**Avis du contrôleur européen de la protection des données sur un projet de recherche financé par l'Union européenne en vertu du septième programme-cadre (7PC) de recherche et de développement technologique - Turbine (TrUsted Revocable Biometric IdeNtitiEs)**

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 le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 41,

donnant effet à son document stratégique intitulé «le CEPD et la recherche et le développement technologique dans l'UE» qui se rapporte au septième programme-cadre en cours ainsi qu'aux futurs programmes-cadres de recherche et de développement technologique;

A ADOPTÉ L'AVIS SUIVANT:

## 1. Introduction

### 1.1 Généralités

1. Pour la première fois, le CEPD adopte un avis donnant effet à son document stratégique intitulé «Le CEPD et la recherche et le développement technologique dans l'UE» qui décrit le rôle que pourrait jouer l'institution en ce qui concerne les projets de recherche et de développement technologique (RDT) relevant du septième programme-cadre de recherche et développement (7PC) lancé par la Commission fin 2006[1].

2. En 2008, après avoir analysé les différents éléments du projet Européen «Turbine» (*TrUsted Revocable Biometric IdeNtitiEs*), dont l'objectif est de mener des

[1] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_FR.pdf

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

recherches concernant les données biométriques révocables, le CEPD a décidé de répondre favorablement à la demande du groupement d'entreprises et de rendre un avis sur ce projet UE[2]. Le CEPD a estimé que le consortium du projet Turbine répondait aux conditions d'acceptation d'une demande d'avis énoncées par son document stratégique. Le CEPD s'est réjoui du grand intérêt que présente le projet pour les «questions relatives à la protection des données» et a estimé qu'il répondrait aux priorités mentionnées dans son rapport annuel.

1.2. L'instrument d'un avis sur la recherche et le développement technologique dans l'UE

3. Ce document stratégique présente les critères de sélection des projets qui peuvent faire l'objet d'une action du CEPD et décrit la manière dont le CEPD peut contribuer à ces projets. L'une des contributions du CEPD aux projets RDT de l'UE consiste à rendre un avis sur des projets spécifiques de RDT.

4. D'après le document stratégique du CEPD, «le consortium réuni autour d'un projet [*peut*] lui demande[*r*] de rendre un avis. Bien que le CEPD ne contribue pas à une proposition de projet, celle-ci peut prévoir de lui demander un avis au cours du cycle de vie du projet, (à condition que ce dernier soit accepté). Dans ce cas, avant qu'un dossier ne soit soumis en réponse à l'appel à propositions, le CEPD doit en être informé et doit donner son accord pour qu'il soit fait mention de l'avis qu'il sera appelé à rendre par la suite. Le consortium devra préciser, dans les documents présentés en rapport avec sa proposition, que l'avis du CEPD sera rendu en sa qualité d'autorité indépendante.» Le document souligne clairement l'indépendance du CEPD dans la réalisation de ces travaux, ainsi que dans les communications avec les parties prenantes du projet qui le contactent.

1.3 Objectif et portée de l'avis

5. À travers ces différentes contributions, le CEPD se donne pour objectif global de promouvoir et de renforcer l'application du principe «*privacy by design*» (prise en compte du respect de la vie privée lors de la conception) aux projets européens de RDT et de faciliter dès lors la mise en œuvre du cadre réglementaire de l'UE en matière de protection des données. L'avis n'aborde pas uniquement les améliorations techniques envisagées par le projet de recherche en tant que tel, mais aussi la méthodologie de recherche et les procédures appliquées par le projet.

6. L'avis du CEPD n'a pas pour objectif de compléter le rôle des réviseurs du projet, ni des autorités nationales compétentes en matière de protection des données, mais de fournir un avis d'expert sur les aspects relatifs à la protection des données d'un projet particulier. Par conséquent, le CEPD n'analyse pas tous les résultats, mais il a demandé l'accès aux documents du projet qu'il a considérés comme les plus pertinents sur le plan de la protection des données.

7. Le consortium du projet a fourni au CEPD tous les documents pertinents sur les aspects relatifs à la protection des données de la recherche menée dans le contexte du projet Turbine. Le CEPD a également tenu plusieurs discussions avec quelques représentants du consortium afin d'obtenir des éclaircissements et, au besoin, d'autres documents. Enfin, le CEPD a reçu des commentaires du consortium sur un projet de cet avis.

[2] Voir Contrôleur européen de la protection des données, rapport annuel 2008, p. 71.

1.4 Turbine

8. Turbine (TrUsted Revocable Biometric IdeNtitiEs) est un projet de recherche financé par l'Union européenne en vertu du septième programme-cadre (7PC) de recherche et de développement technologique (http://www.turbine-project.eu.). D'après les partenaires de Turbine, les objectifs généraux du projet consistent à:

   - développer une solution technologique renforçant le respect de la vie privée lors de l'authentification électronique de l'identité (eID) par la biométrie des empreintes digitales et

   - démontrer l'efficacité et la sécurité de cette solution pour des applications commerciales de gestion de la carte d'identité électronique (eID) ainsi que ses avantages pour le citoyen dans l'optique du renforcement de la protection de la vie privée et de la confiance de l'utilisateur en la gestion de la carte d'identité électronique par l'utilisation des empreintes digitales.

9. Le projet vise à élaborer une méthode biométrique respectueuse de la vie privée reposant sur les empreintes digitales. L'enjeu principal de Turbine est l'élaboration d'un protocole dit de pseudo-identité (protocole PI) qui a recours à des modèles (biométriques) protégés. Plus particulièrement, dans le protocole de pseudo-identité, les données biométriques sont transformées ce qui permet de diversifier et de dissocier les identités biométriques. Plus spécifiquement, la méthode repose sur le remplacement de l'analyse biométrique de l'empreinte digitale par un dérivé crypté de l'empreinte digitale, appelé «identité biométrique», qui utilise des fonctions spéciales de hachage reposant sur des algorithmes cryptographiques. L'utilisation de différents algorithmes cryptographiques rend possible la production d'un nombre respectif d'identités biométriques pour la même empreinte digitale.

10. Chaque identité biométrique est liée exclusivement à la personne dont l'empreinte digitale a été prise, à la suite de l'application d'un algorithme spécifique. En utilisant la méthode décrite ci-dessus durant le fonctionnement d'un système de biométrie (par ex. pour contrôler l'accès de personnes à des installations), l'identification des personnes se fait par l'intermédiaire de leurs identités biométriques, de façon à ce qu'il ne soit pas nécessaire de conserver leurs empreintes digitales biométriques brutes. Le protocole PI permet également de stocker des données biométriques localement, par exemple sur un jeton, mais d'autres architectures restent possibles.

11. Parmi les caractéristiques importantes du projet, la technologie Turbine vise à protéger le modèle biométrique par transformation cryptographique des informations de l'empreinte digitale en une **clé non inversible** qui permet l'appariement par comparaison bit à bit. Les données biométriques transformées sont considérées comme non inversibles et ne peuvent donc pas être retransformées en échantillons biométriques et modèles originaux. En outre, afin de renforcer la confiance de l'utilisateur, cette clé sera également **révocable**, c'est-à-dire qu'une nouvelle clé indépendante peut être produite afin de délivrer de nouvelles identités biométriques.

12. Le CEPD considère ces deux éléments (le caractère non inversible [irréversibilité] prévu de la clé et la révocabilité de la clé) de cette technologie comme les deux piliers du projet Turbine. Ces aspects présentent le plus grand intérêt pour le CEPD dans l'optique de la protection des données et seront examinés de plus près ci-

dessous, après une analyse des données biométriques qui sont traitées dans le contexte du projet Turbine.

## 2. Analyse juridique

### 2.1 Données biométriques

13. Le CEPD a souligné à plusieurs reprises que l'introduction et le traitement des données biométriques doivent aller de pair avec des garanties particulièrement solides et cohérentes. Par leur nature spécifique, les données biométriques présentent des risques particuliers lors de leur utilisation, qu'il convient de réduire. Ces caractéristiques spécifiques liées aux données biométriques expliquent également l'intérêt que porte le CEPD au projet Turbine et aux objectifs qu'il souhaite réaliser.

14. Le CEPD note que les partenaires du projet ont pris très au sérieux les aspects juridiques liés à l'utilisation de la biométrie.

15. En effet, les préoccupations et exigences juridiques liées au traitement des données biométriques ont été prises en considération dès le début du projet. Ces préoccupations juridiques sont formulées dans différents documents, en particulier dans le document de travail sur la biométrie du groupe de travail «Article 29» sur la protection des données[3], ainsi que dans des avis, dont ceux du CEPD, relatifs à l'utilisation à grande échelle de la biométrie dans l'UE.[4]

16. Le CEPD a reçu un document détaillé reprenant des exigences juridiques, inextricablement liées à des exigences fonctionnelles et techniques, qui a été préparé au cours des premiers mois du projet et soumis au comité consultatif du projet pour contribution et discussion[5]. Pour le CEPD, cela démontre l'engagement des partenaires à appliquer précocement le concept de «*privacy by design*» dans le cycle de vie du projet.

#### 2.1.1 Traitement des données biométriques

17. Les données biométriques constituent les données principales traitées dans le projet Turbine. Il est par conséquent essentiel de déterminer leur statut.

18. D'après le groupe de travail «Article 29»[6], les données biométriques peuvent se définir comme «des propriétés biologiques, des caractéristiques physiologiques, des caractéristiques vivantes ou des actions reproductibles lorsque ces caractéristiques et/ou actions sont à la fois propres à cette personne physique et mesurables, même si les méthodes utilisées dans la pratique pour les mesurer techniquement impliquent un certain degré de probabilité. Parmi les exemples caractéristiques de ces données biométriques figurent les empreintes digitales, la structure de la rétine, la structure faciale, la voix, mais aussi la forme des mains, le système veineux, voire des

---

[3] Groupe de travail «Article 29» sur la protection des données, *Document de travail sur la biométrie*, WP 80, 1er août 2003.

[4] Tel que l'avis du CEPD du 19 octobre 2005 sur trois propositions concernant le système d'information de Schengen de deuxième génération (SIS II) et l'avis du CEPD du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour .

[5] Voir Turbine, résultat D.1.1.1.

[6] Avis 4/2007 sur le concept de données à caractère personnel, WP 136, p. 9.

caractéristiques profondément ancrées ou d'autres caractéristiques comportementales (signature manuscrite, dynamique de frappe sur un clavier, démarche ou élocution particulières, etc.).»

19. Comme l'indique le groupe de travail Article 29: «Ce qui caractérise, entre autres, les données biométriques, c'est qu'elles peuvent être considérées comme *contenu des informations* concernant une personne physique donnée (X a ces empreintes digitales) ainsi que comme élément permettant d'établir un lien entre une information et une personne physique (cet objet a été touché par quelqu'un qui présente ces empreintes digitales et celles-ci correspondent à X; par conséquent, X a touché l'objet). Elles peuvent ainsi servir d'«identificateurs». En effet, en raison du lien unique qui les relie à une personne physique spécifique, les données biométriques peuvent être utilisées pour *identifier* la personne physique.»

20. Dans le cas du projet Turbine, le système de biométrie proposé utilise une méthode qui «pseudonymise» les données biométriques (empreintes digitales) en les remplaçant par des dérivés cryptés et irréversibles (identités biométriques) résultant de l'utilisation de techniques de cryptage à sens unique avec l'application de fonctions de hachage. En raison des moyens techniques utilisés pour produire ces identités biométriques, la récupération des données biométriques brutes à partir de celles-ci est jugée impossible, et une identité biométrique ne peut donc être considérée comme un contenu d'informations caractérisant une personne dans le sens mentionné ci-dessus. Par conséquent, l'utilisation d'une identité biométrique, au lieu de l'empreinte digitale biométrique brute, renforce la protection de cette dernière puisqu'il est jugé impossible, sur le plan technique, de récupérer les informations de l'empreinte digitale directement de l'identité biométrique comme l'a suggéré Turbine. Cependant, comme le lien exclusif entre l'identité biométrique et une personne spécifique existe toujours (puisque seule la prise de l'empreinte digitale de la même personne permettrait à chaque fois de produire la même identité biométrique en utilisant le même algorithme cryptographique), l'identité biométrique permet d'identifier cette personne de la même façon que l'élément biométrique brut. Autrement dit, malgré le fait que l'identité biométrique ne puisse pas, de façon indépendante, entraîner la divulgation des informations liées à une personne, elle pourrait toutefois entraîner l'identification de cette personne dans le cadre du fonctionnement du système biométrique (par exemple durant un contrôle d'accès) en combinaison avec d'autres données personnelles conservées dans le système pour la même personne (par exemple son nom entier). Dans ce sens, l'identité biométrique, telle qu'elle est produite et utilisée par le projet Turbine, constitue aussi des données personnelles[7].

21. Comme mentionné à plusieurs reprises dans des avis relatifs aux données biométriques, le CEPD considère que le traitement de certaines données biométriques autres que le simple stockage de photographies seules présente des risques particuliers au regard des droits et libertés des personnes concernées, c'est ce qui implique que de tels traitements soient soumis à un contrôle préalable (sur la base de l'article 27, paragraphe 1, du règlement n° 45/2001. Ce point de vue repose principalement sur le processus de comparaison qui présente des risques particuliers et sur la nature des données biométriques en raison de certaines caractéristiques inhérentes à ce type de données. Par exemple, les données biométriques transforment irrévocablement le rapport entre le corps et l'identité, car il rend les

[7] Voir le raisonnement dans la décision n° 31/2010 de l'autorité hellénique de protection des données.

caractéristiques du corps humain «lisibles par une machine» et les soumet à des utilisations supplémentaires. Outre la nature très particulière des données, d'autres risques tels que les possibilités d'établir des interconnexions et l'état d'avancement des outils technologiques peuvent avoir des conséquences inattendues ou non souhaitables pour les personnes concernées. Le traitement des données biométriques nécessitera donc des mesures spécifiques qui sont analysées ci-dessous.

### 2.1.2 Caractéristiques de Turbine

22. Dans la vie de tous les jours, l'identité et les données personnelles d'un individu peuvent être compromises. Il est par conséquent important de les protéger. Le même principe s'applique aux données biométriques. Cependant, comme les individus disposent d'un nombre limité d'iris et de doigts, l'usurpation d'identité par l'utilisation de ces données compromet les références biométriques correspondantes et les rend inutilisables. En effet, les données biométriques sont étroitement liées aux individus et en raison de leur intangibilité, elles seraient très vulnérables si elles étaient compromises. Il est donc important de veiller à la qualité des données traitées et à leur sécurité.

23. Le projet Turbine favorise deux caractéristiques particulières des données biométriques traitées et transformées en une clé biométrique.

*Irréversibilité de la clé*

24. Dans le projet Turbine, l'empreinte digitale portant l'identité et l'accès aux informations personnelles d'un individu est transformée en une clé constituée d'une chaîne binaire qui est considérée comme non inversible[8], c'est-à-dire que la chaîne est conçue comme si elle était déconnectée de l'empreinte digitale originale. Ce système doit permettre à un individu d'avoir plusieurs identités ou pseudo-identités auxquelles différentes informations personnelles peuvent être associées: financières, juridiques, de santé, etc. Par conséquent, l'utilisation d'une clé non inversible pour produire des modèles renouvelables semble rendre impossible l'acquisition (à partir de cette clé) des données biométriques de référence originales.

25. L'impossibilité de la réversibilité devrait améliorer la protection des données biométriques de référence qui ne seront plus compromises en raison de leur lien inhérent à l'individu. Cette caractéristique, l'irréversibilité, est la bienvenue du point de vue de la protection et de la sécurité des données, en ce qui concerne les principes de protection des données énoncés dans le règlement n° 45/2001. À titre d'exemple, l'article 4, paragraphe 1, point b), dudit règlement prévoit que 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. En rendant les représentations biométriques irréversibles, le système doit empêcher l'utilisation de données biométriques à d'autres fins que celles initialement prévues. Il veille aussi à ce que les données biométriques elles-mêmes ne soient pas conservées plus longtemps que nécessaire, puisqu'elles sont remplacées par la clé constituée d'une chaîne binaire.

[8] Dans le projet, l'irréversibilité fait référence à la difficulté de dériver davantage d'informations des renseignements protégés que le résultat d'un contrôle (par autres informations, on entend par exemple les données biométriques originales ou des informations médicales).

26. L’article 4, paragraphe 1, point c), prévoit que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou traitées ultérieurement. Étant donné que la chaîne binaire de données remplace les données biométriques de référence, seules les données à caractère personnel nécessaires sont traitées. Ce système permet d’éviter un traitement ultérieur de données supplémentaires qui sont contenues dans la référence biométrique.

27. Du point de vue de la sécurité (tel que développé dans les articles 21 et 22 du règlement n° 45/2001), l’irréversibilité de la clé implique une plus grande sécurité des données biométriques originales puisqu’elles ne seront pas liées à la clé. Cet aspect de la sécurité est aussi renforcé par la caractéristique de révocabilité de la clé.

*Révocabilité de la clé*

28. Le projet Turbine a décrit une procédure permettant de révoquer les pseudo-identités. Grâce à cette solution, la personne concernée disposera d’autres moyens d’authentification pour les services lorsqu’il faudra révoquer les pseudo-identités.

29. La position adoptée par le projet Turbine est que le risque de références biométriques compromises peut être atténué pour certains types d’attaques en prévoyant des méthodes qui permettent de renouveler les modèles. Si plusieurs modèles différents peuvent être récupérés des mêmes données biométriques de référence, le modèle peut être renouvelé s’il est lui-même exposé à une usurpation d’identité. Le modèle compromis peut donc être révoqué.

30. Une caractéristique biométrique ne peut pas être modifiée. En effet, comme les individus ont un certain nombre de doigts et d'yeux, ces données biométriques ne sont pas «renouvelables». Par conséquent, le risque est que des données biométriques compromises le restent à jamais. Sur la base de ces risques, un modèle révocable de ces données biométriques présente plusieurs avantages.

31. En utilisant une clé révocable, la représentation biométrique d’une empreinte digitale à partir de laquelle les données biométriques originales ne peuvent pas être récupérées (irréversibilité) peut être supprimée et reproduite.

32. En révoquant un modèle compromis, le système empêche toute utilisation ultérieure du modèle qui serait incompatible avec la finalité originale (article 4, paragraphe 1, point b), du règlement n° 45/2001), car le système ne reconnaîtrait plus ce modèle comme valide.

33. De plus, la révocabilité du modèle garantit que l’exactitude des données est préservée (article 4, paragraphe 1, point d), du règlement n° 45/2001). Si les données ne sont plus exactes (compromises, etc.), la possibilité de révoquer et de renouveler le modèle sur la base des données biométriques permet de garder les données à jour.

### 2.1.3 Meilleures pratiques relatives à la recherche sur les données biométriques

34. D’après les informations reçues du consortium à l'origine de Turbine, les aspects juridiques de la gestion de l’identité et ceux de l’utilisation des données

biométriques ont fait l'objet d'une analyse et un ensemble de dix «meilleures pratiques» relatives à l'utilisation des données biométriques par les systèmes de gestion des identités ont été recherchées et développées[9]. Le résultat de ces propositions de «meilleures pratiques» a également été envoyé au CEPD. Il repose sur des avis des autorités de la protection des données, du CEPD et du groupe de travail «Article 29» sur la protection des données, d'une part, et sur les nouvelles techniques recherchées, testées et appliquées dans Turbine d'autre part. Les lignes directrices proposées ont également été soumises au comité consultatif du consortium avec lequel elles ont été débattues. Le CEPD estime que ces documents démontrent l'engagement du consortium de ce projet de fonder ses recherches sur une assise juridique solide.

Le projet Turbine a relevé les meilleures pratiques suivantes:

- les données biométriques sont en principe utilisées uniquement à des fins de contrôle;
- contrôle de l'utilisateur sur les données biométriques par défaut;
- identités multiples et pseudonymité;
- révocabilité des identités biométriques et reproduction;
- vérification des références et/ou de l'identité;
- suppression des échantillons et des modèles originaux;
- utilisation des technologies renforçant la protection de la vie privée;
- transparence et informations supplémentaires pour les personnes concernées;
- définition de solutions de secours et de la procédure permettant de faire appel de la décision de comparaison;
- l'organisation (en particulier de la phase d'inscription), la sécurité et la certification du système de gestion des identités biométriques.

35. En octobre, le CEPD a proposé de dresser une liste d'exigences de base communes, prenant en considération les caractéristiques spécifiques des données biométriques. Il doit être possible d'appliquer la liste à tous les types de système utilisant la biométrie. Les exigences communes sont les suivantes:

- Évaluation d'impact ciblée: cette exigence devient plus pertinente compte tenu de l'évolution récente en matière de politiques d'évaluation d'impact sur la confidentialité, brièvement décrite par le groupe de travail «Article 29» et le CEPD.

- Importance accordée au processus d'inscription: l'inscription constitue une étape critique du processus global de l'identification biométrique. Il convient de prendre toutes les mesures nécessaires pour garantir que la phase d'inscription permet à la majorité des individus de s'inscrire. En outre, l'inscription doit aussi prendre en considération le niveau des taux de faux rejets et de fausses acceptations. De plus, les solutions de secours prévues pour remédier aux impossibilités d'inscription doivent être facilement disponibles.

- Solutions de secours: des solutions de secours facilement disponibles doivent être mises en place afin de respecter la dignité des personnes qui peuvent avoir été mal identifiées et de leur éviter de porter le poids des imperfections du système.

[9] Voir Turbine, résultat 1.4.3. («Les meilleures pratiques de Turbine»).

- Mise en évidence du niveau d'exactitude: lié aux solutions de secours, le niveau d'exactitude du système, et en particulier ses taux de faux rejets et de fausses acceptations, doivent faire l'objet d'une définition en fonction de la précision du système et doivent être contrôlés en permanence par rapport à la population utilisant le système. L'investissement nécessaire dans les solutions de secours sera défini sur base du niveau de ces taux.

36. Le CEPD reconnaît qu'approfondir les meilleures pratiques énumérées ci-dessus favorisera la mise en œuvre de mesures appropriées pour tout système de gestion des identités biométriques géré en conformité avec le cadre réglementaire de l'Union européenne. Une telle liste de points à vérifier permettrait en effet de développer des systèmes plus respectueux des données à caractère personnel, si elle est prise en considération dès le début des projets. À la suite de discussions avec les partenaires réunis autour du projet, le CEPD comprend que le projet, bien que ne mentionnant pas stricto sensu le niveau d'exactitude dans sa liste de meilleures pratiques, a pris cet aspect en considération dans les recherches, en établissant des objectifs précis d'exactitude au début de ce projet. En outre, au cours des recherches, ce niveau d'exactitude a été mesuré, vérifié et même amélioré de sorte que ces niveaux précis d'exactitude seront adoptés pour l'utilisation d'un système biométrique dans un environnement opérationnel.

37. Cependant, le CEPD note que la liste des meilleures pratiques élaborée par le projet Turbine ne semble pas insister expressément sur la fixation d'un niveau précis d'exactitude exigé d'un système biométrique. Le CEPD accorde beaucoup d'importance à cette question. Par conséquent, il convient d'établir un taux précis d'exactitude dès le début et de le réexaminer régulièrement. L'appliquer n'est donc pas suffisant, il convient de l'intégrer entièrement dans la liste des meilleures pratiques.

#### 2.1.4 L'utilisation de bases de données biométriques exclusives et accessibles au public

38. En vue de contrôler et d'évaluer les algorithmes mis au point par le projet, les partenaires de Turbine ont réalisé des contrôles d'efficacité. Pour ces contrôles et évaluations, les partenaires de Turbine ont décidé au début du projet (dans la description des travaux) d'effectuer les contrôles sur des bases de données exclusives et des bases de données contenant des empreintes digitales biométriques accessibles au public.

*Bases de données exclusives*

39. En ce qui concerne les bases de données exclusives, le CEPD comprend que certains des partenaires du projet ont utilisé leurs propres bases de données exclusives[10] ainsi qu'une base de données exclusives norvégienne.

[10] Il est encore précisé qu'il s'agit de bases de données concernant des recherches générales appartenant aux entreprises respectives et conservées respectivement en France et en Suède. En Suède, le représentant des données de l'entreprise, dont le nom est communiqué aux autorités suédoises de protection des données, garantit et surveille le traitement correct et légal des données biométriques. En France, des discussions ont été menées avec la CNIL à propos des conditions d'utilisation des bases de données biométriques à des fins de recherche afin d'obtenir l'autorisation pour toutes ces bases de données exclusives en conformité avec la législation française. Le CNIL a adopté une décision en juillet 2010 ('Délibération 2010-336').

40. Le consortium du projet a démontré qu'il s'assurait de la conformité de ces bases de données biométriques exclusives avec les législations nationales en matière de protection des données des pays où ces activités ont lieu et des pays où ces partenaires sont établis.

41. Par exemple, les conditions suivantes ont été définies pour la gestion de la base de données norvégienne:

- Les volontaires ont été informés oralement et par écrit du fait que les échantillons biométriques («données brutes») étaient recueillis pour être stockés dans une base de données utilisée à des fins de recherche.
- Si les volontaires acceptaient, ils *consentaient par écrit* à fournir des images de leurs empreintes digitales à des fins d'enseignement, de recherche et de contrôle. Les formulaires de consentement écrit sont conservés par l'université norvégienne (partenaire du projet) qui effectue les contrôles.
- Les personnes concernées ont également obtenu le droit de formuler des objections à tout moment.
- L'autorité de protection des données en Norvège a été informée de la collecte des données («Meldeskjema») en janvier 2008, avant le début du projet, et leurs règlements ont suivi.
- Des mesures de sécurité techniques et d'organisation ont été prises pour sécuriser et protéger les données biométriques. Par exemple, les données sont stockées sur des ordinateurs avec le nom d'utilisateur/mot de passe dans des pièces fermant à clé. En outre, les ordinateurs ne sont pas connectés à l'internet ni à aucun autre réseau.
- Les données de cette base de données sont conservées uniquement par le Gjøvik University College (GUC), et l'accès est restreint aux chercheurs autorisés du GUC qui doivent utiliser les données. Les tests ont été effectués en Norvège.
- Les données ne sont pas transmises à des tiers ou à des partenaires du projet.

42. Compte tenu des différentes mesures prises concernant les bases de données exclusives, le CEPD se réjouit que les partenaires de Turbine ont mis en œuvre les exigences en matière de protection des données sur la base de la législation nationale sur la protection des données en vigueur dans les États membres où ils ont utilisé les bases de données susmentionnées.

*Bases de données accessibles au public*

43. Les tests de certains des partenaires reposaient également sur des bases de données biométriques accessibles au public. Il a été mentionné que différents partenaires du projet ont utilisé l'une d'elles, produite en Italie.

44. Le CEPD a analysé l'utilisation de *bases de données biométriques accessibles au public* obtenues d'un tiers aux seules fins de recherche et de test.

45. Tel qu'expliqué ci-dessus, le CEPD considère que la présence de certaines données biométriques, autres que des photographies seules, et le recours à un processus de comparaison présente des risques particuliers au regard des droits et libertés des personnes concernées.

46. Par conséquent, compte tenu du raisonnement mentionné ci-dessus, les données biométriques devraient être considérées comme des données à caractère personnel, car elles pourraient être utilisées pour identifier des individus, et la législation nationale en la matière doit être appliquée. Pour certaines autorités nationales de protection des données et pour le CEPD[11], ces bases de données biométriques font l'objet d'une procédure de notification.

47. Par exemple, il apparait pour le CEPD qu'en Italie, différents traitements de données biométriques doivent être notifiés à l'autorité italienne de protection des données (*Garante*). En outre, le traitement et la collecte de données biométriques en vue de créer une base de données biométriques constituent des traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées en raison de leur nature (données biométriques). Dans le cas du projet, il semble par conséquent nécessaire de vérifier si les données biométriques fournies au consortium ont été recueillies en conformité avec le cadre réglementaire national et si l'autorité de protection des données concernée a rendu un avis ou une autorisation attestant de la légalité de la base de données.

48. Suite à l'échange d'informations entre le CEPD et le consortium du projet, le projet fait une distinction entre le pays dans lequel la base de données accessible au public a été créée par un responsable du contrôle des données et les pays dans lesquels les partenaires du projet ont utilisé les données de la base de données.

49. Le consortium du projet a indiqué avoir effectué la vérification de la légalité des traitements dans les pays où cette base de données a été utilisée ultérieurement par les partenaires de Turbine en soumettant ses traitements aux autorités nationales de protection des données. Cependant, le CEPD n'a pas pu établir clairement si cette vérification a été effectuée par le consortium en ce qui concerne la base de données accessible au public produite en Italie. Dans pareil cas, le consortium devrait exiger de la part du fournisseur des données la garantie que celles-ci ont été recueillies dans le respect de la législation nationale en matière de protection des données mettant en œuvre la directive sur la protection des données. Par conséquent, le CEPD n'est pas en mesure d'évaluer si le consortium a reçu des garanties suffisantes démontrant que cette base de données est conforme sur le plan juridique avec la législation nationale du pays où le responsable du contrôle est établi.

2.2. Protocole de contrôle d'accès sécurisé

50. D'après les informations reçues, le protocole de contrôle d'accès sécurisé proposé dans Turbine vise à étendre les propriétés du dispositif d'authentification «match-on-card» (concordance entre les empreintes de l'utilisateur et les données contenues dans la carte), qui fournissent à la fois des garanties solides en matière de protection de la vie privée et une exactitude élevée, pour obtenir une solution qui renforce la procédure d'identification.

51. Il convient d'aborder la question de savoir si le stockage local de données biométriques sur du matériel sécurisé (c'est-à-dire un terminal) sans devoir utiliser un jeton, et leur traitement répondent aux exigences de sécurité et aux exigences en matière de protection de la vie privée et de la protection des données relatives à l'utilisation de données biométriques. Pour ce faire, une analyse contextuelle de la

[11] Le CEPD exige des institutions et organes européens une notification en vue d'un contrôle préalable de ces bases de données biométriques.

situation elle-même est nécessaire et doit reposer sur une analyse effectuée par les autorités nationales chargées de la protection des données.

52. En principe, le CEPD préfère l'utilisation du mode de recherche «un à un» au moyen duquel l'unité d'identification comparerait les données biométriques de l'individu avec un modèle unique (associé à l'identité). Un mode de recherche de ce type fournit des résultats plus précis.

53. Le CEPD accorde généralement sa préférence aux systèmes qui stockent les modèles biométriques dans des puces plutôt que dans des bases de données centrales à moins que des conditions spécifiques ne les exigent. Le stockage sur des puces permet manifestement une meilleure protection de la vie privée en ce sens que le modèle est stocké sur un support (par exemple un badge doté d'une puce) qui est en la possession de chaque personne concernée. La personne concernée par les données a elle-même un contrôle direct sur son modèle et en a la responsabilité. Personne d'autre n'a accès ou n'est en possession de son modèle. Le stockage dans des bases de données centrales pose un autre problème, le risque d'«hameçonnage» (phishing), en facilitant conséquent l'accès à la base de données à des fins autres que celles pour lesquelles elle avait été conçue. Un système décentralisé résout ce problème sans compromettre le niveau de sécurité dans la plupart des cas.

54. En effet, le CEPD considère que les mesures de sécurité ne devraient pas être appliquées uniquement contre les menaces extérieures, mais aussi contre les actes des utilisateurs eux-mêmes, en particulier dans le cas du système décentralisé. Les partenaires du projet Turbine ont souligné que l'analyse sur la sécurité réalisée par le projet aborde les attaques de l'intérieur, y compris celles perpétrées par les utilisateurs enregistrés. En outre, les solutions trouvées par le projet ont été conçues pour être intégrées ultérieurement dans une architecture dotée de toutes les mesures de sécurité classiques, techniques et organisationnelles, y compris les mesures contre les attaques lancées par des utilisateurs de l'intérieur. Le CEPD se réjouit de cette approche visant à préserver l'intégrité des données.

### 2.3 Essais

55. Le CEPD a analysé la façon dont le projet Turbine a mis les recherches en application dans des situations réelles. Comme mentionné dans les documents fournis, deux essais ont été réalisés: l'un à l'aéroport de Thessalonique (Grèce), selon deux scénarios, et un autre dans une fausse pharmacie en Allemagne.

56. Les deux essais visent à décrire la technologie mise au point dans Turbine. Le CEPD est ravi de constater que, dès le début de la mise en œuvre des essais, les partenaires du projet ont établi des contacts avec les autorités nationales de protection des données compétentes et ont soumis les documents appropriés. Le CEPD a aussi facilité les contacts avec les autorités de protection des données compétentes, dans le cadre des actions possibles prévues par son document stratégique.

#### 2.3.1 Essai grec:

57. L'essai grec se rapporte à l'installation d'un système pilote de contrôle d'accès biométrique dans les infrastructures critiques de l'aéroport international «Macedonia» de Thessalonique. L'installation effectuée dans le cadre de Turbine a été réalisée par le contrôleur de données (une société d'applications d'aviation

générale) en collaboration avec d'autres partenaires européens et est financée par l'Union européenne. Les documents fournis au CEPD décrivent les procédures et les mesures appliquées lors de l'essai.

58. Turbine décrit également en détail au CEPD les conditions dans lesquelles le contrôle d'accès utilisant la technologie Turbine a été mis en œuvre à l'aéroport de Thessalonique. Avant tout, le contrôle d'accès est installé uniquement pour contrôler l'accès à des endroits exigeant des mesures de sécurité spéciales. En outre, il n'implique qu'un nombre limité de volontaires.

59. Conformément à la législation nationale, une notification du système a été envoyée à l'autorité grecque de protection des données qui a émis un avis. L'autorité hellénique de protection des données a décidé que l'installation du système biométrique utilisé exclusivement à des fins de recherche scientifique ne contrevenait pas aux dispositions de la législation hellénique en matière de protection des données et a octroyé l'autorisation de procéder à l'essai. L'autorité hellénique de protection des données a toutefois imposé certaines conditions à respecter; l'essai a eu lieu tel que notifié sous réserve que la collecte et la conservation des échantillons biométriques originaux (bruts) pour effectuer des contrôles supplémentaires des performances n'ont pas été autorisées.

60. Le CEPD s'est réjoui qu'une procédure d'inscription sécurisée et respectueuse de la vie privée ait été élaborée dans la mesure où les personnes qui ont mise en place appliqué cette procédure ont été informées, formées et soutenues dans le but de parvenir à une saisie sécurisée et qualitative des données biométriques à des fins de consultation ultérieure.

61. Le CEPD constate également que des présentations ont été préparées et qu'une formation a été donnée en insistant sur l'importance de la protection des données lors de la phase d'inscription. Des experts partenaires de Turbine ont assuré une formation supplémentaire durant la véritable phase d'inscription. En outre, les formulaires de consentement et d'information ont été fournis et examinés avec les volontaires potentiels plusieurs semaines avant le début de l'inscription.

62. Ces procédures contribuent à l'application générale des principes de protection des données au cours du cycle de vie du projet. En garantissant la fourniture d'informations correctes aux individus et l'exactitude des données qui sont traitées dans la phase d'inscription, le projet garantit un niveau élevé de qualité des données.

63. De plus, lors d'une inscription de données biométriques, le CEPD analyse également la façon dont les solutions de secours sont appliquées. Dans le cas de l'essai grec, la solution de secours était garantie par le maintien des mesures existantes de contrôle d'accès qui n'ont pas été remplacées par la solution Turbine. Elles fonctionnaient en même temps ce qui permettait aux participants d'avoir recours aux contrôles d'accès existants en cas de problème avec l'essai de Turbine.

2.3.2 Essai allemand (GADM)

64. Des éclaircissements ont été apportés au sujet de l'essai allemand: en vertu de la législation allemande[12], le GADM ne devait pas être enregistré ou notifié si le délégué à la protection des données était nommé par le contrôleur, ce qui était le cas. Par conséquent, le délégué à la protection des données de Sagem-Orga a été tenu dûment informé par le contrôleur et conserve les informations, comme le prévoit la législation. Pour l'essai GADM, une note d'information a été soumise au délégué à la protection des données de Sagem-Orga afin de respecter les exigences applicables à l'enregistrement prévues dans l'article 4 sexies de la loi fédérale allemande relative à la protection des données. Le délégué à la protection des données de Sagem-Orga a été informé des éléments conformément aux dispositions de la législation allemande, y compris du nom du contrôleur, des noms des personnes en charge du traitement des données, des personnes autorisées à consulter les données et des finalités. Un formulaire de consentement a été préparé pour les volontaires et donne un aperçu clair des finalités pour lesquelles les données seront traitées lors de l'essai. Les volontaires ont aussi été dûment informés de leurs droits.

65. Pour cet essai, il était prévu que les administrateurs de l'inscription seraient informés de la nécessité d'une inscription sécurisée et respectueuse de la vie privée (transparent) et formés de la même manière. Il a également été souligné que les administrateurs de l'enregistrement du GADM sont des experts en traitement de données biométriques et qu'ils sont conscients de la nécessité d'avoir de bonnes données qualitatives de référence.

2.3.3 Résumé

66. Le CEPD conclut que, lors de la réalisation des deux essais, le consortium du projet a appliqué le principe de «privacy by design» de façon à faciliter l'évaluation réalisée par les autorités compétentes de protection des données.

## 3. Conclusion

67. Le CEPD accueille favorablement le projet, car il démontre que l'application du «privacy by design» en tant que principe-clé de la recherche constitue un moyen efficace de garantir des solutions respectueuses de la vie privée. Le «privacy by design» ne porte pas uniquement sur la conception et les solutions techniques des systèmes de TIC, il comprend aussi les différentes étapes de l'élaboration du projet et de ses pratiques organisationnelles. Ce dernier point peut être réalisé en garantissant le respect de la législation, en appliquant les principes de protection des données exigés, et en appliquant les procédures et la formation mises au point dans le but de garantir que toutes les parties concernées sont formées et informées de manière correcte. En outre, les essais donnent la possibilité de contrôler les avantages de l'application du principe dans des situations réelles.

[12] Article 4 quinquies, paragraphe 2 de la loi fédérale allemande sur la protection des données et article 4 septies - voir aussi article 4 quinquies, paragraphe 3 qui se rapporte au consentement comme base pour un enregistrement non obligatoire.

68. Il convient d'encourager la création de meilleures pratiques dans le contexte de l'utilisation de données biométriques afin de garantir que les recherches futures seront basées sur une approche sensée de la vie privée.

69. La mise en œuvre des deux caractéristiques de l'identification biométrique, l'irréversibilité et la révocabilité, contribue de façon significative au respect de la vie privée en fournissant des solutions acceptables à cet égard.

70. Le CEPD recommande de prendre en considération les observations suivantes:

- Lors de l'élaboration d'une liste de meilleures pratiques, il convient aussi de prendre en considération la nécessité de déterminer un niveau précis d'exactitude et de le réexaminer régulièrement.

- En outre, même s'il effectue les recherches conformément à des conditions juridiques strictes, le consortium du projet devrait exiger de ses fournisseurs de données biométriques qu'ils prouvent le plein respect de leur législation nationale en matière de protection des données.

Bruxelles, le 1er février 2011

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données