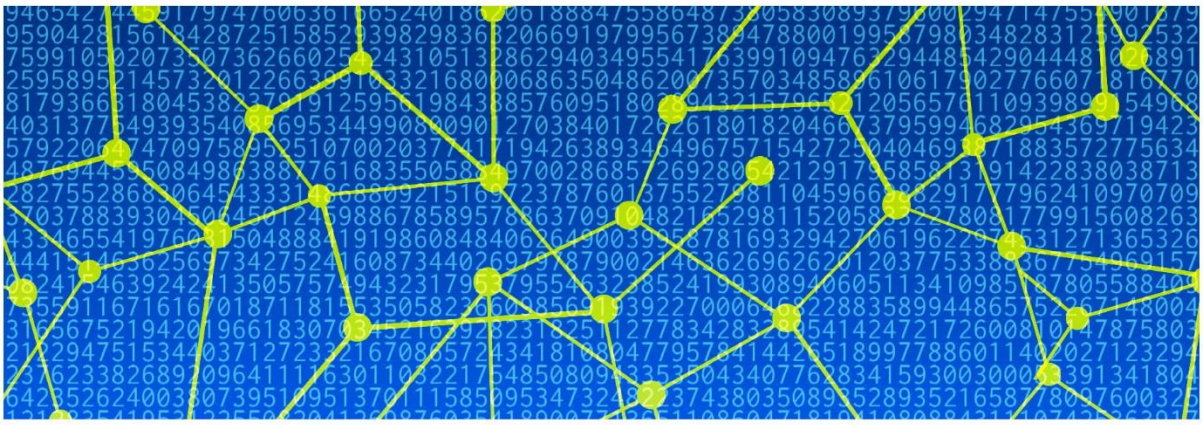

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 07/2016

Avis du CEPD sur le premier paquet de mesures pour une réforme du régime d'asile européen commun (Eurodac, EASO et règlement de Dublin)

21 septembre 2016

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE chargée en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001 «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel, de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis se rapporte à la mission du CEPD de conseil des institutions de l'UE sur les implications de leurs politiques en matière de protection des données et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Le CEPD considère que la conformité aux exigences en matière de protection des données est un élément essentiel du premier paquet de mesures de l'UE pour améliorer le régime d'asile européen commun (RAEC).

Résumé

Depuis plusieurs années, l'Europe est confrontée à une crise migratoire et des réfugiés dont l'urgence est préoccupante, et qui s'est encore aggravée en 2015. La Commission a par conséquent proposé de réformer le règlement de Dublin afin de l'adapter à la situation actuelle. Cette réforme s'accompagne d'une proposition de création d'une Agence de l'Union européenne pour l'asile, afin d'aider les États membres à accomplir leurs devoirs en matière d'asile.

Depuis sa création, Eurodac permet de fournir des preuves dactyloscopiques en vue de déterminer l'État membre auquel il incombe d'examiner la demande d'asile introduite au sein de l'UE.

La Commission a également proposé une refonte du règlement Eurodac. Le principal changement opéré dans ce règlement concerne l'extension du champ d'application d'Eurodac pour enregistrer les ressortissants de pays tiers se trouvant illégalement sur le territoire d'un État membre ou appréhendés dans le cadre du franchissement irrégulier d'une frontière séparant un État membre d'un pays tiers.

Le CEPD reconnaît la nécessité d'une gestion plus efficace de la migration et de l'asile dans l'UE. Toutefois, il recommande des améliorations importantes de façon à mieux prendre en considération les droits et intérêts légitimes des personnes concernées susceptibles d'être affectées par le traitement de données à caractère personnel et, notamment, des groupes vulnérables de personnes nécessitant une protection spécifique, comme les migrants et les réfugiés.

Dans son avis, le CEPD recommande, entre autres, les principaux points suivants:

– mentionner, dans le règlement de Dublin, que l'instauration de l'utilisation d'un identifiant unique dans la base de données de Dublin ne peut en aucun cas servir à d'autres fins que celles décrites dans le règlement de Dublin;

– mener une évaluation complète des répercussions en matière de protection des données et de respect de la vie privée de la refonte du règlement Eurodac de 2016, afin de mesurer l'incidence sur le respect de la vie privée du nouveau texte proposé et de l'extension du champ d'application de la base de données Eurodac;

– réaliser, sur la base d'une étude cohérente ou d'une approche fondée sur des données probantes, une évaluation de la nécessité de collecter et d'utiliser les images faciales des catégories de personnes visées dans la refonte du règlement Eurodac de 2016, et de la proportionnalité de cette collecte;

– effectuer, en complément de l'exposé des motifs, une évaluation détaillée de la situation des mineurs et définir l'équilibre entre les risques et les préjudices inhérents à la procédure de relevé des empreintes digitales des mineurs et les avantages dont ceux-ci peuvent bénéficier.

L'avis définit en outre d'autres lacunes des différentes propositions et contient des recommandations complémentaires en matière de protection des données et de respect de la vie privée, qui devraient être prises en considération au cours du processus législatif.

TABLE DES MATIÈRES

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,

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

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

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION ET CONTEXTE

1. En avril 2016, la Commission a adopté une communication intitulée «Vers une réforme du régime d'asile européen commun et une amélioration des voies d'entrée légale en Europe»[1], qui définissait les priorités aux fins de l'amélioration du régime d'asile européen commun (RAEC). Dans ce contexte, le 4 mai 2016, la Commission a formulé trois propositions dans le cadre du premier paquet de mesures pour la réforme du RAEC:

- une proposition de règlement du Parlement européen et du Conseil sur l'établissement de critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (ci-après la «proposition sur le règlement de Dublin»)[2];
- une proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour l'asile et abrogeant le règlement (UE) nº 439/2010 (ci-après la «proposition sur l'Agence de l'Union européenne pour l'asile» ou «proposition sur l'AUEA»)[3]; et
- une proposition de règlement du Parlement européen et du Conseil relatif à la modification du règlement (UE) nº 603/2013 concernant la création d'«Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace du [règlement nº 604/2013] établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride, et de l'identification des ressortissants de pays tiers ou apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives (refonte 2016) (ci-après «la proposition de refonte du règlement Eurodac de 2016»)[4].

2. Le CEPD a été consulté de façon informelle avant la publication de la refonte du règlement Eurodac et de la proposition sur l'EASO et a transmis à la Commission des observations informelles sur les deux textes.

3. Le CEPD comprend que l'UE doit relever les défis posés par la crise migratoire et des réfugiés depuis 2015 et disposer d'une politique efficace et harmonisée afin de lutter contre l'immigration illégale au sein de l'Union européenne ou vers celle-ci. Dans le plein respect du rôle du législateur consistant à évaluer la nécessité et la proportionnalité des mesures proposées, le CEPD, dans son rôle consultatif, fournira dans le présent avis certaines recommandations en matière de protection des données et de respect de la vie privée, afin d'aider le législateur à respecter les exigences énoncées aux articles 7 et 8 de la Charte des droits fondamentaux, concernant les droits au respect de la vie privée et à la protection des données, ainsi qu'à l'article 16 du traité sur le fonctionnement de l'Union européenne.

4. Le CEPD formulera en premier lieu les recommandations principales à l'égard des trois propositions. Ces recommandations principales portent sur les problèmes majeurs constatés par le CEPD et qui doivent obligatoirement être examinés lors du processus législatif. Les recommandations complémentaires concernent les éléments pour lesquels le CEPD a estimé qu'une clarification, des informations supplémentaires ou des modifications mineures étaient nécessaires. Cette distinction devrait aider le législateur à donner la priorité aux problèmes majeurs abordés dans le présent avis.

II. RECOMMANDATIONS PRINCIPALES DU CEPD

II.1. La proposition sur le règlement de Dublin

5. La proposition sur le règlement de Dublin vise à:

- renforcer la capacité du régime d'asile européen commun à déterminer de manière efficiente et efficace un seul État membre responsable de l'examen d'une demande de protection internationale;

- compléter le système actuel par un mécanisme d'attribution correcteur, pour les cas où certains États membres doivent faire face à un nombre disproportionné de demandeurs d'asile; et

- décourager les abus et empêcher les mouvements secondaires de demandeurs au sein de l'Union, en prévoyant notamment explicitement l'obligation pour les demandeurs de demander l'asile dans l'État membre de première entrée et de demeurer dans l'État membre désigné responsable.

6. Les remarques qui suivent concerneront en particulier les modifications du règlement de Dublin qui ont une incidence sur la protection des données et le respect de la vie privée des personnes physiques.

7. La proposition instaure un nouveau système centralisé d'enregistrement et de suivi qui permet l'enregistrement de toutes les demandes et le suivi de la part de chaque État membre dans l'ensemble des demandes. Aux fins de cette nouvelle base de données, administrée par

eu-LISA, chaque État membre enregistre la demande dans le système automatisé, qui conservera chaque demande sous un numéro unique[5].

8. Le CEPD prend note du fait que la refonte du règlement de Dublin dresse une liste exhaustive des données susceptibles d'être conservées dans le dossier électronique de chaque demandeur (article 23)[6]. La liste paraît, de prime abord, correspondre à l'objectif du règlement de Dublin, c'est-à-dire assurer un accès rapide à une procédure d'asile pour les demandeurs d'asile et l'examen des demandes par un État membre unique et clairement déterminé.

9. Toutefois, l'utilisation d'un identifiant unique pour le dossier de chaque demandeur nécessite des dispositifs de protection spécifiques, dans la mesure où il devient plus facile de contrôler une personne au moyen de plusieurs bases de données (notamment dans des domaines autres que celui de l'asile), et parce que cela peut aussi permettre le profilage d'une personne sur la base de son identifiant unique. Afin d'empêcher une utilisation malveillante des données, le recours à un identifiant unique doit être limité à des objectifs, un contexte et un environnement spécifiques. Par conséquent, **le CEPD recommande de mentionner dans le règlement que l'identifiant unique ne peut en aucun cas être utilisé à d'autres fins que celles décrites dans le règlement de Dublin**, dans le plein respect du principe de limitation de la finalité.

II.2. La proposition de refonte du règlement Eurodac de 2016

10. Les remarques qui suivent concerneront en particulier les modifications du règlement Eurodac qui ont une incidence sur la protection des données et le respect de la vie privée.

a) L'extension du champ d'application d'Eurodac

11. La refonte du règlement Eurodac de 2016 étend le champ d'application de la base de données Eurodac d'origine. Eurodac a été initialement créée afin de fournir des preuves dactyloscopiques permettant de déterminer l'État membre responsable de l'examen d'une demande d'asile présentée dans l'Union. Son objectif premier a toujours été de contribuer à la mise en œuvre du règlement de Dublin.

12. L'extension du champ d'application d'Eurodac, telle que proposée dans la refonte 2016, étend son champ d'application aux fins de l'identification des ressortissants de pays tiers en séjour irrégulier et de ceux qui sont entrés illégalement sur le territoire de l'Union européenne par les frontières extérieures, afin que les États membres puissent utiliser ces informations pour délivrer à un ressortissant de pays tiers de nouveaux documents en vue de son retour.

13. Ce nouvel objectif d'Eurodac a été décrit à l'article 1er, point b), de la proposition de refonte: *«contribuer au contrôle de l'immigration illégale vers l'Union et des mouvements secondaires au sein de celle-ci ainsi qu'à l'identification des ressortissants de pays tiers en séjour irrégulier, afin de définir les mesures appropriées qui doivent être prises par les États membres, notamment l'éloignement et le rapatriement des personnes séjournant sans autorisation».*

14. L'extension du champ d'application d'Eurodac est encore plus importante du point de vue du respect de la vie privée et de la protection des données à la lumière de la communication de la Commission sur des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, qui souligne la nécessité d'améliorer l'interopérabilité des systèmes

d'information en tant qu'objectif à long terme[7]. Le CEPD suivra de près et avec la plus grande attention la tendance visant à faire communiquer entre elles les différentes bases de données disponibles, à étendre leurs objectifs initiaux et à créer plus de possibilités pour une collecte massive d'informations ciblant certaines catégories de personnes. Le CEPD a l'intention de traiter la question de l'interopérabilité dans un document distinct, qui sera bientôt adopté.

15. De l'avis du CEPD, l'objectif décrit à l'article 1, point b), reste vague, car il ne précise pas les mesures spécifiques que les États membres peuvent prendre en complément de l'éloignement et du rapatriement. Étant donné que la portée et la finalité du traitement des données à caractère personnel doivent être définies le plus rigoureusement possible, **le CEPD recommande de préciser davantage le type de mesures qui peuvent être prises par un État Membre dans ce contexte[8]**, en incluant par exemple une liste exhaustive des mesures qui peuvent être prises grâce à la base de données Eurodac par rapport aux finalités poursuivies. Une telle explication permettrait de comprendre quelle est la valeur ajoutée apportée par la base de données Eurodac.

16. Comme cela a déjà été évoqué dans plusieurs avis du CEPD[9], l'extension de **la finalité d'une base de données pose la question du principe de limitation de la finalité**, en vertu duquel les données doivent être utilisées conformément aux finalités initiales en vue desquelles elles ont été collectées. **Le CEPD exprime des préoccupations quant à l'extension du champ d'application de la base de données Eurodac, qui avait été initialement conçue pour contribuer à la mise en œuvre du règlement de Dublin.**

17. **L'extension du champ d'application de la base de données Eurodac ne suscite pas uniquement** des inquiétudes à l'égard du principe de limitation de la finalité, mais également **concernant la proportionnalité du traitement**: une base de données, considérée comme proportionnée lorsqu'elle est utilisée pour une finalité particulière, peut devenir inadéquate ou excessive lorsque l'utilisation est étendue à d'autres finalités par la suite[10].

18. Le CEPD regrette que la refonte ne mentionne aucune évaluation des répercussions des nouvelles dispositions à l'égard de la proportionnalité des mesures (c'est-à-dire: quel type de mesures peuvent être prises une fois que les personnes ont été identifiées comme étant en situation irrégulière?). Une telle évaluation des répercussions semble être une condition essentielle afin d'apprécier de façon adéquate une politique de l'UE qui aura une incidence notable sur les personnes concernées par la base de données. Les seules déclarations contenues dans l'exposé des motifs, renvoyant au principe de respect de la vie privée dès la conception[11] ou aux droits fondamentaux[12], n'expliquent pas en substance pourquoi des mesures moins intrusives n'auraient pas pu mieux convenir à l'approche suivie par la proposition, ou comment la proposition pourrait réduire son incidence sur les droits au respect de la vie privée et à la protection des données. **Le CEPD recommande par conséquent que la Commission mette à disposition une évaluation complète des répercussions en matière de protection des données et de respect de la vie privée dans la refonte du règlement Eurodac de 2016 afin de mesurer l'incidence du nouveau texte proposé sur le respect de la vie privée[13].** Le CEPD remarque, dans ce contexte, qu'un tel exercice a été réalisé pour le deuxième train de mesures «Frontières intelligentes», comme cela a été souligné et salué dans l'avis du CEPD sur le deuxième train de mesures de l'UE «Frontières intelligentes», publié le même jour que le présent avis.

b) L'obligation de relever des empreintes digitales et de capturer des images faciales

- ***L'utilisation de données biométriques supplémentaires: l'image faciale***

19. Actuellement, le règlement Eurodac exige uniquement le relevé et la conservation des empreintes digitales des demandeurs d'une protection internationale dans le système central Eurodac. La proposition ajoute un autre type de donnée biométrique: l'image faciale des personnes.

20. Le CEPD remarque que la proposition n'explique pas le choix d'utiliser des données biométriques supplémentaires, en particulier l'image faciale aux fins de la reconnaissance faciale. L'exposé des motifs renvoie à la communication de la Commission sur un agenda européen en matière de migration[14], dans laquelle il serait suggéré d'ajouter des données biométriques à Eurodac afin d'atténuer certaines des difficultés auxquelles les États membres sont confrontés concernant les empreintes endommagées et le non-respect du processus de relevé des empreintes digitales. Toutefois, la communication de la Commission ne contient aucune référence au cas des empreintes digitales endommagées et ne peut dès lors servir à justifier la collecte d'images faciales.

21. En outre, dans la mesure où les données biométriques sont hautement sensibles, leur collecte et leur utilisation doivent être soumises à une analyse stricte avant de décider de les enregistrer dans une base de données générale, dans laquelle les données à caractère personnel d'un grand nombre de personnes seront traitées. À cet égard, la proposition prévoit qu'eu-LISA réalise une étude sur les logiciels de reconnaissance faciale, afin d'évaluer la précision et la fiabilité avant que le logiciel ne soit intégré au système central[15]. Le CEPD considère qu'une telle évaluation aurait dû être réalisée avant d'inclure ces données et le logiciel de reconnaissance faciale dans la base de données Eurodac.

22. L'évaluation menée par eu-LISA est purement technique et la proposition ne contient ni ne prévoit aucune évaluation portant sur la nécessité d'inclure la reconnaissance faciale. Par conséquent, compte tenu des risques posés par l'intégration de telles données sensibles dans une base de données de grande envergure, **le CEPD recommande la conduite ou la mise à disposition d'une évaluation portant sur la nécessité de collecter et d'utiliser les images faciales des catégories de personnes concernées par la proposition de refonte du règlement Eurodac et sur la proportionnalité de cette collecte, sur la base d'une étude cohérente ou d'une approche fondée sur des données probantes[16].**

23. Par ailleurs, le CEPD remarque que les articles 15 et 16 de la proposition semblent contradictoires: alors que l'article 15 prévoit que l'État membre et eu-LISA doivent assurer une comparaison systématique des empreintes digitales et de l'image faciale, l'article 16 prévoit que la reconnaissance faciale doit uniquement être utilisée en dernier ressort, lorsque la qualité des empreintes digitales ne permet pas une comparaison ou lorsque la personne refuse de se soumettre au relevé des empreintes. **Le CEPD recommande d'expliquer que la comparaison des empreintes digitales et/ou des images faciales doit être uniquement réalisée en dernier ressort.**

- ***L'abaissement de l'âge minimal pour le relevé des empreintes digitales***

24. La proposition prévoit un nouvel âge minimal pour le relevé de données biométriques effectué sur les enfants. Cet âge sera à présent de 6 ans, au lieu de 14 ans précédemment, sur la base d'un rapport du Centre commun de recherche[17] qui indique que les empreintes digitales

relevées chez les enfants âgés de six ans et plus peuvent être utilisées dans des applications de recherche de concordance automatisée telles qu'Eurodac si des précautions suffisantes sont prises pour obtenir des images de bonne qualité.

25. Le considérant 20 bis dispose que «*les ressortissants de pays tiers considérés comme étant des personnes vulnérables et les mineurs ne devraient pas être contraints de donner leurs empreintes digitales ou leur image faciale.*». L'article 2, paragraphe 2, prévoit que le processus de relevé des empreintes digitales des enfants est réalisé d'une manière adaptée aux enfants et tenant compte de leur spécificité et que les enfants sont informés de manière adaptée à leur âge et sont accompagnés d'un adulte.

26. Le CEPD salue ces mesures de précaution, étant donné que les mineurs de moins de 14 ans sont vulnérables et ne sont pas à même de comprendre intégralement les circonstances entourant le traitement de leurs données, particulièrement lorsque ces données sont aussi sensibles que des informations biométriques. Le CEPD comprend les raisons pour lesquelles cet âge a été abaissé, telles qu'elles sont expliquées dans l'exposé des motifs[18], par rapport aux cas d'enfants séparés de leur famille ou s'échappant des établissements de soins ou des services sociaux à l'enfance.

27. Toutefois, l'argument principal utilisé dans la proposition, à savoir que de nombreux États membres collectent les données biométriques de mineurs n'ayant pas encore 14 ans pour les visas, les passeports, les titres de séjour comportant des éléments biométriques, et pour le contrôle de l'immigration en général, n'est pas convaincant en tant que tel. Le simple fait que certains États membres ont adopté cette pratique ne signifie pas qu'une telle mesure soit efficace, proportionnée et utile. Le **CEPD recommande que l'exposé des motifs fournisse une évaluation plus détaillée de la situation des mineurs et définisse de manière plus approfondie l'équilibre entre les risques et les préjudices inhérents à une telle procédure pour les mineurs et les avantages dont ceux-ci peuvent bénéficier. En outre, le CEPD recommande de préciser ce qui est entendu par les termes «d'une manière adaptée aux enfants», étant donné que cette formulation peut donner lieu à des interprétations multiples en fonction de l'autorité compétente.**

c) La durée de conservation

28. En vertu de l'article 18, paragraphes 2 et 3, les catégories de données visées à l'article 14, paragraphe 1, et à l'article 17, paragraphe 1, seront conservées pour une durée de cinq ans. Afin de justifier cette nouvelle obligation de conservation de ces catégories de données, l'exposé des motifs renvoie au fait qu'Eurodac n'est plus seulement une base de données concernant les demandeurs d'asile et qu'une telle durée de conservation est nécessaire pour permettre un contrôle suffisant de l'immigration irrégulière et des mouvements secondaires à l'intérieur et à destination de l'UE.

29. En outre, selon l'exposé des motifs, la durée de cinq ans correspond à la durée maximale d'une interdiction d'entrée imposée à une personne à des fins de gestion de la migration, telle qu'elle est prévue dans la directive «retour»[19], à la durée de conservation des données relatives à un visa (règlement VIS[20]), et à la durée proposée pour la conservation des données dans le système d'entrée/sortie[21].

30. Conformément au droit de l'UE en matière de protection des données, les données à caractère personnel doivent uniquement être conservées pendant une durée n'excédant pas celle

nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement[22]. Le CEPD considère qu'une référence à la durée de conservation d'un autre instrument n'est pas pertinente en tant que telle, dans la mesure où lesdits instruments peuvent avoir des finalités différentes et où leur durée de conservation peut être justifiée par d'autres éléments. Le considérant 33 de la proposition fait également référence au droit à la protection des données à caractère personnel, en tant qu'élément ayant été pris en considération afin de déterminer la durée de conservation de cinq ans proposée. Toutefois, le considérant n'expose pas comment le droit à la protection des données a été pris en considération afin de définir la durée de conservation.

31. **Pour toutes ces raisons, le CEPD considère que la durée de conservation de cinq ans n'est pas suffisamment justifiée dans la proposition et recommande de fournir plus de détails et d'explications quant à la nécessité, dans ce contexte, de cette durée de cinq ans (et non d'une durée plus longue ou plus courte) afin d'atteindre les nouveaux objectifs de la base de données Eurodac. En outre, le CEPD recommande d'expliquer plus en détail comment il a été tenu compte de la protection des données en pratique.**

32. Par ailleurs, même s'il était justifié, en principe, de faire correspondre la durée de conservation desdites données avec la durée maximale théorique aux fins de l'imposition d'une interdiction d'entrée (à savoir, cinq ans), dans un tel cas, la durée de conservation devrait correspondre à la durée *réelle* de l'interdiction d'entrée imposée à un ressortissant d'un pays tiers donné, qui peut être inférieure à cinq ans. Cela signifie qu'une fois que l'interdiction d'entrée d'une personne a expiré, les informations relatives à cette personne doivent être effacées de la base de données Eurodac, et non uniquement après la période de cinq ans, qui représente la durée maximale théorique. **Le CEPD recommande par conséquent de réduire en tout état de cause la durée de conservation à la durée réelle de l'interdiction d'entrée imposée à une personne spécifique, qui peut aller jusqu'à cinq ans.**

33. Enfin, le début de la période de conservation est censée être la date à laquelle les empreintes digitales ont été relevées[23]. Toutefois, les empreintes peuvent être relevées plusieurs fois, par différents opérateurs, pouvant même se trouver dans plusieurs États membres différents. Si le relevé d'empreintes est lié au franchissement irrégulier d'une frontière pour la première fois[24], il peut être répété plusieurs fois ultérieurement si le migrant séjourne illégalement sur le territoire d'un État membre[25]. Avec cette formulation, le CEPD comprend que la durée de conservation peut être actualisée à chaque fois qu'une personne est appréhendée en lien avec le franchissement illégal d'une frontière ou sur le territoire d'un État membre. Cela conduirait à une durée de conservation théoriquement illimitée. Pour cette raison, **le CEPD recommande de préciser dans la proposition que le début de la durée de conservation est la date du traitement du premier relevé d'empreintes digitales réalisé par un État membre.**

d) L'accès à des fins répressives

34. Alors que l'accès à des fins répressives aux données concernant les demandeurs d'une protection internationale est verrouillé (elles sont alors «non accessibles») après trois ans, tel n'est pas le cas des données de personnes qui ne demandent pas de protection internationale, ou auxquelles celle-ci n'est pas accordée[26]. L'explication fournie dans l'exposé des motifs[27] fait référence à la probabilité du renouvellement du titre de séjour, qui serait plus élevée pour les demandeurs d'asile que pour les personnes n'introduisant pas cette demande.

35. Le CEPD ne comprend pas pourquoi les autorités répressives devraient avoir un accès prolongé aux catégories de données concernant des individus ne bénéficiant pas d'une protection internationale. Il n'existe aucune indication ou preuve que cette catégorie de personnes fasse davantage l'objet d'enquêtes de la part des autorités répressives que les demandeurs d'asile ayant obtenu une protection internationale. En outre, la simple probabilité d'un renouvellement du titre de séjour ne peut justifier une telle différence de traitement. **Par conséquent, le CEPD recommande d'adopter la même période de trois ans déjà en vigueur à l'égard du verrouillage de l'accès à des fins répressives aux données concernant les deux catégories de personnes.**

III. RECOMMANDATIONS COMPLÉMENTAIRES

III.1. La proposition de refonte du règlement Eurodac

a) L'effacement anticipé et le marquage des données

36. Actuellement, le règlement Eurodac prévoit que les données relatives aux ressortissants de pays tiers en séjour irrégulier qui ne déposent pas de demande d'asile dans l'Union européenne sont, dans certains cas, effacées de manière anticipée, ce qui signifie que leurs données sont supprimées avant la fin de la période de conservation de 18 mois. Cette suppression anticipée se produit une fois qu'un permis de résidence ou la nationalité d'un État membre est acquis ou lorsque la personne a quitté le territoire des États membres.

37. La proposition de refonte du règlement Eurodac prévoit que les données ne seront plus effacées de manière anticipée pour les ressortissants de pays tiers ou apatrides en séjour irrégulier auxquels un document de séjour a été accordé ou qui ont quitté le territoire de l'Union européenne. Selon l'exposé des motifs, «*[i]l est en effet nécessaire de conserver ces données, pour le cas où une personne resterait sur le territoire alors que son document de séjour, qui ne confère normalement qu'une autorisation temporaire, a expiré, ou pour le cas où un ressortissant de pays tiers tenterait d'entrer à nouveau dans l'UE de manière irrégulière après son retour dans un pays tiers*».

38. Au lieu d'être supprimées de manière anticipée, la proposition de refonte du règlement Eurodac prévoit que les données des migrants ayant reçu un document de résidence seront «marquées»[28]. Le CEPD aimerait faire remarquer que le terme «marquage» n'est pas défini dans le règlement Eurodac et que la proposition de refonte n'indique pas le type d'informations que ce marquage doit contenir. Par conséquent, **le CEPD recommande de définir ce qui est entendu par «marquage» dans le règlement Eurodac et d'indiquer les informations devant être contenues dans ledit marquage.**

39. À des fins répressives, le marquage des données semble être une mesure intermédiaire entre la pleine utilisation des données aux fins initialement prévues et l'effacement des données. Dans ce cas, cela signifie que les données resteront accessibles à des fins répressives. Toutefois, pour les catégories des ressortissants d'un pays tiers en séjour irrégulier ou des apatrides[29], un marquage en vertu de l'article 19, paragraphe 4, aurait une autre fonction, à savoir la transmission du statut d'une personne titulaire d'un titre de séjour dans un État membre aux autorités d'un autre État membre. Par conséquent, **le CEPD recommande également de définir dans la proposition de refonte quels sont les objectifs du marquage des données et**

d'expliquer la distinction entre le marquage à des fins répressives[30] et celui aux fins du contrôle de l'immigration[31].

40. Les données relatives aux personnes ayant obtenu un titre de séjour dans un État membre resteraient alors dans la base de données Eurodac, assorties d'un marquage, tandis que les données relatives à une personne ayant acquis la nationalité d'un État membre seront supprimées de la base de données dès que l'État membre d'origine sera informé que la personne concernée a acquis ladite nationalité. Une troisième catégorie de personnes, les demandeurs d'asile auxquels a été accordée une protection internationale, sera enregistrée dans la base de données Eurodac pendant cinq ans, mais l'accès à leurs données par les autorités répressives sera limité à trois ans.

41. Le CEPD considère qu'un tel écart de traitement entre différentes catégories de ressortissants de pays tiers, à l'égard de l'accès à leurs données à des fins répressives, n'est pas expliqué de manière satisfaisante dans la proposition. En effet, rien ne prouve la nécessité, à des fins répressives, d'une durée d'accès plus longue pour les personnes séjournant légalement et pourvues d'un titre de séjour que pour les personnes auxquelles une protection internationale a été accordée. **Le CEPD recommande par conséquent d'étendre l'application de la durée limitée de l'accès à des fins répressives (trois ans) aux personnes auxquelles un titre de séjour a été accordé par un État membre.**

42. **En outre, le CEPD recommande d'imposer à chaque État membre accordant ou reconnaissant la nationalité à une personne de transmettre cette information à eu-LISA, afin que les données relatives à la personne concernée puissent être effacées d'Eurodac de façon systématique et automatique.** Le libellé de l'article 18, paragraphe 1, peut en effet suggérer que l'effacement anticipé des données d'un ancien ressortissant d'un pays tiers ne pourrait pas intervenir immédiatement, étant donné qu'il dépend des informations détenues par l'État membre d'origine.

b) Les transferts internationaux et le traitement ultérieur

43. L'article 37 de la proposition fait référence à une interdiction générale de transférer les données à caractère personnel obtenues conformément à la proposition à tout pays tiers, toute organisation internationale ou toute entité de droit privé établie ou non dans l'Union. En vertu de cette disposition, la même interdiction doit s'appliquer à tout traitement ultérieur des données au niveau national au sens de l'article 3 de la directive 2016/680[32].

44. Les raisons expliquant la mention de la seule directive 2016/680 ne sont pas claires: le traitement des données à caractère personnel est également réglementé en des termes identiques par la directive 95/46, qui sera remplacée par le règlement général sur la protection des données (règlement 2016/679)[33] en mai 2018. Dans les cas où le traitement se produit dans un contexte répressif et d'asile/d'immigration, la directive 2016/680 et le règlement général sur la protection des données pourraient même être applicables en même temps.

45. On pourrait penser que la dernière partie de ce paragraphe visait à éviter toute utilisation ultérieure des données collectées conformément au règlement Eurodac par toute autre entité à toute fin autre que les objectifs cités à l'article 1er de la proposition. Si tel est le cas, le CEPD tient à rappeler que le principe de limitation de la finalité est consacré à l'article 5, point b), du

règlement 2016/679 et à l'article 4, point b), de la directive 2016/680. Par conséquent, une référence à ces dispositions pourrait clarifier l'objectif du texte.

46. Pour ces raisons, **le CEPD recommande de préciser la signification de la dernière partie du premier paragraphe de l'article 37** et de la rendre conforme au nouveau cadre de la protection des données qui entrera en vigueur et sera appliqué en mai 2018, en faisant par exemple référence, d'une part, au principe de limitation de la finalité et, d'autre part, aux principes relatifs aux transferts internationaux (une telle référence figure déjà au paragraphe 4).

47. En outre, l'articulation entre les principes généraux aux fins des transferts internationaux, tels qu'indiqués aux paragraphes 1, 2 et 3 de l'article 37 et les cas dans lesquels lesdits transferts sont autorisés en vertu du règlement 2016/679 et de la directive 2016/680, tels qu'ils sont exposés au paragraphe 4, n'est pas claire. Il est difficile de déterminer si un transfert international est interdit en règle générale et si les paragraphes de la disposition sont cumulatifs ou doivent être lus séparément. **Le CEPD recommande de préciser les cas dans lesquels un transfert international est autorisé ou interdit en vertu des différents paragraphes de l'article 37.**

48. Un nouveau paragraphe 3 a été ajouté à l'article 37 en vue d'interdire la communication à un pays tiers d'informations concernant le fait qu'une demande de protection internationale a été introduite dans un État membre, en particulier si ledit pays tiers est également le pays d'origine du demandeur. Tout d'abord, bien que le CEPD comprenne et soutienne l'objectif de la mesure, ce nouveau principe ne paraît rien ajouter à l'interdiction des transferts incluse dans l'article 37, paragraphe 1, de la proposition[34]. Deuxièmement, le CEPD ne comprend pas la signification de la dernière partie de la phrase, qui précise que cette interdiction doit avoir un effet particulier lorsque le pays concerné est également le pays d'origine du demandeur[35]. Si l'interdiction est générale, alors son application ne saurait faire l'objet d'une plus grande attention lorsque les données du demandeur sont susceptibles d'être transférées vers son pays d'origine. **Le CEPD recommande de clarifier la signification de la dernière partie de ce paragraphe, en expliquant, par exemple, s'il doit exister une différence dans le cas où le pays** qui recevra les données est le pays d'origine du demandeur.

49. L'article 38 prévoit la possibilité de transférer des données aux fins du retour. Il s'agit d'une dérogation à l'interdiction générale de transfert des données à un pays tiers ou à une organisation internationale visée à l'article 37. Conformément aux principes de proportionnalité et de minimisation des données, **le CEPD recommande de mentionner à l'article 38, paragraphe 1, que seules les données strictement nécessaires aux fins du retour peuvent être transférées par les États membres.**

c) La possibilité d'infliger des sanctions, dont la rétention

50. L'article 2, paragraphe 3, de la proposition dispose que les États membres peuvent prévoir des sanctions administratives, conformes à leur droit national, pour non-respect de l'obligation de relever les empreintes digitales et de capturer l'image faciale. Cette disposition mentionne également la rétention, qui ne doit être utilisée «*qu'en dernier ressort, pour déterminer ou vérifier l'identité d'un ressortissant de pays tiers*».

51. Le CEPD estime que la formulation de la disposition peut être source de confusion, dans la mesure où elle semble laisser entendre que la rétention peut être considérée comme une

sanction pour le refus de se soumettre au relevé des empreintes digitales. Toutefois, étant donné que la proposition prévoit qu'une telle mesure de rétention serait uniquement autorisée afin de vérifier ou de déterminer l'identité d'une personne, une telle mesure ne doit pas être considérée comme une sanction pour non-respect de l'obligation de se soumettre au relevé des empreintes digitales.

52. En outre, le CEPD ne comprend pas en quoi une sanction ou une peine peut être un élément «*effectif, proportionné et dissuasif*»[36] incitant le migrant à se soumettre au relevé d'empreintes. Le renvoi au document de travail des services de la Commission[37], auquel il est fait référence dans la proposition, ne donne aucune autre indication à cet égard.

53. Dans ce contexte, il convient de rappeler que la directive «retour»[38] ne prévoit pas explicitement qu'une peine de rétention puisse être infligée en cas de refus de se soumettre au relevé des empreintes digitales, contrairement à ce que semble laisser entendre le document de travail des services de la Commission susmentionné.

54. Enfin, le CEPD partage l'opinion du groupe de coordination du contrôle d'Eurodac, qui a affirmé que «*dans la mesure où l'objectif d'Eurodac n'est pas d'ajouter le critère 'empreintes digitales lisibles' à la liste des critères à satisfaire afin de se voir accorder l'asile, mais de repérer et d'empêcher les demandes multiples, le fait que les empreintes digitales d'une personne soient illisibles ne devrait pas être utilisé contre elle*». *En effet, cela relèverait d'un comportement discriminatoire*»[39].

55. En vertu du droit de l'UE en matière de protection des données, le consentement n'est pas la seule base légale pour le traitement des données à caractère personnel: un traitement de données peut être fondé sur une obligation légale[40]. Toutefois, l'utilisation de mesures de coercition afin d'obtenir des empreintes digitales peut se révéler préoccupante pour la dignité humaine. En effet, forcer quelqu'un à donner ses empreintes digitales est une atteinte au droit au respect de la vie privée, étant donné que cela a une incidence directe sur l'intégrité du corps. Pour ces raisons, **le CEPD recommande de supprimer la possibilité d'infliger des sanctions et des peines, dont la rétention, dans le cadre du relevé de données biométriques et d'autoriser la rétention uniquement lorsque celle-ci se limite strictement à ce qui est nécessaire aux fins de l'identification d'une personne.**

56. En outre, le considérant 30 indique que *«les ressortissants de pays tiers considérés comme étant des personnes vulnérables et les mineurs ne devraient pas être contraints de donner leurs empreintes digitales ou leur image faciale, sauf dans des cas dûment justifiés admis par le droit national.»* Cette formulation paraît impliquer que d'autres personnes pourraient y être contraintes. Une telle coercition ne devrait avoir lieu dans aucun cas. Par conséquent, **le CEPD recommande de préciser dans un considérant qu'en aucun cas la coercition ne peut être utilisée afin d'obtenir les empreintes d'une personne**.

d) La gestion opérationnelle

57. L'article 5, paragraphe 2, propose d'accorder à eu-LISA la capacité d'utiliser des données à caractère personnel réelles provenant d'Eurodac à des fins de test. L'utilisation de données à caractère personnel à des fins de test ne dispense pas de respecter le régime de la protection des données dans son intégralité. Éléments notables:

- l'article 5 de la proposition indique qu'eu-LISA est autorisée à utiliser les informations provenant d'Eurodac à des fins de test, «*a) pour établir des diagnostics et effectuer des réparations, lorsque des défauts sont découverts dans le système central; et b) pour tester de nouvelles technologies et techniques permettant d'améliorer les performances du système central ou la transmission de données à ce dernier*». *Le même article prévoit également que «les données à caractère personnel réelles choisies pour les tests sont anonymisées de façon à ce que la personne concernée ne soit plus identifiable».* Cependant, Eurodac est principalement une base de données contenant des informations d'identification, à la fois biométriques et biographiques. Intrinsèquement, les empreintes digitales et les images faciales identifient une personne; elles doivent être considérées comme des données à caractère personnel. Par conséquent, il n'est pas possible d'anonymiser les données, dans la mesure où les empreintes digitales et les images faciales permettront toujours l'identification de l'individu[41]. Pour cette raison, **le CEPD recommande de reconsidérer la formulation de ce paragraphe afin de le rendre cohérent avec le commentaire ci-dessus**, et ce, si la recommandation de suppression de la possibilité d'utiliser des données réelles à des fins de test, mentionnée dans le prochain paragraphe, n'est pas suivie;

- en outre, malgré la justification donnée dans l'exposé des motifs[42], le CEPD ne voit pas pourquoi l'utilisation de données réelles est nécessaire à des fins de test. Par ailleurs, la proposition souligne à juste titre le besoin de sécuriser les données à caractère personnel, quelle qu'en soit l'utilisation: «réelle» ou «à des fins de test». Cela obligera eu-LISA à disposer de deux environnements de «production», similaires du point de vue de la sécurité. Aucune analyse coût/avantage n'a été réalisée afin de confirmer que les avantages prévus liés à l'utilisation de données à caractère personnel réelles à des fins de test compensent l'augmentation des coûts. Étant donné les risques découlant de l'utilisation de données réelles à des fins de test et l'absence de valeur ajoutée dans l'utilisation desdites données, **le CEPD recommande la suppression de l'article 5, paragraphe 2, de la proposition de refonte, autorisant l'utilisation de données réelles à des fins de test;**

- la proposition est suffisamment stricte au sujet des personnes pouvant accéder aux données Eurodac et de la façon dont il est possible d'accéder à ces données. Toutefois, si les données à caractère personnel peuvent être utilisées à des fins de test, il n'existe aucune mesure de protection supplémentaire quant aux personnes pouvant accéder auxdites données ou au moment où celles-ci peuvent être utilisées (p. ex., quels types de mesures de protection doivent-ils être mis en place par eu-LISA lorsqu'elle fait appel à des prestataires externes pour réaliser ces tests?). Si des données de production réelles sont utilisées à des fins de test, les personnes pouvant accéder à ces données ainsi que le moment et les modalités dudit accès doivent être clairement précisés. **Le CEPD recommande par conséquent de préciser que des mesures de protection appropriées concernant l'accès des prestataires externes aux données peuvent être instaurées,** par exemple au moyen d'une référence aux articles 24 et 28 du règlement général sur la protection des données.

e) L'accès

58. L'article 7 de la proposition de refonte du règlement Eurodac confie aux autorités nationales uniques désignées et aux unités de ces autorités la responsabilité de vérifier que les conditions

d'accès aux données Eurodac par les autorités répressives nationales sont satisfaites. Toutefois, les autorités nationales demandant un accès aux données d'Eurodac et les autorités chargées de la vérification accordant cet accès peuvent appartenir à la même autorité. En effet, l'article 7 prévoit que «*[l]'autorité désignée et l'autorité chargée de la vérification peuvent appartenir à la même organisation si le droit national le permet, mais l'autorité chargée de la vérification agit en toute indépendance quand elle exécute ses tâches au titre du présent règlement*» et que «*[l]'autorité chargée de la vérification est distincte des autorités désignées, et ne reçoit d'elles aucune instruction concernant le résultat de ses vérifications*». Dans ces circonstances, l'autorité chargée de la vérification ne peut pas être indépendante de l'autorité désignée dans la mesure où elles font partie de la même organisation. Par conséquent, **le CEPD recommande de modifier cette disposition afin d'imposer que les autorités désignées et les autorités chargées de la vérification ne fassent pas partie de la même organisation.** La même recommandation s'applique à l'unité spécialisée d'Europol qui sera désignée par Europol en tant que point d'accès central, conformément à l'article 27, paragraphe 2. Étant donné les spécificités d'Europol, il convient de définir un mécanisme efficace en vertu duquel l'autorisation préalable d'accès aux données d'Eurodac doit être soumise au contrôle d'un organe suffisamment indépendant de l'autorité désignée[43].

III.2. La proposition sur l'AUEA

59. L'objectif de la **proposition sur l'AUEA** est de renforcer le rôle de l'EASO et d'en faire une agence (Agence de l'Union européenne pour l'asile – AUEA) qui facilite la mise en œuvre et améliore le fonctionnement du RAEC.

a) Les relations entre les experts de l'Agence et les autorités des États membres

60. Conformément à l'article 17 de la proposition sur l'AUEA, l'Agence pourra déployer des équipes d'appui «asile» dans les États membres qui lui demandent une assistance opérationnelle et technique. Ces équipes seront composées d'experts issus du personnel de l'Agence, d'experts des États membres ou d'experts détachés auprès de l'Agence par les États membres. Toutefois la proposition n'explique pas au nom ou sous l'autorité de qui ces experts exécuteront leurs tâches et traiteront les données à caractère personnel, et, par conséquent, qui sera responsable et devra rendre compte des activités de traitement des données. Il est possible de supposer que les autorités des États membres d'accueil concernées seront les responsables du traitement des données à caractère personnel. **Le CEPD recommande d'indiquer dans le texte de la proposition que la responsabilité finale du traitement des données à caractère personnel incombe aux États membres, qui seront considérés comme les «responsables du traitement» conformément au droit de l'UE en matière de protection des données.**

b) L'accès de l'Agence aux bases de données

61. En vertu de l'article 19, paragraphe 3, l'État membre d'accueil dans lequel une équipe d'appui «asile» est déployée aura non seulement l'obligation de donner accès aux bases de données européennes aux experts faisant partie de l'équipe, mais également la possibilité de les autoriser à consulter ses bases de données nationales, afin de réaliser les objectifs et d'exécuter les tâches décrits dans le plan opérationnel. Les bases de

données nationales et européennes que ces experts seront autorisés à consulter doivent être indiquées dans le plan opérationnel [article 19, paragraphe 2, point e)], qui est contraignant pour l'Agence, pour l'État membre d'accueil et pour les États membres participants. **Le CEPD recommande de préciser également que les experts sont uniquement autorisés à consulter les bases de données dans le respect des actes légaux régissant ces bases de données et du droit relatif à la protection des données.**

c) Le traitement des données par l'Agence

62. Le CEPD salue le fait que l'article 31, paragraphe 1, de la proposition dresse une liste exhaustive des finalités pour lesquelles la future Agence traitera des données à caractère personnel, conformément au principe de limitation de la finalité, et exige que ce traitement respecte le principe de proportionnalité et soit strictement limité aux données à caractère personnel nécessaires à ces finalités (article 31, paragraphe 2)[44]. En outre, l'article 30 indique que l'Agence peut traiter les données à caractère personnel «à des fins administratives», sans donner plus d'explications quant à ce terme. **Le CEPD recommande de préciser davantage ce qui est entendu par «fins administratives».** Le CEPD rappelle également qu'en vertu de l'article 5, point b), du règlement nº 45/2001[45], applicable aux institutions et organismes de l'Union européenne, un traitement des données à caractère personnel est possible lorsque celui-ci est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public ou dans l'exercice légitime de l'autorité publique dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées. Par conséquent, l'Agence est autorisée à procéder au traitement des informations nécessaires dans ce contexte sans qu'il soit nécessaire que le règlement prévoie une disposition spécifique.

63. Le CEPD salue également le fait que l'article 31, paragraphe 3, d'une part, limite de façon explicite les transferts de données à caractère personnel des États membres et autres agences de l'UE à l'Agence aux seules finalités visées à l'article 31, paragraphe 1, et, d'autre part, interdit tout autre traitement par l'Agence des données à caractère personnel conservées à des fins autres que celles visées à l'article 31, paragraphe 1. Il s'agit d'une référence claire au principe de limitation de la finalité[46].

64. Le CEPD salue le fait que l'article 32, paragraphe 1, dresse une liste exhaustive des catégories de données à caractère personnel collectées ou transmises à l'Agence lors de la fourniture d'une assistance opérationnelle et technique aux États membres et que l'article 32, paragraphe 2, précise en outre les cas dans lesquels ces données peuvent être traitées.

65. Le CEPD salue également le fait que l'article 32, paragraphe 3, impose à l'Agence la suppression pure et simple des données à caractère personnel «*dès qu'elles ont été transmises à l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres ou utilisées pour l'analyse des informations sur la situation de l'asile*» et définit une durée maximale de conservation des données limitée à trois mois dans tous les cas. À cet égard, le considérant 40 explique en outre qu'«*[u]ne durée de conservation plus longue n'est pas nécessaire pour les fins auxquelles l'Agence traite des données à caractère personnel dans le cadre du présent règlement*». Ce point est conforme aux principes

de la protection des données, selon lesquels les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles ont été collectées.

d) Le système d'information qui sera développé par l'Agence et les moyens techniques qu'elle utilisera

66. Conformément à l'article 29, paragraphe 2, l'Agence proposée développera et exploitera un système d'information permettant d'échanger des informations classifiées ainsi que les données à caractère personnel visées aux articles 31 et 32. **Le CEPD rappelle qu'un tel système doit être conçu conformément au principe de la protection des données dès la conception et que des mesures techniques et organisationnelles adéquates doivent être mises en œuvre afin de maintenir la sécurité du système et d'empêcher le traitement non autorisé des données[47].**

67. L'article 23 de la proposition vise à permettre à l'Agence d'acquérir ou de louer par crédit-bail les équipements techniques (potentiellement des équipements pour le relevé d'empreintes digitales) que l'Agence peut déployer dans des États membres, dans la mesure où les équipes d'appui «asile» en ont besoin, et pour compléter les équipements déjà mis à disposition par les États membres ou d'autres agences de l'Union européenne. Le CEPD est préoccupé par la sécurité des équipements techniques et, par extension, des données à caractère personnel traitées au moyen de ces équipements. Étant donné que les équipements techniques passent de main en main entre l'Agence et les États membres, mais aussi entre les membres des équipes, il est important de garantir un niveau de sécurité adapté aux risques encourus pendant toute la durée des opérations. **Par conséquent, le CEPD recommande d'apporter des précisions quant aux responsabilités en vue de garantir la sécurité des équipements utilisés, responsabilités qui devraient être définies à toutes les étapes du cycle de vie des équipements, à savoir de leur acquisition à leur destruction, en passant par leur stockage et leur utilisation.**

IV. CONCLUSION

68. Le CEPD salue les efforts réalisés sur le plan de la protection des données dans les différents textes. Il constate que la culture de la protection des données commence à être intégrée au processus législatif et peut également être observée dans la rédaction des propositions.

69. Dans le plein respect du rôle du législateur pour ce qui est d'apprécier la nécessité et la proportionnalité des mesures proposées, le CEPD, dans son rôle consultatif, formule dans le présent avis certaines recommandations en matière de protection des données et de respect de la vie privée à l'égard des trois propositions examinées.

70. **Concernant la proposition sur le règlement de Dublin**, le CEPD exprime son inquiétude à l'égard du fait que l'identifiant unique puisse être utilisé à des fins différentes, comme l'identification des personnes dans d'autres bases de données, rendant la comparaison des bases de données facile et simple. Le CEPD recommande de préciser que toute autre utilisation de l'identifiant doit être interdite.

71. **Concernant la proposition de refonte du règlement Eurodac**, le CEPD considère que l'extension du champ d'application d'Eurodac est préoccupante au regard du respect du principe de limitation de la finalité, tel que consacré à l'article 7 de la Charte des droits fondamentaux de l'Union européenne. Le CEPD recommande également de préciser davantage les types de mesures autres que l'éloignement et le rapatriement qui pourraient être prises par les États membres sur la base des données d'Eurodac. Le CEPD recommande que la Commission publie une évaluation complète des répercussions en matière de protection des données et de respect de la vie privée dans la refonte du règlement Eurodac de 2016, afin de mesurer l'incidence du texte proposé sur le respect de la vie privée.

72. Le CEPD est également préoccupé par l'ajout des images faciales: le règlement ne fait référence à aucune évaluation de la nécessité de collecter et d'utiliser les images faciales des catégories de personnes visées dans la proposition de refonte du règlement Eurodac. En outre, le CEPD estime que la proposition doit préciser les cas dans lesquels une comparaison des empreintes digitales et/ou des images faciales est effectuée, dans la mesure où la formulation de la proposition de refonte semble laisser entendre qu'une telle comparaison doit avoir lieu systématiquement.

73. Le CEPD recommande aussi qu'une évaluation détaillée soit publiée, en complément de l'exposé des motifs, concernant la situation des mineurs, l'équilibre entre les risques et les préjudices inhérents à une telle procédure pour les mineurs et les avantages dont ceux-ci peuvent bénéficier. Dans ce contexte, la signification du relevé des empreintes des mineurs d'une façon adaptée aux enfants doit être mieux définie dans le règlement (c'est-à-dire, dans un considérant).

74. Concernant la durée de conservation, qui sera en principe de cinq ans, le CEPD recommande de donner plus de détails et d'explications quant aux raisons et à la façon dont une durée de conservation des données de cinq ans a été considérée nécessaire dans ce contexte afin d'atteindre les nouveaux objectifs de la base de données Eurodac. En outre, le CEPD recommande de réduire la durée de conservation à la durée réelle de l'interdiction d'entrée imposée à la personne concernée. Enfin, le CEPD recommande de préciser dans la proposition que le début de la durée de conservation est la date du traitement du premier relevé d'empreintes digitales réalisé par un État membre.

75. Pour terminer, le CEPD recommande de verrouiller l'ensemble des données à des fins répressives après trois ans et d'arrêter de distinguer les différentes catégories de ressortissants de pays tiers à cet égard.

76. **Au-delà des principales lacunes de la proposition recensées ci-dessus, les recommandations exprimées par le CEPD dans le présent avis concernent les aspects suivants:**

- **concernant la proposition de refonte du règlement Eurodac,**

  - le CEPD recommande d'indiquer dans le texte de la proposition que la responsabilité finale du traitement des données à caractère personnel incombe aux États membres, qui seront considérés comme les responsables du traitement, au sens de la directive 95/46/CE;

- l'article 37 doit être réécrit afin de préciser dans quels cas un transfert international est autorisé ou interdit, particulièrement en ce qui concerne le transfert vers le pays d'origine du demandeur;

- l'article 38, paragraphe 1, doit préciser que seules les données strictement nécessaires aux fins du retour peuvent être transférées par les États membres;

- la coercition doit être interdite pour obtenir les empreintes digitales des personnes. Ceci doit être précisé dans le règlement Eurodac;

- dans ce contexte, le CEPD recommande de préciser que la rétention ne saurait être considérée comme une sanction pour le non-respect de l'obligation de fournir des empreintes digitales;

- l'utilisation de données réelles par eu-LISA à des fins de test est particulièrement préoccupante et ne doit pas être autorisée par le règlement Eurodac. L'autre solution, consistant à utiliser des données fictives, doit être examinée et évaluée par le législateur, en tenant compte du risque pour la vie privée des personnes concernées. En tout état de cause, le texte ne doit pas considérer que les données biométriques peuvent être anonymisées, étant donné qu'elles se rapportent toujours à une personne et sont donc considérées comme des données à caractère personnel;

- concernant le traitement des informations par eu-LISA, le CEPD recommande de préciser que des mesures de protection adéquates à l'égard de l'accès aux données par des prestataires externes doivent être mises en place;

- enfin le CEPD salue les efforts visant à s'assurer que l'accès par les autorités répressives est évalué par un organe indépendant. Toutefois, les autorités désignées et les autorités chargées de la vérification ne doivent pas faire partie de la même organisation, afin de préserver l'indépendance de l'autorité chargée de la vérification;

- **concernant la proposition sur l'AUEA,**

- le CEPD recommande de préciser que les experts de l'Agence sont uniquement autorisés à consulter les bases de données dans le respect des actes légaux régissant ces bases de données et des règles en matière de protection des données;

- le CEPD recommande de préciser davantage ce qui est entendu par «fins administratives» à l'article 30, paragraphe 3, étant donné que tout objectif poursuivi par une administration pourrait correspondre à ce terme;

- le CEPD recommande d'apporter des précisions quant aux responsabilités pour ce qui est de garantir la sécurité des équipements utilisés par l'Agence, responsabilités qui devraient être définies à toutes les étapes du cycle de vie des équipements, à savoir de leur acquisition à leur destruction, en passant par leur stockage et leur utilisation.

Bruxelles, le 21 septembre 2016

(**signature**)

Giovanni BUTTARELLI
Contrôleur européen de la protection des données

REMARQUES

[1] COM (2016) 197 final.
[2] COM (2016) 270 final.
[3] COM (2016) 271 final.
[4] COM (2016) 272 final.
[5] Voir articles 22, 23, 44 et 45 de la proposition.
[6] Voir article 23, paragraphe 2, de la proposition sur le règlement de Dublin.
[7] COM (2016) 205 final.
[8] Elle pourrait par exemple figurer dans un considérant.
[9] Avis du CEPD du 18 février 2009 sur la proposition de règlement concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (CE) nº [.../...][établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride] [COM(2008)825] du 18 février 2009.
Avis du CEPD du 7 octobre 2009 sur la proposition modifiée de règlement du Parlement européen et du Conseil relatif à la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (CE) nº (…/…) (établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride), et sur la proposition de décision du Conseil pour les demandes de comparaison avec les données d'Eurodac présentées par les services répressifs des États membres et Europol à des fins répressives.
Avis du CEPD du 30 septembre 2010 sur la communication «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice».
Avis du CEPD du 12 septembre 2012 sur la proposition modifiée de règlement du Parlement européen et du Conseil relatif à la création du système «EURODAC» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) nº […/…] [.....] (refonte).
[10] Avis du CEPD du 7 juillet 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions sur la migration, paragraphe 17.
[11] Page 8 de la proposition.
[12] Page 9 de la proposition.
[13] Dans ce contexte, voir article 35 du règlement général sur la protection des données [règlement (UE) nº 2016/679]; voir également l'avis du CEPD du 7 juillet 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la migration, paragraphe 15.
[14] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Un agenda européen en matière de migration, COM(2015) 240 final.
[15] Exposé des motifs, pages 5 et 13.
[16] Il est même permis de douter de la possibilité de mettre en place une telle politique, dans la mesure où plusieurs documents rédigés par la Commission semblent indiquer que les empreintes digitales endommagées restent un cas assez isolé (voir http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/border/588_emn_ahq_eurodac_fingerprinting_en.pdf, et notamment la réponse de la Belgique; voir également le résumé de la requête ad hoc nº 588 du REM, *Eurodac Fingerprints* (Les empreintes digitales dans Eurodac), disponible à l'adresse http://statewatch.org/news/2015/mar/eu-com-compulsory-fingerprinting-asylum-applicants-ms-responses-summary.pdf, ainsi que le rapport sur l'inspection coordonnée relative aux empreintes digitales illisibles, de mai 2013, du groupe de coordination du contrôle d'Eurodac, disponible à l'adresse https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med_20130705_report_escg_unreadable_fingerprints.pdf).
[17] Fingerprint Recognition for Children, rapport technique du Centre commun de recherche, 2013, disponible à l'adresse http://publications.jrc.ec.europa.eu/repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20%28pdf%29.pdf.
[18] Page 10 de l'exposé des motifs.

[19] Directive 2008/115/CE du Parlement européen et du Conseil du 16 décembre 2008 relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier.
[20] Règlement (CE) nº 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS).
[21] Proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour enregistrer les données relatives aux entrées et aux sorties des ressortissants de pays tiers qui franchissent les frontières extérieures des États membres de l'Union européenne ainsi que les données relatives aux refus d'entrée les concernant, portant détermination des conditions d'accès à l'EES à des fins répressives et portant modification du règlement (CE) nº 767/2008 et du règlement (UE) nº 1077/2011, COM/2016/0194 final.
[22] Article 6, paragraphe 1, point e), de 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.
[23] Article 17 de la proposition de refonte du règlement Eurodac.
[24] Article 13 de la proposition de refonte du règlement Eurodac.
[25] Voir article 14 de la proposition de refonte du règlement Eurodac.
[26] Voir article 19 du règlement.
[27] Partie sur l'explication détaillée des différentes dispositions de la proposition.
[28] Voir article 18 de la proposition de refonte.
[29] Les catégories concernées par l'article 13, paragraphe 2, et l'article 14, paragraphe 3, de la proposition de refonte.
[30] Voir l'article 19, paragraphe 2, deuxième alinéa, et la référence aux fins de l'article 1er, paragraphe 1, point c).
[31] Voir l'article 19, paragraphe 4, et la référence aux fins de l'article 1er, paragraphe 1, point b).
[32] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
[33] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[34] À l'exception du fait que le premier paragraphe fait référence à des données obtenues par un État membre ou Europol, et non aux informations que ceux-ci ont créées. Toutefois, il semble que ce paragraphe ne doive pas être lu de façon restrictive et doive bénéficier d'une interprétation large, ainsi que d'une portée étendue, incluant l'ensemble des données traitées conformément au règlement Eurodac, quelle que soit leur provenance.
[35] Il en va de même pour l'article 38, paragraphe 2.
[36] Tel que mentionné à l'article 3, paragraphe 3, de la proposition sur Eurodac.
[37] Document de travail des services de la Commission relatif à la mise en œuvre du règlement Eurodac en ce qui concerne l'obligation de relever les empreintes digitales, SWD (2015) 150 final, auquel il est fait référence dans l'exposé des motifs.
[38] Directive 2013/33/UE du Parlement européen et du Conseil du 26 juin 2013 établissant des normes pour l'accueil des personnes demandant une protection internationale (refonte).
[39] *Report on the coordinated inspection on unreadable fingerprints* (Rapport sur l'inspection coordonnée relative aux empreintes digitales illisibles) de mai 2013, du groupe de coordination du contrôle d'Eurodac, disponible à l'adresse: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/13-06-10_Report_unreadable_fingerprints_EN.pdf. Il était également indiqué dans le rapport du groupe de coordination du contrôle d'Eurodac que «les procédures doivent préciser que les empreintes digitales illisibles ne sauraient être utilisées en tant que telles contre les demandeurs, et que toute conséquence néfaste pour les demandeurs doit être justifiée par des preuves suffisantes.
[40] Voir article 7, point c), de la directive 95/46/CE.
[41] Voir l'avis du CEPD du 25 novembre 2015 sur une notification de contrôle préalable reçue du délégué à la protection des données de l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) concernant l'«étude relative aux tests d'imagerie multispectrale/de balayage optique dans le cadre d'Eurodac», disponible à l'adresse: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2015/15-11-25_Eurodac_MSI_Optical_Scan_Test_Study_euLISA_FR.pdf.
[42] Voir page 16 de l'exposé des motifs: «Lors des tests du système central Eurodac, eu-LISA a dû se contenter d'utiliser des 'données fictives' pour l'environnement de test, ainsi que pour expérimenter de nouvelles

technologies, de sorte que les résultats obtenus n'ont pas été de bonne qualité, en raison des données utilisées. La proposition prévoit l'utilisation de données à caractère personnel réelles dans les tests du système central à des fins de diagnostic et de correction, ainsi que l'utilisation de nouvelles technologies et techniques, moyennant le respect de conditions strictes et du principe de l'anonymisation des données aux fins des tests, empêchant leur utilisation en vue d'une identification individuelle».

[43] Pour le même raisonnement, voir le paragraphe 86 de l'avis 6/2016 du CEPD sur le deuxième train de mesures de l'UE relatif aux «Frontières intelligentes».

[44] En vertu de l'article 4, paragraphe 1, point b), du règlement (CE) nº 45/2001 et de l'article 6, paragraphe 1), point b), de la directive 95/46/CE, les données à caractère personnel doivent être «*collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités*».

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

[46] Voir, ci-dessus, paragraphe 16.

[47] Voir article 25 du règlement général sur la protection des données (règlement 2016/679) et l'article 22 du règlement nº 45/2001.