AVIS DU CEPD SUR L'AIPD DE L'ETIAS
(Dossier 2021-0640)

1. INTRODUCTION

- Le présent avis porte sur l'analyse d'impact relative à la protection des données (AIPD) réalisée par l'eu-LISA pour le système européen d'information et d'autorisation concernant les voyages (ETIAS).

- Le CEPD émet le présent avis conformément à l'article 57, paragraphe 1, point g), et à l'article 58, paragraphe 3, point c), du règlement (UE) 2018/1725[1] (le «règlement»).

2. CONTEXTE

L'ETIAS est établi par le règlement (UE) 2018/1240[2] (le «règlement ETIAS»). Il collectera et stockera des données à caractère personnel concernant les voyageurs exemptés de l'obligation de visa dans les États Schengen afin de déterminer si ces voyageurs présentent des risques en matière de sécurité, d'immigration irrégulière ou d'épidémie.

---

[1] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

[2] Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 (JO L 236 du 19.9.2018, p. 1.)

L'ETIAS consistera en un système d'information à grande échelle composé du système d'information ETIAS[3] (développé par l'eu-LISA), de l'unité centrale ETIAS[4] (créée au sein de l'Agence européenne de garde-frontières et de garde-côtes, Frontex) et des unités nationales ETIAS[5] (établies au sein d'une autorité compétente désignée dans chaque État membre)[6]. Le système d'information ETIAS se compose de plusieurs éléments, dont le système central ETIAS (qui comprend la liste de surveillance), les interfaces uniformes nationales, les infrastructures de communication, le portail pour les transporteurs, etc.[7]

Le règlement ETIAS impose à l'eu-LISA de développer le système d'information ETIAS et d'en assurer la gestion technique[8]. À cet égard, l'eu-LISA est chargée de respecter les principes de respect de la vie privée dès la conception et par défaut tout au long du cycle de vie du développement de l'ETIAS[9]. Le CEPD note que l'expression «respect de la vie privée dès la conception et par défaut» désigne la notion large des mesures technologiques visant à garantir la protection de la vie privée. Dans le présent avis, le CEPD emploie l'expression «protection des données dès la conception et protection des données par défaut» visé à l'article 27 du règlement, qui impose au responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles destinées à mettre en œuvre les principes relatifs à la protection des données[10].

Outre son rôle de développeur du système, les articles 57 et 58 du règlement ETIAS désignent l'eu-LISA comme responsable du traitement en ce qui concerne la gestion de la sécurité de l'information dans le système central ETIAS et comme sous-traitant en ce qui concerne le traitement de données à caractère personnel dans le système d'information ETIAS.

---

[3] Article 6 du règlement ETIAS.
[4] Article 7 du règlement ETIAS.
[5] Article 8 du règlement ETIAS.
[6] Article 3 du règlement ETIAS.
[7] Article 6, paragraphe 2, du règlement ETIAS.
[8] Articles 6, paragraphe 1, et 73 du règlement ETIAS.
[9] Article 73, paragraphe 3, du règlement ETIAS.
[10] Si les mesures prises au titre de l'article 27 du règlement contribueront aussi à atteindre l'objectif plus général de «respect de la vie privée dès la conception», le CEPD estime qu'un spectre plus large d'approches peut être pris en considération pour atteindre l'objectif de «respect de la vie privée dès la conception», qui comporte une dimension visionnaire et éthique, conforme aux principes et aux valeurs consacrés dans la Charte des droits fondamentaux de l'UE [Avis préliminaire du CEPD sur le respect de la vie privée dès la conception (avis 5/2018), disponible à l'adresse: https://edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf)]

Frontex (l'Agence européenne de garde-frontières et de garde-côtes) est considérée comme responsable du traitement des données à caractère personnel dans le système central ETIAS, tandis que l'unité nationale ETIAS de chaque État membre est considérée comme responsable du traitement des données à caractère personnel dans le système central ETIAS par cet État membre[11].

Compte tenu de la taille et de la complexité de l'ETIAS, le CEPD a organisé, le 6 décembre 2019 et le 24 mars 2020, deux réunions au niveau du personnel avec des membres de Frontex et de l'eu-LISA (y compris leurs DPD) ainsi que de la Commission européenne[12]. L'objectif de ces réunions était d'obtenir une compréhension claire du processus en place pour le développement de l'ETIAS, en particulier en ce qui concerne l'élaboration de l'analyse d'impact relative à la protection des données (AIPD), qui est un outil essentiel pour mettre correctement en œuvre les principes de protection des données dès la conception et protection des données par défaut.

L'élaboration de l'AIPD est une obligation qui incombe au responsable du traitement d'une activité de traitement de données. Dans le cas de l'ETIAS, cette obligation incombe conjointement à Frontex, aux unités nationales ETIAS et à l'eu-LISA. En tant que responsables conjoints du traitement de l'ETIAS, chacun d'eux devrait traiter non seulement les risques en matière de protection des données liés à leurs propres opérations de traitement des données au sein du système, mais aussi ceux liés à leurs interactions avec d'autres opérations de protection des données et d'autres systèmes. Ces AIPD ne peuvent donc pas être réalisées indépendamment l'une de l'autre.

Il est ressorti de ces discussions que l'eu-LISA, en sa qualité de développeur du système[13], avait assumé la responsabilité de coordonner l'ensemble du développement technique du système, y compris l'AIPD[14].

---

[11] Article 57 du règlement ETIAS.

[12] Des réunions au niveau du personnel ont eu lieu le 6 décembre 2019 (avec Frontex et l'eu-LISA) et le 24 mars 2020 (avec Frontex, l'eu-LISA et la Commission européenne).

[13] Articles 6 et 73 du règlement ETIAS.

[14] Réunion au niveau du personnel du 24 mars 2020 (avec Frontex, l'eu-LISA et la Commission européenne).

En conséquence, le 13 mai 2020, le CEPD a adressé à l'eu-LISA des recommandations préliminaires en ce qui concerne l'AIPD de l'ETIAS[15], qui complètent les orientations déjà fournies dans sa boîte à outils en matière de responsabilité.[16]

Le 17 juin 2021, l'eu-LISA a demandé l'avis du CEPD sur l'AIPD qu'elle avait réalisée pour l'ETIAS et a indiqué que le document envoyé pour consultation était l'AIPD finale.

3. ANALYSE DE L'AIPD

3.1. Nécessité d'une AIPD conformément à l'article 39 du règlement

En vertu de l'article 39 du règlement, lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Conformément à l'article 39, paragraphe 4, du règlement, le CEPD a établi une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise[17]. L'eu-LISA a relevé deux opérations de traitement à partir de cette liste (à savoir les «bases de données sur les exclusions» et le «traitement à grande échelle de catégories particulières de données à caractère personnel») justifiant la nécessité d'une AIPD[18].

---

[15] Lettre au DPD de l'eu-LISA du 13 mai 2020 (DH/GC/vm/ D(2020) 1207 C 2019-0495).

[16] La boîte à outils du CEPD en matière de responsabilité se compose de trois documents:

- Un résumé: lignes directrices relatives à la documentation des opérations de traitement pour les institutions, organes et agences de l'Union (IUE);
- Partie I: registres, registres centraux et quand procéder à une analyse d'impact relative à la protection des données; et
- Partie II: analyses d'impact relatives à la protection des données et consultation préalable.

Ces documents peuvent être consultés à l'adresse suivante: https://edps.europa.eu/node/4582_en.

[17] Décision du Contrôleur européen de la protection des données du 16 juillet 2019 concernant les listes d'AIPD publiées au titre de l'article 39, paragraphes 4 et 5, du règlement (UE) nº 2018/1725.

[18] Voir le tableau 4 «Base juridique» aux pages 20 et 21 de l'AIPD.

Le CEPD estime que l'eu-LISA devrait expliquer plus en détail l'identification de ces deux opérations de traitement dans le cadre de l'ETIAS. Cette étape d'explication est d'autant plus importante qu'elle fournit une première analyse des risques découlant de l'utilisation du système que l'AIPD doit traiter avec soin en définissant des mesures d'atténuation.

À cet égard, le CEPD rappelle sa liste non exhaustive de critères permettant d'évaluer si les traitements sont susceptibles d'entraîner des risques élevés[19], ainsi que sa «boîte à outils en matière de responsabilité»[20].

Dans le cadre de l'explication de la réalisation d'une AIPD, le CEPD note que l'ETIAS collectera et traitera un volume considérable de données à caractère personnel (y compris sur des infractions pénales) concernant des millions de personnes et recoupera ces données avec des données stockées dans plusieurs autres systèmes informatiques à grande échelle, y compris des bases de données centrales pour la coopération des services répressifs. Ces données seront utilisées pour étayer les décisions susceptibles d'être préjudiciables aux personnes. En outre, un ensemble de règles d'examen sera utilisé pour dresser le profil des personnes concernées et déterminer automatiquement les éventuels individus à risque pour lesquels un traitement manuel de leurs demandes sera requis.

L'incidence pourrait être importante, étant donné que le refus d'entrée sur le territoire Schengen sur la base du traitement des données dans ETIAS peut entraîner une série de conséquences négatives pour les personnes. Ces conséquences comprennent une restriction à la jouissance de leur liberté de circulation, une incidence financière lorsqu'elles se rendent dans l'UE à des fins professionnelles ou pour des problèmes de santé si elles se rendent dans l'UE pour obtenir un traitement médical qu'elles ne peuvent obtenir dans leur propre pays. En outre, l'accès des services répressifs aux données stockées dans l'ETIAS peut également porter préjudice aux personnes, qui pourraient être au centre de l'attention des services répressifs et faire l'objet de mesures d'enquête.

---

[19] Décision du Contrôleur européen de la protection des données du 16 juillet 2019 concernant les listes d'AIPD publiées au titre de l'article 39, paragraphes 4 et 5, du règlement (UE) nº 2018/1725.

[20] En particulier, le chapitre 4 de la boîte à outils en matière de responsabilité (partie I) contient des critères permettant de déterminer quand une AIPD est obligatoire, ainsi qu'une liste d'opérations à risque.

À la lumière de ce qui précède, le CEPD estime que l'eu-LISA devrait expliquer plus en détail les types d'opérations de traitement recensés qui ont conduit à la décision de procéder à une AIPD, par exemple en tenant compte de la liste non exhaustive de critères du CEPD permettant d'évaluer si les traitements sont susceptibles d'entraîner des risques élevés.

L'identification approfondie des critères de risque élevé peut aider l'équipe chargée de l'AIPD en fournissant une vue d'ensemble des indicateurs de risque élevé qui devraient être traités au cours de la phase d'évaluation. Il s'agit également d'un bon exercice pour former le personnel de l'eu-LISA et faire en sorte qu'à l'avenir, aucun critère ne soit omis, ce qui conduirait à des décisions injustifiées de ne pas procéder à une AIPD, tandis que le traitement des données pertinent pourrait présenter un risque élevé pour les droits fondamentaux des personnes concernées.

Le CEPD recommande à l'eu-LISA d'expliquer plus en détail les types d'opérations de traitement recensés qui ont conduit à la décision de procéder à une AIPD, en tenant compte de la liste non exhaustive de critères du CEPD permettant d'évaluer si les traitements sont susceptibles d'entraîner des risques élevés.

3.2. Structure de l'AIPD

Le CEPD se réjouit que l'AIPD suive de manière générale la structure du modèle de rapport de l'AIPD prévu dans la boîte à outils en matière de responsabilité.[21] Après une analyse détaillée de chacun des éléments de l'AIPD afin de déterminer s'ils fournissent les informations requises par le règlement comme expliqué dans la boîte à outils en matière de responsabilité, nous formulons les recommandations et suggestions d'amélioration suivantes dans les sections ci-dessous.

[21] Voir annexe III de la boîte à outils, partie II

3.3. Portée de l'AIPD

L'eu-LISA a fourni une description de la portée de l'AIPD dans le résumé. Plus particulièrement, elle mentionne que «cette AIPD évalue les risques en matière de protection des données recensés dans le cadre de la conception et du développement de l'ETIAS. Il s'agit d'une première étude qui devra être complétée par des contributions synergiques de Frontex et des États membres afin de réaliser une évaluation exhaustive de tous les risques liés à la mise en place de l'ETIAS» (p. 8). Dans le même temps, l'analyse des risques se concentre sur les responsabilités de l'eu-LISA en ce qui concerne la conception, le développement et la gestion de la sécurité de l'information de l'ETIAS.

Le CEPD considère que, compte tenu de la complexité du système et des différents rôles des acteurs concernés, l'AIPD reçue n'est pas la version finale de l'AIPD de l'ETIAS. Étant donné que l'eu-LISA coordonne la mise en œuvre du système et applique le principe de la protection des données dès la conception et protection des données par défaut, l'eu-LISA est chargée de mettre à jour cette AIPD en tenant compte des contributions reçues des États membres et de Frontex en ce qui concerne les risques recensés dans leurs AIPD respectives.

Le CEPD recommande à l'eu-LISA d'élaborer une AIPD complète qui inclue les risques recensés par toutes les parties prenantes (à savoir Frontex, les États membres, Europol et l'eu-LISA) et ceux découlant du développement et du fonctionnement de l'ETIAS, avant la mise en service du système.

3.4. Identification proactive des risques par les principaux acteurs concernés

Compte tenu de la complexité de l'ETIAS, notamment en ce qui concerne ses liens avec d'autres systèmes et le rôle clé de plusieurs parties prenantes, il est essentiel d'assurer une bonne coordination entre toutes ses parties prenantes afin d'élaborer des stratégies appropriées pour faire face à tous les risques recensés. En particulier, trois acteurs principaux participent à l'ETIAS: l'eu-LISA, Frontex (l'unité centrale ETIAS) et les États membres (les unités nationales ETIAS). Europol est également un acteur important participant à l'ETIAS,

car elle introduira des données dans la liste de surveillance ETIAS[22] et fera partie du comité d'examen ETIAS, conseillant Frontex sur les règles d'examen ETIAS[23].

Lors de l'élaboration et de la conception de l'ETIAS, l'eu-LISA doit tenir compte de tous les risques pour les personnes concernées résultant de l'utilisation du système dans son ensemble. Ce n'est qu'une fois que l'ETIAS sera opérationnel que certaines parties du traitement relèveront de la responsabilité et du contrôle de Frontex (l'unité centrale ETIAS) et des États membres (les unités nationales ETIAS).

Frontex et les États membres doivent effectuer leurs propres AIPD sur leurs activités de traitement avant la mise en service de l'ETIAS. Toutefois, celles-ci peuvent introduire de nouvelles exigences fonctionnelles pour l'ETIAS, dans le cadre de mesures d'atténuation. Outre le fait de s'y attendre à un stade ultérieur de la conception, l'eu-LISA devrait adopter une position proactive de soutien dans l'identification de ces risques et de la manière dont le système pourrait contribuer à les éviter ou à les atténuer. L'analyse globale des flux de données et la participation des autres parties prenantes à l'examen de cette AIPD sont utiles en ce sens.

L'AIPD indique que l'eu-LISA a consulté de nombreuses parties prenantes externes (notamment Frontex, les représentants des États membres et Europol) et que les résultats de ces consultations ont été inclus comme contributions dans l'élaboration de l'AIPD (sous-section 4.5.2). Toutefois, le CEPD n'a pas trouvé, dans l'AIPD, d'exemples de risques découlant de ces activités de traitement de données ou liés aux interactions entre le système et les opérations de traitement relevant de la responsabilité de l'unité centrale ETIAS, des unités nationales ETIAS ou d'Europol.

Parmi les risques qui pourraient être recensés à un stade précoce, on peut citer:

- les retards dans le traitement manuel de la demande ETIAS par l'unité centrale ETIAS, l'unité nationale ETIAS ou Europol (dans le cadre de la consultation au titre de l'article 29) ou dans le traitement des demandes d'accès des personnes concernées.

  Bien que le règlement ETIAS ait tenu compte des seuils légaux déclenchant le traitement des demandes, il peut y avoir des cas d'urgence où des ressortissants de

[22] Article 34 du règlement ETIAS.
[23] Articles 9 et 33 du règlement ETIAS.

pays tiers (les «RPT») doivent voyager dans l'intervalle de temps avant la date limite, mais ne peuvent le faire en raison du traitement manuel. Dans le cadre de l'atténuation de ces risques, l'eu-LISA et les parties prenantes concernées devraient examiner si et comment le système pourrait contribuer à les réduire au maximum, par exemple en fournissant des rapports sur les demandes pendantes ou des alertes pour les demandes qui atteignent la date limite ou la date du voyage;

- des erreurs ou retards dans le traitement manuel de la demande ETIAS dus à un personnel insuffisamment formé, entraînant l'incapacité des RPT à voyager.

  Dans le cadre de l'atténuation de ces risques, l'eu-LISA et les parties prenantes concernées devraient examiner si et comment le système pourrait contribuer à la détection de telles erreurs par des agents utilisant le système, par exemple en fournissant des statistiques sur le nombre de demandes que l'utilisateur a rejetées par rapport aux demandes d'accès introduites par les RPT;

- les risques liés à la qualité des données, tels que les erreurs dans les données insérées dans la liste de surveillance ETIAS par les États membres et/ou Europol ou dans d'autres bases de données consultées par le système ETIAS (5.5.-traitement automatisé).

  L'eu-LISA et les parties prenantes concernées devraient examiner si et comment le système pourrait contribuer à la détection de telles erreurs.

Le CEPD recommande d'inclure dans l'AIPD les risques liés aux interactions du système avec les opérations de traitement relevant de la responsabilité d'autres parties prenantes (à savoir l'unité centrale ETIAS, les unités nationales ETIAS et/ou Europol), en concertation étroite avec celles-ci.

3.5. Description du traitement

L'établissement du contexte et la description des opérations de traitement constituent le fondement d'une AIPD solide et sont essentiels pour identifier correctement les risques pour les droits fondamentaux des personnes. Comme souligné dans la boîte à outils en matière de

responsabilité[24], la description devrait permettre au lecteur (par exemple, les personnes concernées par le traitement, le CEPD ou d'autres parties prenantes) de comprendre clairement les opérations de traitement, y compris les raisons et la manière dont elles sont effectuées.

La description doit notamment comprendre:

- un organigramme des données du processus: qu'est-ce qui est collecté à partir d'où/auprès de qui, qu'est-ce qui en est fait, où est-ce conservé, à qui cela est-il donné?
- une description de la ou des finalités du traitement: comme pour les autres éléments, cette explication devrait être donnée étape par étape, en distinguant les finalités le cas échéant[25];
- une description de ses interactions avec d'autres processus – ce processus repose-t-il sur des données à caractère personnel fournies par d'autres systèmes? Les données à caractère personnel de ce processus sont-elles réutilisées dans d'autres processus?
- une description de l'infrastructure d'appui: bases de données, intégration de nouvelles technologies, etc.

Le chapitre 4 de l'AIPD vise à fournir une description générale du traitement, tandis que le chapitre 5 présente de manière plus détaillée les différentes activités de traitement.

Compte tenu de la complexité du système, le CEPD juge approprié d'adopter une approche descendante, c'est-à-dire de donner une vue d'ensemble des principales opérations de traitement et de passer ensuite à une description plus détaillée et plus précise de ces opérations. Toutefois, comme expliqué plus en détail ci-dessous (points 3.4.1 et 3.4.2), le CEPD note que la vue d'ensemble est incomplète, tandis que certaines étapes intermédiaires font défaut et que certaines étapes spécifiques ne sont pas suffisamment détaillées pour permettre une visualisation et une compréhension claires du système.

[24] Voir boîte à outils du CEPD en matière de responsabilité, partie I, page 7.

[25] Dans le cadre de cette description, il convient de fournir une brève explication des raisons pour lesquelles l'organisation doit effectuer cette opération de traitement et sur la manière dont elle se limite à ce qui est nécessaire pour atteindre la finalité du traitement (nécessité et proportionnalité).

3.5.1. Description générale (chapitre 4 de l'AIPD)

Le CEPD note que de nombreux éléments pour une description générale de l'activité de traitement des données sont mentionnés au chapitre 4. Toutefois, la manière dont ils sont présentés et décrits ne permet pas une compréhension claire, fluide et complète de l'activité de traitement des données. Cette situation est aggravée par l'absence d'un organigramme des données montrant la manière dont les données à caractère personnel transitent par le système (d'où viennent les données, où vont-elles, comment évoluent-elles et où finissent-elles).

Le CEPD souligne l'importance d'une visualisation claire de l'ensemble du système. Cela pourrait commencer par la vue d'ensemble du système, qui est ensuite décomposée en principales opérations de traitement de données, qui sont à leur tour divisées en sous-processus. Des organigrammes des données pourraient être réalisés en plusieurs couches imbriquées. Un seul processus sur un organigramme de haut niveau pourrait être étendu pour montrer un organigramme des données plus détaillé. En d'autres termes, une hiérarchie des organigrammes des données pourrait être établie, en commençant par une vue abstraite du système et en se terminant par un certain nombre d'organigrammes représentant les sous-processus du niveau le plus bas.

Le niveau le plus élevé («niveau 0») pourrait simplement montrer le système, les entités externes avec lesquelles il interagit et les flux de données entre le système et les entités externes. Le premier niveau pourrait inclure les principales opérations de traitement de données, tandis qu'un second niveau irait dans le sens d'un approfondissement des principales opérations de traitement. Le CEPD note que l'AIPD est dépourvu des organigrammes des données de «niveau 0» et de «niveau 1» qui permettraient une visualisation et une compréhension claires du système.

L'aperçu synthétique de l'ETIAS à la page 29 donne une bonne vue d'ensemble des composantes du système, ce qui permet de reconstituer l'architecture du système, mais une visualisation des flux de données et des principales opérations de traitement des données fait défaut.

Il est également difficile d'obtenir cette visualisation dans la description générale.

La section 4.3 (description générale de l'activité de traitement des données) contient soit des aspects trop détaillés (par exemple, le fait que l'unité centrale ETIAS devrait être opérationnelle 24 heures sur 24), soit des aspects incomplets (par exemple, l'identification d'entités externes).

Les informations relatives à l'activité de traitement des données (par exemple, les données collectées, les destinataires, etc.) sont simplement énumérées à la section 4.2, mais sont sans lien entre elles. Ce lien est toutefois essentiel pour obtenir une vue d'ensemble complète de l'activité de traitement des données. Par exemple, tous les destinataires des données énumérées au point 4.3.4 ne sont pas intégrés dans la description.

En outre, plusieurs flux de données attendus ne figurent pas dans la description du système. Par exemple, la révocation de l'autorisation de voyage ETIAS (qui pourrait entraîner des risques liés à l'absence de notification de l'utilisateur) ou la vérification par les RPT de leur demande ou de la validité de l'ETIAS.

À la lumière de ce qui précède, le CEPD recommande d'ajouter deux organigrammes des données («niveau 0» et «niveau 1») au chapitre 4 de l'AIPD afin de permettre une visualisation claire de la manière dont les informations entrent dans le système et en sortent en général, de ce qui les modifie et du lieu où les informations sont stockées. Le premier organigramme doit montrer le système, les entités externes avec lesquelles il interagit et les flux de données entre le système et les entités externes. Le second devrait étoffer le premier et inclure les principales opérations de traitement des données.

Le CEPD recommande également de revoir la structure du chapitre 4 afin de décrire de manière claire, ciblée et complète ces deux organigrammes des données.

3.5.2. Description systématique (chapitre 5 de l'AIPD)

Le chapitre 5 décrit plus en détail les principales opérations de traitement indiquées dans la description générale (voir chapitre 4). Cela pourrait être considéré comme l'organigrammes des données «de niveau 2».

Pour chaque opération principale de traitement, l'AIPD prévoit:

- un organigramme;
- un tableau énumérant les différentes étapes mentionnées dans l'organigramme, y compris pour chacune d'entre elles;
    - une référence à la sous-section décrivant chaque étape;
    - la finalité;
    - le support des données;
- une description du processus pour chaque étape;
- une vue d'ensemble.

Le CEPD se félicite de cette approche. Il constate toutefois un certain manque de clarté, d'exhaustivité et/ou de cohérence.

L'organigramme, le tableau et les descriptions de chaque étape ne sont pas toujours présents ou alignés. Par exemple, la section 5.6 relative au traitement manuel ne comporte pas de tableau. À la section 5.5, les différentes étapes mentionnées dans le tableau ne figurent ni dans l'organigramme ni dans la description (par exemple, divulgation/transfert des données). Dans cette même section, des éléments de la vue d'ensemble n'apparaissent pas dans l'organigramme (par exemple, le CIR) et inversement (par exemple, les règles d'examen). Les utilisateurs qui exécutent chaque étape de l'action ne sont pas toujours indiqués. Une formulation différente est utilisée pour une même étape (par exemple, le tableau de la section 5.5 mentionne la «fusion des ensembles de données» tandis que l'organigramme et la description font référence au «résultat consolidé»).

En outre, l'AIPD devrait clarifier et décrire davantage certaines principales opérations de traitement de données plutôt que de se limiter à copier les dispositions juridiques. Par exemple, la section 5.5 sur les opérations de traitement automatisé devrait décrire, pour chaque système (SIS, VIS, etc.), les données contenues dans la demande du RPT qui seront utilisées pour la comparaison, ainsi que les situations (c'est-à-dire les données ou la combinaison de données) qui déclencheront une réponse positive.

À la lumière des observations qui précèdent, le CEPD recommande de veiller à ce qui suit:
- un organigramme, un tableau et une description sont inclus pour chaque opération principale de traitement de données;
- toutes les étapes sont recensées dans l'organigramme et le tableau et sont décrites de manière claire et cohérente;
- la description de chaque étape inclut l'utilisateur, l'action, les données et le support.

3.6. Évaluation de la nécessité et de la proportionnalité

Le chapitre 6 de l'AIPD indique qu'il vise à évaluer la nécessité et la proportionnalité des activités de traitement ETIAS énumérées au chapitre 4.

Toutefois, au lieu d'évaluer la conception technique et les fonctionnalités choisies par l'eu-LISA pour mettre en œuvre le règlement ETIAS, le chapitre 6 évalue principalement le règlement ETIAS. Le CEPD souligne qu'une telle évaluation relève de la responsabilité du législateur et non de l'eu-LISA.

L'eu-LISA doit se conformer à la législation et la mettre en œuvre telle qu'elle a été adoptée. L'AIPD à effectuer par l'eu-LISA en tant que responsable du traitement des données concerne ses sélections dans la conception technique[26].
Elle devrait s'efforcer de répondre à la question suivante: «comment l'eu-LISA peut-elle s'acquitter des tâches qui lui sont confiées par le législateur en garantissant à la fois la conformité et le respect de la vie privée?»

Par exemple, lorsque le projet de demande est soumis et stocké, le système recueille des informations auprès de l'utilisateur (RPT), telles que l'adresse IP, l'horodatage et les informations relatives à l'appareil (section 5.3.10). Cela pourrait être effectué à des fins de journalisation, d'audit et de statistiques sur le navigateur de l'utilisateur (afin de garantir la fourniture de statistiques adéquates sur les navigateurs à prendre en charge).

L'eu-LISA devrait évaluer la nécessité et la proportionnalité de chaque donnée collectée dans ce contexte. Elle devrait veiller à ce que seules les données nécessaires à l'appareil de l'utilisateur soient collectées et à ce qu'il existe une politique adéquate consistant à ne pas révéler ces informations à d'autres entités (par exemple, les services répressifs) si elles ne concernent pas l'enquête sur l'auteur d'une demande pour une autre personne ou pour non-répudiation. Le risque de ne pas recenser et de ne traiter que les données nécessaires pourrait avoir pour danger que l'utilisateur soit soumis à un profilage ou à une utilisation non autorisée de ces informations.

[26] Voir boîte à outils du CEPD en matière de responsabilité, partie I, pages 7 et 8.

Un autre exemple pourrait concerner l'utilisation d'outils spécifiques. Dans certaines conditions, le demandeur est autorisé à passer l'entretien requis à distance[27]. Le responsable de l'unité nationale ETIAS et le RPT conviennent de l'outil à utiliser à partir d'une liste d'outils présélectionnés par l'eu-LISA. Si l'outil d'entretien recueille plus de données à caractère personnel sur le RPT que nécessaire (par exemple, des données de connexion), il existe un risque de profilage et d'utilisation non autorisée de ces données.

La responsabilité de l'eu-LISA comprend l'analyse des données à caractère personnel que ces outils présélectionnés collectent au sujet des RPT et de leurs appareils, ainsi que la question de savoir s'il s'agit du minimum requis pour atteindre l'objectif visé par la conduite de l'entretien. Par ailleurs, tout transfert de données à caractère personnel (contenu de la communication ou métadonnées) à des tiers et à des pays tiers devrait faire l'objet d'une analyse approfondie sous l'angle de la légalité, mais aussi de la nécessité et de la proportionnalité.

Le CEPD recommande de revoir le chapitre 6 et d'expliquer:
- pourquoi la conception et les fonctionnalités techniques proposées de l'ETIAS constituent des moyens efficaces pour mettre en œuvre le règlement ETIAS;
- si l'eu-LISA a envisagé des solutions de remplacement; et
- pourquoi les solutions retenues sont les moyens les moins intrusifs du point de vue des droits fondamentaux.

3.7. Analyse des risques et mise en place de maîtrise des risques identifiés

Un risque est un événement possible qui pourrait causer des dommages ou pertes, ou affecter la capacité à atteindre les objectifs. Lors de la définition d'un risque dans le contexte d'une AIPD, l'objectif est de protéger les libertés et droits fondamentaux des personnes concernées et/ou de respecter les principes de protection des données prévus par le cadre juridique applicable (qui visent également à protéger les droits des personnes concernées). S'il existe

[27] L'article 27, paragraphe 4, du règlement ETIAS dispose ce qui suit: «Si le consulat le plus proche du lieu de résidence du demandeur est distant de plus de 500 kilomètres, le demandeur se voit offrir la possibilité de procéder à l'entretien à l'aide de moyens de communication audiovisuels à distance. Si la distance est inférieure à 500 kilomètres, le demandeur et l'unité nationale ETIAS de l'État membre responsable peuvent décider d'un commun accord d'utiliser de tels moyens de communication audiovisuels.»

également un risque de conformité pour l'organisation, l'accent est mis sur l'incidence sur les droits et libertés des personnes concernées[28].

Comme indiqué ci-dessus (points 3.4 et 3.5), la description fournie dans l'AIPD pour le système et les processus de données ne favorise pas un concept clair de l'ensemble du système, ce qui est nécessaire pour recenser les risques de haut niveau et pour comprendre l'incidence qu'ils pourraient avoir sur les personnes concernées (RPT).

L'évaluation des risques effectuée dans le cadre d'une AIPD comprend la détermination des éléments suivants[29]:

- ce qui pourrait mal se passer (le risque);
- ce qui pourrait conduire à la réalisation du risque (la source);
- la probabilité que le risque puisse nuire aux personnes (la probabilité);
- quel serait l'incidence négative pour les personnes (incidence);
- quelle serait la gravité de l'incidence négative (gravité);
- quelles seraient les mesures de contrôle appropriées pour éliminer, atténuer ou réduire au maximum les risques (mesures d'atténuation).

Le chapitre 7 (p. 120) énumère les risques recensés tout au long du chapitre 5, qui décrit la fonctionnalité (par exemple, le risque 1 à la page 60). Le CEPD note que la plupart des risques sont liés à une action erronée dans le traitement (par exemple, l'accès non autorisé à des données privées dans le cadre du risque 1) ou à une atteinte à un principe de protection des données (par exemple, équité, transparence, exactitude, sécurité dans le cadre du risque 1). Toutefois, l'incidence sur la personne concernée n'est pas indiquée. Le CEPD souligne qu'il importe de décrire les quatre éléments, à savoir la source, le risque, l'incidence et la ou les mesures d'atténuation afin de permettre une évaluation appropriée des risques.

Un exemple des éléments attendus est donné ci-dessous pour le risque 1:

- source: courriel erroné saisi par la personne concernée;

---

[28] Voir boîte à outils du CEPD en matière de responsabilité, partie II, pages 8 à 10.

[29] Voir groupe de travail «Article 29», «Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679», adoptées le 4 avril 2017 par le CEPD, disponibles à l'adresse: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_en*, pages 17 et 22.

- risque: accès non autorisé - la personne non autorisée qui accède à la demande peut retirer la demande, communiquer les informations à d'autres personnes ou utiliser les informations à d'autres fins;
- incidence:sur le plan financier, sur la réputation, l'usurpation d'identité;
- atténuation: validation du courriel avant que l'utilisateur n'introduise des données à caractère personnel.

Le CEPD note que l'AIPD contient une base de connaissances pour les évaluations de l'incidence, qui énumère des exemples d'incidences physiques, matérielles et morales sur la personne. Il suggère de décrire l'incidence de chaque risque en se fondant sur cette base de connaissances.

En outre, le CEPD note que l'AIPD énumère 21 risques que l'eu-LISA considère comme limités ou négligeables après l'application des mesures d'atténuation. Toutefois, cette liste n'inclut pas les risques éliminés ou considérés comme faibles après leur atténuation au moyen des mesures de sécurité de base de l'eu-LISA. Le CEPD souligne que ces risques et mesures d'atténuation devraient être présentés dans l'AIPD afin de démontrer que tous les risques pertinents ont été recensés mais sont considérés comme atténués. Une telle pratique guiderait également l'intégration de ces mesures dans la conception de la mise en œuvre du système ETIAS lors des prochaines étapes.

En outre, le CEPD note que l'analyse de sécurité (section 7.1.7) est incomplète, étant donné que l'évaluation des risques en matière de sécurité pour l'ETIAS n'est pas encore réalisée. Étant donné que le processus de gestion de la sécurité de l'information comprend une évaluation des risques en matière de sécurité pour les actifs de l'organisation (y compris les données à caractère personnel), en mettant l'accent sur l'organisation, toute décision relative à la mise en œuvre de mesures d'atténuation sera fondée sur les coûts et l'incidence sur l'organisation.

Les résultats de l'évaluation des risques en matière de sécurité (risques résiduels après mesures d'atténuation) devraient être intégrés à l'AIPD, afin d'évaluer également le risque du point de vue des personnes concernées. Bien qu'une explication analytique des risques en matière de sécurité (par exemple, par type d'attaque d'utilisateurs malveillants) ne soit pas nécessaire, il convient de fournir une description générale de ces risques (par exemple, des acteurs externes malveillants qui obtiennent un accès non autorisé aux données du

demandeur via le site web), de les cartographier en fonction des risques liés à la protection des données (accès non autorisé, par exemple) et de les réévaluer.

Le CEPD se félicite que l'eu-LISA ait déjà recensé certains risques en matière de sécurité, dans le cadre du processus de l'AIPD (par exemple [...]). Elle a également recensé au préalable des risques spécifiques en matière de sécurité qui auront une incidence significative sur les données à caractère personnel, en supposant des vulnérabilités de [...].

Toutefois, le CEPD note qu'aucun risque lié aux incidents de sécurité au sein de l'unité centrale ETIAS n'a été relevé. Il rappelle que l'eu-LISA agit en tant que responsable du traitement des données en ce qui concerne la gestion de la sécurité de l'information du système central ETIAS et attend une évaluation approfondie des risques en matière de protection des données découlant des risques en matière de sécurité de l'information.

Dans l'ensemble, parmi les exemples de risques à prendre en considération figurent:

- Les risques liés à l'accès non autorisé à la demande présentée, par exemple pour les raisons suivantes:
    - une autre personne qui accède au courrier électronique de l'utilisateur et obtient le lien de la demande, puis retire ou modifie cette demande,
    - une erreur technique du système qui envoie le lien à un autre demandeur,
    - l'utilisateur se trompe en saisissant son adresse électronique et l'hyperlien de la demande est envoyé à une autre adresse électronique,
    - l'utilisateur est amené à penser à tort qu'en sauvegardant le projet de demande, sa demande est soumise,
    - l'utilisateur perd l'accès au compte de messagerie électronique ou le fournisseur de messagerie électronique cesse ses activités.

- Les risques liés au traitement automatisé de la demande (y compris la gestion de la liste de surveillance), par exemple la fourniture des données du demandeur à Europol, pour les raisons suivantes:
    - une réponse positive contenant des données Europol, lorsque le demandeur est enregistré en tant que victime ou témoin;
    - une réponse faussement positive résultant d'une mise en œuvre technique erronée des indicateurs de risques visés à l'article 33 (sous-section 5.5.1);

- une liste de surveillance non actualisée (sous-section 5.9.5).

- Les risques liés au paiement des droits de la demande ETIAS, par exemple en raison de:
  - l'utilisation abusive des données de paiement par la banque du demandeur (elle sait que le titulaire de la carte a effectué une transaction pour le paiement des droits à ETIAS, mais pas les détails de la demande);
  - un problème technique résultant de l'absence de confirmation du paiement.

- Les risques liés à l'accès par les services répressifs ou les services de contrôle aux frontières, par exemple pour les raisons suivantes:
  - identification d'une réponse positive erronée à partir des résultats: les données des demandeurs sont saisies dans les systèmes des services répressifs;
  - recherche approfondie du système, sans remplir les critères de recherche (infraction grave, demandeur présent à la frontière, informations déjà présentes dans le système EES, etc.);
  - le stockage et l'utilisation des données consultées à d'autres fins.

- Risques liés à l'accès par les unités nationales ETIAS au système central ETIAS:
  - l'exportation non autorisée de données stockées dans le système central ETIAS par les unités nationales ETIAS et l'importation de ces données dans les systèmes nationaux à d'autres fins de traitement.

- Les risques liés à l'accès par les transporteurs, par exemple pour les raisons suivantes:
  - recherche de demandeurs qui ne vont pas voyager;
  - accès à des données non actualisées dans la base de données en lecture seule (un ETIAS a été délivré au cours des dernières 24 heures).

- Les risques liés à l'exercice des droits d'accès des personnes concernées, par exemple pour les raisons suivantes:
  - vérification incorrecte de l'identité d'un demandeur présentant une demande d'accès/de rectification/d'effacement;
  - incapacité à identifier clairement l'autorité qui introduit des données relatives au demandeur dans l'un des systèmes consultés par le système central ETIAS.

- Les risques liés aux incidents de sécurité des données ou à la conservation des données, par exemple pour les raisons suivantes:
    - absence d'information de la personne concernée en cas de violation de données (que ses données aient été consultées, modifiées ou supprimées);
    - non-effacement des données provenant des demandes ou des journaux conformément à la politique de conservation des données;
    - absence de combinaison des journaux provenant de différents systèmes pour enquêter sur un incident de sécurité tel qu'un accès non autorisé.

À la lumière de ce qui précède, le CEPD recommande ce qui suit:

- réexaminer l'AIPD une fois que la description générale des flux de données dans le système sera complète afin de s'assurer qu'aucun risque de niveau élevé n'a été négligé;
- veiller à ce que, pour chaque risque spécifique recensé, la source, l'incidence et la mesure d'atténuation soient décrits;
- énumérer *tous* les risques recensés, y compris les risques faibles;
- réexaminer l'AIPD et réévaluer les risques en matière de protection des données, sur la base des risques en matière de sécurité recensés à l'issue de l'évaluation des risques en matière de sécurité ETIAS.

4. CONCLUSIONS

Le CEPD se réjouit que l'AIPD suive de manière générale la structure du modèle de rapport de l'AIPD prévu dans la boîte à outils en matière de responsabilité. Il se félicite également de l'approche descendante du rapport (description d'une vue d'ensemble des principales opérations de traitement puis passage à une description plus détaillée et plus précise de ces opérations), compte tenu de la complexité de l'ETIAS.

En tant qu'outil vivant, l'AIPD ne doit pas être fixée une fois pour toutes, mais peut être complétée et développée tout au long de la mise en œuvre et du fonctionnement de l'ETIAS. Toutefois, l'analyse ci-dessus a montré qu'à ce stade précoce de la mise en œuvre, des éléments importants font toujours défaut ou ne sont pas présentés de manière claire et complète pour permettre une identification et une évaluation adéquates et complètes des risques pour les droits fondamentaux de la personne.

Compte tenu de la complexité du système ETIAS, y compris, entre autres, ses liens avec d'autres systèmes, et du rôle clé de plusieurs parties prenantes, le CEPD recommande à l'eu-LISA d'élaborer une version complète de l'AIPD, qui inclurait les risques et les mesures d'atténuation recensés par d'autres responsables du traitement dans leurs propres évaluations des risques en matière de protection des données, avant le déploiement du système. Cela permettra de faire en sorte que les risques découlant de l'utilisation globale de l'ETIAS soient traités de manière adéquate.

Le CEPD formule les recommandations suivantes à l'intention de l'eu-LISA afin de garantir le respect du règlement ETIAS (en particulier en ce qui concerne la mise en œuvre du principe de la protection des données dès la conception et protection des données par défaut) et du règlement:

- Indiquer et décrire tous les critères applicables conduisant à la décision de procéder à une AIPD.

- Fournir une AIPD complète, incluant les risques recensés par les AIPD des autres parties prenantes (à savoir l'unité centrale ETIAS, les unités nationales ETIAS et/ou Europol), avant la mise en service de l'ETIAS.

- Inclure dans l'AIPD les risques liés aux interactions du système avec les opérations de traitement relevant de la responsabilité d'autres parties prenantes (à savoir l'unité centrale ETIAS, les unités nationales ETIAS et/ou Europol) en concertation étroite avec ces dernières.

- Ajouter deux organigrammes des données («niveau 0» et «niveau 1») au chapitre 4 de l'AIPD afin de permettre une visualisation claire de la manière dont les informations entrent dans le système et en sortent en général, de ce qui les modifie et du lieu où les informations sont stockées. Le premier montrerait le système, les entités externes avec lesquelles il interagit et les flux de données entre le système et les entités externes. Le second étofferait le premier et inclurait les principales opérations de traitement des données.

- Au chapitre 5, veiller à ce qui suit:
  - un organigramme, un tableau et une description sont inclus pour chaque opération principale de traitement de données;
  - toutes les étapes sont recensées dans l'organigramme et le tableau et sont décrites de manière claire et cohérente;
  - la description de chaque étape inclut l'utilisateur, l'action, les données et le support.

- Explication au chapitre 6:
  - pourquoi la conception et les fonctionnalités techniques proposées de l'ETIAS constituent des moyens efficaces pour mettre en œuvre le règlement ETIAS;
  - si l'eu-LISA a envisagé des solutions de remplacement; et

- pourquoi les solutions retenues sont les moyens les moins intrusifs du point de vue des droits fondamentaux.

– Réexaminer l'AIPD une fois que la description générale des flux de données dans le système sera complète afin de s'assurer qu'aucun risque de niveau élevé n'a été négligé.

– Veiller à ce que, pour chaque risque spécifique recensé, la source, l'incidence et la mesure d'atténuation soient décrits.

– Énumérer *tous* les risques recensés, y compris les risques faibles.

– Réexaminer l'AIPD après l'évaluation des risques en matière de sécurité ETIAS.

Fait à Bruxelles, le *

Wojciech Rafał WIEWIÓROWSKI
(signature électronique)