europol devrait aussi être chargé de la rectification, de l'effacement et du verrouillage des données fournies par d'autres organes de l'Union européenne.

139. À l'article 40, paragraphe 6, de la proposition, ce à quoi les termes «données incorrectes transférées par d'autres moyens appropriés» font référence n'est pas très clair. Il convient de clarifier cette formulation.

[81] Article 39, paragraphe 2, de la proposition.
[82] Article 39, paragraphe 2, de la proposition.
[83] Article 39, paragraphes 3 et 4, de la proposition.

140. Enfin, l'article 40 de la proposition devrait aussi mentionner les conditions et les motifs relatifs à la restriction du droit de rectification, d'effacement et de verrouillage de la même manière que pour le droit d'accès.

Responsabilité en matière de protection des données (article 41)

141. L'article 41 fixe la répartition des responsabilités en matière de protection des données. Le CEPD considère qu'il ne définit pas clairement la responsabilité de toutes les parties concernées. En ce qui concerne l'article 41, paragraphe 4, il convient de préciser que la responsabilité en matière de respect de tous les principes applicables en matière de protection des données (et pas uniquement la «légalité du transfert») appartient à l'expéditeur des données. Le CEPD recommande de modifier l'article 41 en conséquence.

142. Pour ce qui est de l'article 41, paragraphe 2, le CEPD fait remarquer que, tandis que les États membres sont considérés comme responsables de la qualité des données qu'ils fournissent, Europol est considéré responsable des données fournies par les organes de l'Union européenne. Le CEPD recommande, pour des raisons de cohérence, que les organes de l'Union européenne soient responsables de la qualité des données jusqu'au transfert, y compris le moment du transfert.

143. L'article 41, paragraphe 5, de la proposition établit les responsabilités respectives d'Europol et de l'organe de l'Union européenne destinataire lorsque les données sont transférées à la suite d'une demande émanant du destinataire. Cependant, conformément aux exigences similaires de l'article 7 du règlement (CE) n° 45/2001, le CEPD recommande d'ajouter les précisions suivantes:
- Europol est tenu de vérifier la compétence du destinataire et d'évaluer à titre provisoire la nécessité du transfert de ces données;
- si des doutes se font jour quant à la nécessité de ce transfert, Europol demande au destinataire un complément d'informations;
- le destinataire veille à ce que la nécessité du transfert des données puisse être ultérieurement vérifiée;
- le destinataire traite les données à caractère personnel uniquement aux fins qui ont motivé leur transmission.
L'article 41, paragraphe 5, doit être modifié en conséquence. Il convient également de veiller à ce que les échanges avec Eurojust et l'OLAF soient couverts, en vertu de l'article 27 de la proposition.

Contrôle préalable (article 42)

144. L'article 42 de la proposition prévoit l'intervention du CEPD au moyen d'une notification en vue d'un contrôle préalable par Europol portant sur le traitement de données opérationnelles à caractère personnel qui feront partie d'un nouveau fichier à créer lorsque:
- le traitement des données à caractère personnel concerne des catégories particulières de données mentionnées à l'article 36, paragraphe 2, à savoir des données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou croyances, l'appartenance syndicale, des données relatives à la santé ou à la vie sexuelle;
- le type de traitement, en particulier s'il utilise de nouvelles technologies ou procédures ou de nouveaux mécanismes, comporte par ailleurs des risques

spécifiques pour les libertés et droits fondamentaux, et en particulier la protection des données à caractère personnel, des personnes concernées.
En revanche, les données administratives à caractère personnel[84] sont soumises à la procédure de contrôle préalable prévue par l'article 27 du règlement (CE) n° 45/2001 (voir le point 57 ci-dessus).

145. Le CEPD salue les exigences relatives au contrôle préalable, notamment lorsque le type de traitement présente des risques spécifiques pour les libertés et droits fondamentaux, et en particulier la protection des données à caractère personnel, des personnes concernées[85].

146. La proposition invite à effectuer un contrôle préalable de chaque «nouveau fichier». Comme déjà mentionné aux points 35 et 36 ci-dessus, la proposition est axée sur les finalités pour lesquelles les données ont été fournies plutôt que sur des fichiers prédéfinis. Le CEPD fait dès lors remarquer que ce n'est pas le fichier lui-même, mais son utilisation en vue d'une finalité ou de finalités liées, qui déterminera si un contrôle préalable est ou non requis. À la lumière de cette évolution, il n'est pas nécessaire de mentionner des «fichiers» en tant que déclencheurs d'un contrôle préalable. Au contraire, Europol devrait remplir une notification en vue d'un contrôle préalable avec le CEPD pour tout ensemble de traitements servant une finalité ou des finalités liées relatives à ses activités principales, dans la mesure où ces traitements relèvent du champ d'application des exigences de contrôle préalable. Le CEPD recommande dès lors de modifier l'article 42 en conséquence.

Délégué à la protection des données (article 44)

147. Le CEPD salue non seulement le fait que le délégué à la protection des données (DPD) est directement nommé par le conseil d'administration, mais aussi les autres dispositions de l'article 44 de la proposition visant à garantir l'indépendance du DPD, comme le fait qu'il/elle agira en toute indépendance, ne peut être licencié(e) qu'avec l'accord du CEPD et ne peut recevoir aucune instruction concernant la réalisation de ses tâches.

148. Le CEPD apprécie aussi l'obligation pour le DPD de garantir un enregistrement spécifique du transfert et de la réception des données à caractère personnel (article 44, paragraphe 7, point b)). Le CEPD propose que cet enregistrement spécifique fasse partie du registre des traitements effectués par Europol (voir le point 151 ci-dessous).

149. L'article 44, paragraphe 8, prévoit que le DPD remplisse les fonctions définies dans le règlement (CE) n° 45/2001 en ce qui concerne les «données à caractère personnel des membres du personnel d'Europol ainsi que les données administratives à caractère personnel». Étant donné que la définition des données

[84] Les données administratives à caractère personnel sont définies à l'article 2, point o), de la proposition comme étant «l'ensemble des données à caractère personnel traitées par Europol à l'exception de celles qui sont traitées en vue de remplir les objectifs fixés à l'article 3, paragraphes 1 et 2». Voir les points 108 et 109 ci-dessus.
[85] Article 42, paragraphe 1, point a), de la proposition.

administratives à caractères personnel[86] inclut les données du personnel d'Europol, le CEPD recommande, pour des raisons de cohérence, de ne mentionner dans cette disposition que les données administratives à caractère personnel.

150. La tâche du DPD visant à garantir la légalité et le respect des dispositions de la proposition concernant le traitement des données à caractère personnel ne porte pas préjudice à l'obligation d'Europol de respecter les obligations qui lui incombent. Le CEPD recommande dès lors de modifier l'article 44, paragraphe 7, point a), en remplaçant les termes «garantir, de manière indépendante, la légalité et le respect des dispositions du présent règlement concernant le traitement des données à caractère personnel» par «garantir, de manière indépendante, l'application interne des dispositions du présent règlement concernant le traitement des données à caractère personnel».

151. Comme déjà mentionné (voir le point 149 ci-dessus), le DPD remplit les fonctions prévues par le règlement (CE) n° 45/2001 en ce qui concerne les données administratives à caractère personnel. Pour ce qui est des principales activités de traitement des données (données opérationnelles) d'Europol, les tâches du DPD sont décrites à l'article 44, paragraphe 7, de la proposition. Afin d'assurer la cohérence des tâches du DPD à l'égard des données administratives et des données opérationnelles, le CEPD recommande d'ajouter les tâches suivantes à l'article 44, paragraphe 7:
- tenir un registre de tous les traitements effectués par Europol, contenant suffisamment d'informations (finalité(s) du traitement, description des catégories de personnes concernées et de données, destinataires, délais pour le verrouillage et l'effacement, transferts vers des pays tiers ou des organisations internationales, mesures de sécurité);
- notifier au CEPD les traitements visés à l'article 42 (contrôle préalable)[87].

152. Il convient d'attribuer au DPD les moyens pour contrôler les incidents concernant les données à caractère personnel, ce qui lui permettrait d'identifier les principales questions de sécurité et domaines d'amélioration, en coopération avec l'équipe en charge de la sécurité. Le CPED propose donc d'ajouter à l'article 44, paragraphe 7, la tâche consistant à tenir un registre de ces incidents touchant tant les données opérationnelles que les données administratives à caractère personnel.

153. L'article 44, paragraphe 9, prévoit que, dans le cadre de ses fonctions, le DPD a accès à toutes les données traitées par Europol et à tous les locaux d'Europol. L'article 44, paragraphe 11, accorde le même accès aux membres du personnel du DPD dans la mesure où cet accès est nécessaire à la réalisation de leurs tâches. Le CEPD propose d'ajouter à ces deux articles que cet accès est possible à n'importe quel moment et sans demande préalable.

Données administratives à caractère personnel et données relatives au personnel (article 48)

[86] L'article 2, point o), de la proposition définit les données administratives à caractère personnel comme étant «les données à caractère personnel traitées par Europol à l'exception de celles qui sont traitées en vue de remplir les objectifs fixés à l'article 3, paragraphes 1 et 2».
[87] Pour ce qui est du contrôle préalable, voir les observations ci-dessus (points 144 à 146).

154. Considérant que la définition des données administratives à caractère personnel inclut des données relatives au personnel d'Europol (voir les points 108 et 109 ci-dessus), le CEPD propose, pour des raisons de clarté, de supprimer les références aux données relatives au personnel dans le titre et le corps de l'article 48.

155. En outre, afin d'éviter toute confusion en ce qui concerne le champ d'application de la proposition, le CEPD recommande de mentionner expressément à l'article 48 que le règlement (CE) n° 45/2001 s'applique à toutes les données administratives à caractère personnel à l'exclusion des dispositions de la proposition.

Droit de porter plainte devant le CEPD (article 49)

156. L'article 49 de la proposition prévoit le droit, pour toute personne concernée, de porter plainte devant le CEPD concernant des violations présumées des dispositions régissant le traitement des données à caractère personnel contenues dans la proposition.

157. En vertu de l'article 49, paragraphe 2, de la proposition, lorsqu'une plainte a trait à l'exercice du droit d'accès (à savoir le refus ou la restriction du droit d'accès par Europol) ou du droit de rectification, d'effacement et de verrouillage (à savoir, le refus du droit de restriction, d'effacement ou de verrouillage par Europol), le CEPD consulte les autorités nationales de contrôle ou l'organe judiciaire compétent de l'État membre d'où les données proviennent ou de l'État membre qui est directement concerné. La décision du CEPD quant à la plainte est prise en étroite coopération avec l'autorité nationale de contrôle ou l'organe judiciaire compétent.

158. Le CEPD salue le fait que l'article 49, paragraphe 2, de la proposition inclue la coopération des autorités nationales et leur participation active à la décision du CEPD lorsque les données en jeu sont fournies par les États membres. Cependant, cette disposition donne lieu aux observations suivantes:

- bien que le CEPD soit pleinement d'accord avec la nécessité de consultation, il ne comprend pas comment la décision peut être prise «en étroite coopération». Afin d'assurer la sécurité juridique, y compris des personnes concernées, il convient de préciser que c'est le CEPD qui décide, sa décision étant soumise à l'examen de la Cour de justice, mais que les autorités des États membres ne peuvent être codécideurs. Il propose de supprimer la deuxième phrase de l'article 49, paragraphe 2;
- le texte doit refléter le fait que plus d'un État membre peut avoir fourni des données sur la personne concernée ou peut être concerné par la communication de données à la personne concernée;
- il convient de préciser que lorsque les données en jeu ne proviennent pas des États membres, les autorités nationales ne devraient pas être consultées.

159. Un élément n'est pas clair: l'article 49, paragraphes 3 et 4, de la proposition couvre-t-il les situations dans lesquelles une plainte a trait à l'exercice du droit d'accès ou du droit de rectification, d'effacement et de verrouillage, ou cette disposition traite-t-elle des plaintes en général? Conformément au partage des responsabilités prévu à l'article 41 de la proposition, ces dispositions visent à préciser le champ d'application des pouvoirs du CEPD en matière de plaintes liées au traitement des données par Europol, en fonction de l'origine des données. En particulier, si la plainte a trait à des données provenant d'États membres, le CEPD

coopère avec les autorités nationales de contrôle afin de vérifier si le traitement des données au niveau des États membres concernés était légitime.

160. Cependant, ces dispositions ne mentionnent pas le traitement des données générées par Europol lui-même, par exemple lorsqu'il a extrait des données de sources à la disposition du grand public. Elles n'indiquent pas précisément le fait que, bien que les autorités nationales de contrôle doivent participer lorsque les données en jeu proviennent d'un État membre, le CEPD est la seule autorité de contrôle compétente en ce qui concerne le traitement ultérieur des données par Europol, quelle que soit leur origine. En outre, la référence aux «contrôles nécessaires» à réaliser n'est pas claire et est insuffisante. Les pouvoirs de contrôle du CEPD définis dans la proposition (article 46) ne se limitent pas à veiller à ce que les «contrôles nécessaires» ont été effectués par le responsable du traitement. Dès lors, il convient de réécrire l'article 49, paragraphes 3 et 4, afin de clarifier le point soulevé par le CEPD.

Le principe de responsabilité

161. Dans le contexte de la réforme de la protection des données, le CEPD a souligné la nécessité de consolider la responsabilité des responsables du traitement. Il a aussi précisé que le nouveau cadre doit prévoir des dispositions qui motivent les responsables du traitement à inclure à titre préventif des nouveaux outils dans leurs processus opérationnels pour veiller au respect de la protection des données (principe de responsabilité)[88]. Le CEPD a dès lors salué l'introduction de dispositions générales sur la «responsabilité» et la «prise en compte du respect de la vie privée dès la conception» dans la proposition de règlement sur la protection des données[89].

162. En règle générale, le responsable du traitement doit adopter des politiques et mettre en œuvre des mesures appropriées pour veiller au respect des règles relatives à la protection des données, et être en mesure de prouver ce respect, et pour assurer le contrôle de l'efficacité des mesures. Dans ce contexte, la proposition de règlement sur la protection des données introduit, entre autres, les principes de protection des données dès la conception et de protection des données par défaut, ainsi que l'obligation pour le responsable de mener une évaluation de l'impact sur la protection des données avant de commencer certains traitements. La proposition de directive sur la protection des données contient une version simplifiée du même principe.

163. Pour des raisons de cohérence avec la réforme de la protection des données et en vue de veiller à ce que toutes les exigences en matière de protection des données soient prises en considération, le CEPD recommande d'ajouter dans les dispositions essentielles de la proposition que: i) une évaluation d'impact similaire à celle qui est décrite dans la proposition de règlement sur la protection des données est menée pour tous les traitements relatifs aux données à caractère personnel; ii) les principes de protection des données dès la conception et de protection des données par défaut

[88] Voir l'avis du CEPD du 14 janvier 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social, au Comité des régions intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», points 99 à 117.
[89] Voir l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, point II.6.

sont appliqués à la création ou à l'amélioration des systèmes de traitement des données à caractère personnel; iii) le responsable adopte des politiques et prend des mesures appropriées pour veiller au respect des règles relatives à la protection des données, et être en mesure de prouver ce respect, et pour assurer le contrôle de l'efficacité des mesures; et iv) le DPD d'Europol et, si nécessaire, les autorités de contrôle sont impliquées dans toutes les discussions clés sur le traitement des données à caractère personnel.

IV. OBSERVATIONS SUR LA COMMUNICATION

164. La communication propose un programme européen de formation des services répressifs (ci-après le «programme de formation») en vue de transmettre aux agents des services répressifs les connaissances et les compétences dont ils ont besoin pour prévenir la criminalité transfrontalière et lutter contre ce phénomène, et ce efficacement, grâce à une coopération efficace avec leurs collègues européens. Le programme de formation vise, entre autres, à faire en sorte que les instruments de coopération en matière de répression que l'Union européenne a conçus au fil des années (comme le système d'informations Prüm[90] et les bases de données d'Europol en matière de renseignements criminels) soient mieux connus et utilisés lors des contacts tant bilatéraux que multilatéraux entre États membres.

165. La communication mentionne que le programme de formation devrait être axé sur l'amélioration des savoirs, des aptitudes et des compétences, et s'articuler autour de quatre volets allant des connaissances génériques à des connaissances très spécialisées. Le premier volet est consacré aux connaissances de base sur la dimension européenne de l'action répressive et devrait inclure les principes de la coopération efficace en matière de répression, les droits fondamentaux, le rôle d'Europol, de Frontex et d'Eurojust et l'utilisation des outils et canaux européens de gestion de l'information comme l'«initiative suédoise»[91] et le «système d'information Schengen». Le CEPD souligne que les connaissances de ce premier volet devraient aussi inclure des connaissances spécifiques sur la protection des données. Ces éléments doivent figurer dans le programme de formation.

166. Le paragraphe 5.5 définit les rôles et responsabilités et mentionne un certain nombre d'acteurs devant jouer un rôle dans la mise en œuvre du programme de formation. Le CEPD n'est pas mentionné, mais est disponible pour jouer un rôle dans le cadre de la mise en œuvre. Dans sa stratégie 2013-2014, le CEPD s'est positionné en tant que centre d'excellence, chargé, entre autres, de la tâche de sensibiliser l'opinion à la protection des données.[92]

V. CONCLUSIONS

Généralités

[90] Décision 2008/615/JAI du Conseil et décision 2008/616/JAI du Conseil, JO, L 210 du 6.8.2008.
[91] Décision-cadre 2006/960/JAI du Conseil, JO L 386 du 29.12.2006, p. 89.
[92] Stratégie 2013-2014 du CEPD, disponible sur le site internet du CEPD.

167. Le CEPD souligne que la proposition est essentielle du point de vue du traitement des données à caractère personnel. Le traitement d'informations, comprenant des données à caractère personnel, est une des principales raisons d'être d'Europol et la proposition prévoit déjà une protection solide des données. Le présent avis détaillé a dès lors été adopté en vue de consolider la proposition.

168. Le CEPD note que la décision du Conseil relative à Europol en vigueur fournit un régime solide de protection des données et considère que ce niveau ne devrait pas être abaissé, indépendamment des discussions sur la proposition de directive relative à la protection des données. Il convient de préciser ces points dans le préambule.

169. Le CEPD salue le fait que la proposition met Europol en conformité avec les exigences de l'article 88, paragraphe 2, du TFUE, ce qui garantira que les activités d'Europol bénéficieront de la pleine participation de toutes les institutions de l'Union européenne concernées.

170. Le CEPD salue l'article 48 de la proposition qui prévoit que le règlement (CE) n° 45/2001, y compris les dispositions sur le contrôle, s'applique entièrement aux données administratives et concernant le personnel. Le CEPD regrette cependant le fait que la Commission n'ait pas choisi d'appliquer le règlement (CE) n° 45/2001 aux activités principales d'Europol, et de limiter la proposition à des règles spécifiques et des dérogations supplémentaires, qui tiennent dûment compte des spécificités du secteur des services répressifs. Il note toutefois que le considérant 32 de la proposition mentionne expressément le fait que les règles relatives à la protection des données au niveau d'Europol devraient être renforcées et se fonder sur les principes du règlement (CE) n° 45/2001. Ces principes constituent aussi un important point de référence pour le présent avis. .

171. Le CEPD recommande de préciser dans les considérants de la proposition que le nouveau cadre de la protection des données des institutions et des organes de l'Union européenne s'appliquera à Europol dès son adoption. En outre, l'application à Europol du régime de protection des données des institutions et organes de l'Union européenne devrait être précisée dans l'instrument remplaçant le règlement (CE) n° 45/2001, comme annoncé pour la première fois en 2010, dans le cadre de la révision du train de mesures sur la protection des données. Au plus tard dès l'adoption du nouveau cadre général, les principaux nouveaux éléments de la réforme de la protection des données (à savoir le principe de responsabilité, l'analyse d'impact relative à la protection des données, la prise en compte du respect de la vie privée dès la conception et la protection de la vie privée par défaut et la notification de violations de données à caractère personnel) devraient aussi s'appliquer à Europol. Il convient de mentionner également ce point dans le préambule.

Europol: une nouvelle structure des informations

172. Le CEPD comprend la nécessité de flexibilité en raison de l'évolution du contexte, ainsi qu'à la lumière des rôles croissants d'Europol. L'architecture des informations existante ne constitue pas nécessairement la référence pour l'avenir. C'est au législateur européen qu'il revient de définir la structure des informations d'Europol. Dans son rôle en tant que conseiller auprès du législateur européen, le

CEPD se concentre sur la question de savoir dans quelle mesure le choix des législateurs est limité par les principes de la protection des données.

173. En ce qui concerne l'article 24 de la proposition, il:

- recommande de définir dans la proposition les notions d'analyse stratégique, thématique et opérationnelle et de supprimer la possibilité de traiter les données à caractère personnel aux fins de l'analyse stratégique ou thématique, à moins qu'une justification solide ne soit donnée;
- en ce qui concerne l'article 24, paragraphe 1, point c, il recommande de définir clairement une finalité spécifique pour chaque cas d'analyse opérationnelle et d'exiger que seules les données à caractère personnel pertinentes soient traitées conformément à la finalité spécifique définie;
- recommande d'ajouter dans la proposition les éléments suivants: i) toutes les opérations de vérification croisée par les analystes d'Europol sont expressément motivées, ii) l'extraction de données à la suite d'une consultation est limitée au strict minimum requis et est expressément motivée, iii) la traçabilité de toutes les opérations liées aux vérifications croisées est garantie, et iv) seul le personnel autorisé responsable de la finalité pour laquelle les données ont initialement été collectées peut modifier ces données.

Renforcement du contrôle de la protection des données

174. L'article 45 de la proposition reconnaît que le contrôle du traitement prévu dans la proposition est une tâche qui nécessite aussi la participation active des autorités nationales chargées de la protection des données[93]. La coopération entre le CEPD et les autorités nationales de contrôle est essentielle en vue du contrôle efficace dans ce domaine.

175. Le CEPD salue l'article 45 de la proposition. Cet article indique que le traitement de données par les autorités nationales est soumis à un contrôle au niveau national, ce qui reflète dès lors le rôle clé des autorités nationales de contrôle. Il salue également l'exigence selon laquelle les autorités nationales de contrôle devraient tenir le CEPD informé de toute action prise à l'égard d'Europol.

176. Le CEPD salue:

- les dispositions sur le contrôle qui prévoient une architecture solide en matière de contrôle sur le traitement des données. Ces dispositions prennent en considération les responsabilités au niveau national et au niveau de l'Union européenne et établissent un système en vue de coordonner toutes les autorités participant à la protection des données;

- la reconnaissance, dans la proposition, de son rôle en tant qu'autorité créée pour contrôler toutes les institutions et tous les organes de l'Union européenne;

[93] Voir aussi la résolution n° 4 de la conférence de printemps des autorités européennes de protection des données (Lisbonne, 16 et 17 mai 2013).

- l'article 47 sur la coopération et la coordination avec les autorités nationales de contrôle, mais propose de préciser que la coopération envisagée inclut la coopération tant bilatérale que collective. Un considérant devrait souligner l'importance de la coopération entre les différentes autorités de contrôle et fournir des exemples de la manière dont cette coopération pourrait être améliorée.

Transfert

177. Le CEPD propose d'insérer à l'article 26, paragraphe 1, de la proposition une phrase indiquant que les autorités compétentes des États membres ont accès aux informations et recherchent des informations sur la base du besoin d'en connaître et dans la mesure où ces informations sont nécessaires en vue de l'accomplissement légitime de leurs tâches. Il convient de modifier l'article 26, paragraphe 2, et de le mettre en conformité avec l'article 27, paragraphe 2.

178. Le CEPD salue le fait qu'en principe, le transfert vers des pays tiers et des organisations internationales ne peut avoir lieu que si ce transfert est adéquat ou si un accord contraignant fournit des garanties appropriées. Un accord contraignant garantira la sécurité juridique ainsi que la responsabilité d'Europol en ce qui concerne le transfert. Un accord contraignant doit toujours être nécessaire pour les transferts massifs, structurels et fréquents. Le CEPD comprend cependant qu'il existe des situations dans lesquelles un accord contraignant ne peut être requis. Ces situations devraient être exceptionnelles et fondées sur une réelle nécessité, uniquement dans des cas limités. Elles devraient également être fondées sur des garanties solides, aussi bien au niveau du fond qu'au niveau de la procédure.

179. Le CEPD recommande fortement de supprimer la possibilité pour Europol de supposer l'autorisation des États membres. Le CEPD conseille également d'ajouter que l'autorisation devrait être accordée «avant le transfert», à la deuxième phrase de l'article 29, paragraphe 4. Le CEPD recommande également d'ajouter à l'article 29 un paragraphe exigeant qu'Europol consigne de manière détaillée les transferts de données à caractère personnel.

180. Le CEPD recommande d'ajouter à la proposition une disposition transitoire relative aux accords de coopération existants et régissant les transferts de données à caractère personnel par Europol. Cette disposition devrait réviser ces accords dans un délai raisonnable afin de les aligner sur les exigences de la proposition. Elle devrait être insérée dans les principales dispositions de la proposition, maximum deux ans après l'entrée en vigueur de la proposition.

181. Pour des raisons de transparence, le CEPD recommande aussi d'ajouter, à la fin de l'article 31, paragraphe 1, qu'Europol publie sur son site internet la liste, régulièrement mise à jour, de ses accords de coopération internationaux avec les pays tiers et les organisations internationales.

182. Le CEPD recommande d'ajouter expressément, à l'article 31, paragraphe 2, que les dérogations ne peuvent s'appliquer aux transferts fréquents, massifs ou structurels, en d'autres termes aux ensembles de transferts (et pas uniquement aux transferts occasionnels).

183. Le CEPD recommande de prévoir un paragraphe spécifique consacré aux transferts effectués avec l'autorisation du CEPD. Ce paragraphe, qui devrait logiquement précéder celui sur les dérogations, prévoira que le CEPD peut autoriser un transfert ou un ensemble de transferts lorsqu'Europol apporte des garanties suffisantes quant à la protection de la vie privée, des libertés et droits fondamentaux des personnes et quant à l'exercice des droits correspondants. En outre, cette autorisation sera accordée avant le transfert/l'ensemble de transferts, pour une période ne dépassant pas un an, renouvelable.

Autres

184. Le présent avis comprend de nombreuses autres recommandations, visant à améliorer encore la proposition. Quelques recommandations plus significatives sont énumérées ci-dessous:

a. supprimer la possibilité pour Europol d'accéder directement aux bases de données nationales (article 23);
b. lorsque l'accès concerne des systèmes d'information européens, n'accorder l'accès que sur la base du système de «hit/no hit» (à savoir une réponse positive ou négative). Toute information relative au «hit» doit être communiquée à Europol après l'approbation et l'autorisation explicites du transfert par l'État membre (si l'accès concerne des données fournies par un État membre), l'organe de l'Union européenne ou l'organisation internationale et doit être soumise à une évaluation, tel que mentionné à l'article 35 de la proposition. Le CEPD recommande de mentionner ces conditions à l'article 23 de la proposition;
c. consolider l'article 35 de la proposition en faisant en sorte que l'évaluation par l'État membre fournisse les informations obligatoires. Le CEPD propose de supprimer, à l'article 35, paragraphes 1 et 2, la formulation «autant que possible» et de modifier l'article 36, paragraphe 4, en conséquence;
d. remplacer l'aperçu de toutes les données à caractère personnel mentionné à l'article 36, paragraphe 2, par les statistiques sur ces données pour chaque finalité. Étant donné que les catégories particulières de personnes concernées mentionnées à l'article 36, paragraphe 1, méritent aussi une attention spécifique, le CEPD propose d'inclure les statistiques relatives à ces données.
e. inclure dans la proposition une disposition selon laquelle Europol doit adopter une politique transparente et facilement accessible expliquant son traitement des données à caractère personnel et aux fins de l'exercice des droits des personnes concernées. Cette politique devrait prendre une forme intelligible et utiliser un langage clair et simple. Cette disposition devrait aussi indiquer que cette politique doit être facilement accessible sur le site internet d'Europol ainsi que les sites internet des autorités nationales de contrôle;
f. étant donné que l'article 41 ne définit pas clairement la responsabilité de tous les acteurs concernés, il convient, en ce qui concerne l'article 41, paragraphe 4, de préciser que la responsabilité en matière de respect de tous les principes applicables en matière de protection des données (et pas uniquement la «légalité du transfert») appartient à l'expéditeur des données. Le CEPD recommande de modifier l'article 41 en conséquence;

g. ajouter dans les dispositions essentielles de la proposition que: i) une évaluation d'impact similaire à celle décrite dans la proposition de règlement sur la protection des données est menée pour tous les traitements relatifs aux données à caractère personnel, ii) les principes de protection des données dès la conception et de protection des données par défaut sont appliqués à la création ou à l'amélioration des systèmes de traitement des données à caractère personnel, iii) le responsable adopte des politiques et prend des mesures appropriées pour veiller au respect des règles relatives à la protection des données, et être en mesure de prouver ce respect, et pour assurer le contrôle de l'efficacité des mesures, et iv) le DPD d'Europol et, si nécessaire, les autorités de contrôle participent aux discussions sur le traitement des données à caractère personnel.

Il a également formulé quelques suggestions concernant la communication adoptée parallèlement à la proposition.

.

Fait à Bruxelles, le 31 mai 2013

(signé)

Peter HUSTINX

Contrôleur européen de la protection des données

Annexe 1: Observations sur les incidences financières de la proposition

Le CEPD a analysé avec soin les avis de la Commissions concernant l'incidence que le contrôle d'Europol pourrait avoir pour l'institution, en ce qui concerne tant les ressources financières que les ressources humaines.

Le CEPD avait déjà analysé cette incidence potentielle dans le cadre du cadre financier pluriannuel (2014-2020) et avait envoyé son avis à la Commission et à l'autorité budgétaire fin mars 2013 à la suite de la procédure budgétaire. Cet avis se fondait sur les hypothèses suivantes:

- **Objectif général**: contrôler le respect, par les agences de l'ancien troisième pilier, des règles relatives à la protection des données et veiller à ce respect. Des estimations budgétaires ont été faites sur la base du scénario le plus probable à l'époque (à savoir, le contrôle d'une agence, prenant effet en 2016).

- **Objectifs spécifiques**: réaliser des activités de contrôle relatives tant au traitement des données concernant le personnel qu'aux données relatives aux activités principales.

    1. Contrôle du traitement des données concernant le personnel: ce contrôle n'aura pas d'incidence considérable sur le budget dans la mesure où il sera inclus dans les activités de contrôle du CEPD.

    2. Contrôle des activités principales d'Europol: cette tâche comprendra des activités comme:
        - des réunions de coordination avec les autorités nationales chargées de la protection des données (1 jour, Bruxelles);
        - au moins 1 inspection par an (5 jours, La Haye);
        - des réunions relatives à l'inspection annuelle, 3 fois par an (1 jour, La Haye);
        - publication et traduction de rapports/procès-verbaux de réunions et d'avis.

L'allocation de ressources humaines et financières complémentaires sera absolument nécessaire en vue de réaliser ces objectifs spécifiques. Des crédits supplémentaires seront nécessaires pour couvrir les coûts des missions, l'organisation de réunions et la préparation, la traduction et la publication de documents et au moins trois équivalents temps plein (1 AD6, 1 AST3 et 1 END/AC) seront nécessaires.

Le tableau contenant les calculs détaillés des coûts qui a été produit dans le cadre du cadre financier pluriannuel est joint à la présente annexe pour information.

Une comparaison entre les estimations comprises dans la proposition de la Commission et les prévisions du CEPD montre quelques similitudes et une différence importante. En ce qui concerne les besoins estimés en matière de dépenses administratives supplémentaires (page 92 de la proposition de la Commission), les coûts prévus pour les réunions et les missions sont semblables dans les deux propositions. En revanche, les estimations des coûts relatifs aux publications et aux traductions sont différentes parce que les prévisions du CEPD incluent une éventuelle publication au Journal officiel.

En ce qui concerne les besoins estimés en ressources humaines (page 91 de la proposition de la Commission), il semble que le nombre minimal de postes nécessaires pour mener les activités de contrôle ait été fortement sous-estimé dans la proposition de la Commission. Sur la base de notre expérience dans ce type d'activités, nous estimons qu'au moins trois équivalents temps plein sont strictement nécessaires pour atteindre les objectifs (voir, par exemple, les estimations de la Commission elle-même pour les activités autres que le contrôle, qui prévoient cinq équivalents temps plein).

Sur la base de ces considérations, nous recommanderions que les coûts raisonnables estimés par le CEPD et communiqués à l'autorité budgétaire dans le cadre du cadre financier pluriannuel soient pris en considération et que la proposition de la Commission soit modifiée en conséquence.

MFF 2014-2020 - EUROPOL SUPERVISION

	Persons	Days	Times/ year	Daily allowance	Hotel	Transport	Eurest	2013	2014	2015	2016	2017	2018	2019	2020	MFF 2014-2020
Gneral objective: monitor and ensure compliance with the DP rules of ex 3rd pillar agencies																
3 Coordination meetings in Bxl with national DPAs (meetings)	27	1	3	92	2.700	48.600	364	59.116,14	-	-	62.734,52	63.989,21	65.269,00	66.574,38	67.905,86	326.472,97
1 Inspection (5 days) at The Hague (DPAs experts - meetings)	8	5	1	93	6.800	4.800		15.320,00	-	-	16.257,71	16.582,86	16.914,52	17.252,81	17.597,86	84.605,76
Subtotal meetings								**74.436,14**	**-**	**-**	**78.992,23**	**80.572,07**	**82.183,51**	**83.827,18**	**85.503,73**	**411.078,72**
1 Inspection (5 days) at The Hague (EDPS staff - missions)	2	5	1	93	1.700	250		2.880,00	-	-	3.056,28	3.117,40	3.179,75	3.243,35	3.308,21	15.905,00
3 Meetings at The Hague in connection with the annual inspection (EDPS staff - missions)	2	1	3	93	1.020	750		2.328,00	-	-	2.470,49	2.519,90	2.570,30	2.621,71	2.674,14	12.856,54
Subtotal missions								**5.208,00**	**-**	**-**	**5.526,77**	**5.637,31**	**5.750,05**	**5.865,05**	**5.982,35**	**28.761,54**
Publications								**20.460,01**			**21.712,33**	**22.146,57**	**22.589,50**	**23.041,29**	**23.502,12**	**112.991,82**
Translations								**132.308,06**			**140.406,38**	**143.214,50**	**146.078,79**	**149.000,37**	**151.980,38**	**730.680,42**
Total other administrative expenditure								**232.412,21**	**-**	**-**	**246.637,70**	**251.570,45**	**256.601,86**	**261.733,90**	**266.968,58**	**1.283.512,50**
Staff																
1 AD7											96.000,00	99.360,00	102.837,60	106.436,92	110.162,21	514.796,72
1 AST5											84.000,00	86.940,00	89.982,90	93.132,30	96.391,93	450.447,13
1 END / 1 AC											60.000,00	62.100,00	64.273,50	66.523,07	68.851,38	321.747,95
Total staff cost								**-**	**-**	**-**	**240.000,00**	**248.400,00**	**257.094,00**	**266.092,29**	**275.405,52**	**1.286.991,81**
GRAND TOTAL								**232.412,21**	**-**	**-**	**486.637,70**	**499.970,45**	**513.695,86**	**527.826,19**	**542.374,10**	**2.570.504,31**

MFF 2014-2020 EUROPOL SUPERVISION	CFP 2010-2020 CONTRÔLE EUROPOL
Persons	Personnes
Days	Jours
Times/year	Fois/an
Daily allowance	Indemnité journalière
Hotel	Hôtel
Transport	Transport
Eurest	Eurest
General objective: monitor and ensure compliance with the DP rules of ex 3rd pilar agencies	Objectif général: contrôler le respect, par les agences de l'ancien 3e pilier, des règles relatives à la protection des données et veiller à ce respect
3 coordination meeting in Bxl with national DPAs (meetings)	3 réunions de coordination à Bruxelles avec les délégués nationaux à la protection des données (réunions)
1 inspection (5 days) at The Hague (DPAs experts – meetings)	1 inspection (5 jours) à La Haye (délégués nationaux à la protection des données – réunions)
Subtotal meetings	Sous-total réunions
1 inspection (5 days) at The Hague (EDPS staff – missions)	1 inspection (5 jours) à La Haye (personnel du CEPD – missions)
3 meetings at The Hague in connection with the annual inspection (EDPS staff – mission)	3 réunions à La Haye relatives à l'inspection annuelle (personnel du CEPD – mission)
Subtotal missions	Sous-total missions
Publications	Publications
Translations	Traductions
Total of other administrative expenditure	Total autres dépenses administratives
Staff	personnel
1 AD7	1 AD7
1 AST5	1 AST5
1 END/1AC	1 END/AC
Total staff cost	Total coût personnel
GRAND TOTAL	Total général