



**Observations informelles du CEPD sur le projet d'AIPD soumis par [...] concernant une base de données liée à [...]
(Dossier 2021-0116)**

Contexte

L'[IUE]

[...].

La base juridique

[...]

Il existe donc une base juridique claire pour la création, par l'[IUE], d'une base de données [...] d'informations provenant des autorités [compétentes] concernant [...].

La demande

Le 29 janvier 2021, [...] a demandé au Contrôleur européen de la protection des données (le «CEPD») un avis informel sur un projet d'analyse d'impact relative à la protection des données (l'«AIPD») élaboré par ses soins (la «demande»).

L'AIPD concerne le projet de l'[IUE] consistant à créer une base de données [...] concernant [...]. L'[IUE] «s'est félicitée des échanges informels avec l'équipe de surveillance du CEPD» à cet égard.

L'approche

L'AIPD a été principalement évaluée par rapport aux principes énoncés à l'article 39 du règlement 2018/1725 (le «RPDUE»)¹ et au document du CEPD intitulé «Accountability on the ground Part II:: Data Protection Impact Assessments & Prior Consultation» (la «boîte à outils en matière de responsabilité»)². Les 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) 2016/679³ ont également été prises en compte dans la mesure où elles sont applicables par analogie.

Le précédent avis du CEPD sur la demande de consultation préalable du Parquet européen concernant les risques identifiés dans l'AIPD de son système de gestion des dossiers (l'«avis du CEPD sur l'AIPD du Parquet européen»)⁴ a servi de document d'orientation supplémentaire dans

¹ <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32018R1725>

² https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf

³ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

⁴ https://edps.europa.eu/sites/default/files/publication/20-10-01_prior_consultation_opinion_eppo_dpia_cms_2020-0568_21p_fr.pdf

le cadre de cette analyse.

Analyse de l'AIPD

Nous nous félicitons d'emblée que l'AIPD suive la structure du modèle de rapport d'AIPD prévu dans la boîte à outils en matière de responsabilité⁵. Nous analyserons chacun des éléments de l'AIPD pour vérifier s'ils fournissent les informations requises par le RPDUE et précisées dans la boîte à outils en matière de responsabilité. Nos principales recommandations et suggestions d'amélioration sont soulignées dans les observations formulées ci-dessous.

1. Nom du projet: Le titre du projet met l'accent sur l'objet du traitement. Cependant, il serait plus lisible si l'[IUE] avait recours à une formulation un peu plus descriptive (par exemple, «*La création d'une base de données [...] sur [...]... conformément à*»). De même, avant d'utiliser un acronyme dans tout le texte, nous suggérons d'en expliquer la signification (par exemple, en ajoutant [...]).

2. Validation/approbation: La liste définit la chaîne d'approbation. Toutefois, elle n'explique pas qui est chargé de l'approbation finale de l'AIPD. S'il est fait mention de l'étape où le «*responsable délégué du traitement donne son approbation*», l'étape suivante semble être celle où le «*responsable délégué du traitement rend compte au DE*», lequel est, selon toute vraisemblance, le directeur exécutif de l'[IUE]. Il apparaît que l'approbation du DE, ou tout au moins la prise en compte par celui-ci de l'AIPD approuvée par un responsable délégué du traitement, est absente. En résumé, nous recommandons que l'aval du directeur exécutif (c'est-à-dire le niveau de direction le plus élevé) en faveur de l'AIPD soit clairement prévu dans l'analyse elle-même.

3. Révision: Le texte donne des informations sur l'état actuel de l'AIPD. Une AIPD devrait également comporter des informations sur le cycle de révision. Conformément à la boîte à outils en matière de responsabilité, la durée du cycle de révision devrait être déterminée en fonction des risques présentés par l'opération de traitement. Par défaut, le CEPD recommande un cycle de révision de deux ans, avec une révision extraordinaire en cas de changements importants dans les opérations de traitement⁶. Il est donc recommandé que l'[IUE] envisage un cycle de révision approprié et qu'elle y fasse référence dans l'AIPD.

4. Résumé: L'[IUE] donne une bonne vue d'ensemble de l'opération de traitement, des principaux risques et des mesures prises pour y remédier, tels qu'ils figurent actuellement dans l'AIPD (voir point 9.f de l'AIPD). .. En outre, il convient de noter que l'[IUE] envisage la nécessité de conclure un accord de responsabilité conjointe du traitement avec les autorités [compétentes], conformément aux lignes directrices applicables du CEPD⁷. Nous nous réjouissons de la conclusion d'un tel accord. Nous ne doutons pas que, le moment venu, l'[IUE] définira les obligations et les responsabilités pertinentes dans cet accord avec un niveau de détail approprié.

5. Raisons de cette AIPD: L'[IUE] explique la nécessité de l'AIPD sur la base d'arguments qui sont conformes à l'article 39 du RPDUE et aux éléments figurant dans la liste des critères permettant d'évaluer si les opérations de traitement sont susceptibles d'entraîner des risques élevés au regard du document du CEPD intitulé «Accountability on

⁵ Voir annexe 3 de la boîte à outils en matière de responsabilité.

⁶ Voir section 3.8 de la boîte à outils en matière de responsabilité.

⁷ Lignes directrices du CEPD sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement dans le cadre du règlement (UE) 2018/1725:

[https://edps.europa.eu/sites/edp/files/publication/19-11-](https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_fr.pdf)

[07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_fr.pdf)

the ground Part I: Records, Registers and when to do Data Protection Impact Assessments⁸». L'[IUE] fait en outre explicitement référence à la décision du CEPD du 16 juillet 2019 sur les listes d'AIPD publiées en vertu de l'article 39, paragraphes 4 et 5, du règlement (UE) 2018/1725⁹. En résumé, comme l'indique le modèle, l'[IUE] utilise une liste positive qu'elle complète aussi par une brève explication des résultats. Cette approche est satisfaisante.

6. Principaux acteurs concernés: La boîte à outils en matière de responsabilité suggère ici de fournir une vue d'ensemble de «*qui est intervenu, quand et sur quelle partie*». La description fournie n'est pas incompatible avec cette suggestion. Cependant, pour l'instant, elle est évidemment limitée du fait que l'AIPD est encore un projet et qu'elle n'a pas été finalisée. En d'autres termes, l'[IUE] devrait veiller à compléter les informations pertinentes au fur et à mesure de l'avancement du projet.

7. Description du traitement¹⁰: L'AIPD suit le modèle. Nous recommandons néanmoins à l'[IUE] d'inclure ici une explication plus détaillée de la base juridique, notamment en décrivant précisément la portée des dispositions applicables, de manière à ce que l'AIPD soit un document autonome, qui puisse être compris par le lecteur sans avoir à recourir à d'autres informations.

(a) L'AIPD comporte un **diagramme de flux de données du processus (organigramme)**, expliquant l'interaction des différentes parties prenantes [compétentes] avec la base de données;

L'AIPD explique également i) **les sources des données**. Il serait toutefois utile au lecteur que l'[IUE] identifie clairement (et pas seulement à l'aide d'acronymes) les autorités compétentes et ajoute des notes de bas de page citant les dispositions juridiques pertinentes qui sont déjà mentionnées dans le texte (en particulier [...]);

L'AIPD recense en outre ii) **le type de données collectées**. Nous recommandons ici d'inclure une brève explication de certaines notions, ne serait-ce que dans des notes de bas de page [...]

L'AIPD explique ensuite iii) **ce qui est fait avec les données**, à savoir leur collecte, leur analyse, leur transmission aux autorités [compétentes] et leur utilisation par l'[IUE] aux fins de [...]. Ces explications semblent être satisfaisantes. Toutefois, nous recommandons à l'[IUE] d'expliquer plus avant quels outils analytiques de tiers l'[IUE] peut utiliser et quels sont les rôles et responsabilités de ces tiers dans le traitement lui-même.

L'AIPD explique également iv) **où et pendant combien de temps les données sont conservées**. La période de conservation proposée est de 10 ans. L'[IUE] explique qu'elle peut décider, au cas par cas, d'effacer les données avant l'expiration de cette période. Nous en déduisons donc que l'action normale qui est appliquée aux données conservées après l'expiration de cette période de 10 ans est l'effacement. Il serait néanmoins utile de le préciser

⁸ Voir le modèle d'évaluation des seuils de l'annexe 1, page 29:

https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf

⁹ Voir la liste positive de l'annexe 2 à la page 7:

https://edps.europa.eu/sites/edp/files/publication/19-07-16_edps_dpia_list_en.pdf

¹⁰ Article 39, paragraphe 7, point a), du RPDUE: «L'analyse contient au moins [...] une description systématique des opérations de traitement envisagées et des finalités du traitement [...]»

dans le texte de l'AIPD. Il serait également judicieux que l'[IUE] explique de manière plus précise comment est effectuée l'évaluation régulière de la nécessité de conserver certaines données sous une forme identifiable.

De même, l'[IUE] reconnaît que la période de conservation normale qui est fixée dans [...] est de cinq ans, mais que celle-ci peut être prolongée de cinq années supplémentaires dans certaines conditions [...]. À cet égard, l'[IUE] fait valoir que les périodes de conservation varient entre États membres et rappelle que la question de la conservation a déjà été traitée dans un cas similaire par le CEPD dans un avis [...] rendu dans le cadre d'un contrôle préalable. [...] l'[IUE] est également prête à réévaluer et à adapter la période de conservation si celle-ci s'avérait excessive ou insuffisante. En l'espèce, il convient donc de recommander à l'[IUE], dans les mêmes termes que dans l'avis du CEPD [...], de procéder à une évaluation de la nécessité de la période de conservation de 10 ans au terme des 10 premières années de pratique [...]. À partir de cette évaluation, l'[IUE] devrait être en mesure de démontrer si cette période de conservation plus longue est effectivement nécessaire.

Enfin, l'[IUE] précise v) **à qui et sur quelle base elle transfère les données**: l'AIPD énumère les autorités [compétentes] auxquelles elle peut transférer les données. Bien que ces précisions paraissent, en principe, satisfaisantes, on pourrait faire valoir que des détails supplémentaires devraient être fournis, à savoir les références exactes, si possible, aux protocoles et aux mémorandums d'accord mentionnés.

(b) Description détaillée des finalités du traitement: La boîte à outils en matière de responsabilité suggère que l'[IUE] explique le processus étape par étape, en faisant la distinction entre les finalités lorsque cela est nécessaire. L'[IUE] semble fournir des informations qui sont probablement satisfaisantes compte tenu du fait que le projet vient tout juste de démarrer.

(c) Description des interactions avec d'autres processus: L'explication fournie à cet égard paraît satisfaisante. Il semblerait néanmoins utile de préciser comment les données peuvent être alimentées à partir de bases de données ou de plateformes déjà contrôlées par l'[IUE]. Tout d'abord, une analyse juridique plus complète de la compatibilité des finalités devrait être effectuée de façon à renforcer le principe de responsabilité. Ensuite, une explication technique et organisationnelle est nécessaire afin de mieux comprendre les éventuels risques en jeu.

(d) Description de l'infrastructure de soutien: Celle-ci n'a pas encore été définie. Une description précise de l'infrastructure, avec un accent particulier sur la fonction de partage des données, sera très importante pour évaluer le respect des exigences légales et les éventuels risques découlant de l'application. En outre, une évaluation approfondie des risques liés à la sécurité de l'information devrait être menée à bien, afin de démontrer le caractère approprié des mesures techniques et organisationnelles relatives à la sécurité des données à caractère personnel et des systèmes informatiques permettant de les traiter, en conformité avec l'article 4, paragraphe 1, point f), et l'article 33 du RPDUE et avec la boîte à outils en matière de responsabilité.

8. Nécessité et proportionnalité¹¹: Ce point est mal numéroté: il devrait constituer un point à part entière (8) et non une sous-catégorie supplémentaire (e) des descriptions figurant au point 7) du projet d'AIPD. L'[IUE] semble expliquer suffisamment a) pourquoi les données à caractère personnel sont nécessaires pour remplir le mandat qui lui a été confié. Toutefois, en ce qui concerne le point b), la proportionnalité, c'est-à-dire la question de savoir si les données nécessaires respectent également les limites de ce qui est proportionné pour réaliser les tâches, l'[IUE] se réfère essentiellement à la pertinence et à l'exactitude des données utilisées ainsi qu'aux garanties mises en place pour s'assurer qu'elles sont traitées correctement. Conformément à l'article 39, paragraphe 7, point b), du règlement, la boîte à outils en matière de responsabilité prévoit l'obligation de comparer les avantages du traitement et les risques qu'il présente au regard des droits fondamentaux. Nous recommandons à l'[IUE] d'expliquer clairement pourquoi le traitement, tel qu'il est envisagé, est proportionné pour permettre à l'[IUE] de remplir son mandat.

9. Analyse des risques et mise en place de contrôles pour les risques identifiés¹²: Ce point est mal numéroté: il devrait constituer un point à part entière (9) et non une sous-catégorie supplémentaire (f) des descriptions figurant au point 7) du projet d'AIPD.

La boîte à outils en matière de responsabilité suggère de se concentrer d'abord sur les risques pour les droits et libertés des personnes concernées, puis sur les risques de conformité pour l'institution, et ce non seulement dans le cas où quelque chose ne se passerait pas comme prévu, mais aussi dans le cas où tous les processus fonctionneraient normalement.

Le projet d'AIPD semble suivre précisément ce plan et l'analyse semble être en bonne voie, mais elle nécessitera des avancées supplémentaires en ce qui concerne certaines caractéristiques spécifiques qui restent à définir. En particulier, la conception et l'efficacité des contrôles et des mesures d'atténuation liés aux risques n^{os} 12 et 13 devraient être mieux expliquées afin d'atteindre le niveau de gravité et de vraisemblance résiduelle souhaité.

10. Observations des personnes concernées (le cas échéant): Compte tenu de la portée de l'opération de traitement qui fait l'objet de l'AIPD, il semble raisonnable de ne pas envisager de consultation des personnes concernées.

11. Observations du DPD: Informations susceptibles d'être mises à jour au fur et à mesure de l'évolution des travaux sur l'AIPD.

Résumé des recommandations et des suggestions d'amélioration du CEPD

Recommandations:

- Expliquer clairement qui approuve l'AIPD;
- Prévoir un cycle de révision de l'AIPD approprié;
- Mieux décrire les dispositions juridiques applicables, notamment en incluant les citations exactes;
- S'assurer que les futurs accords de responsabilité conjointe du traitement prévoient les informations nécessaires pour comprendre les obligations et responsabilités des responsables

¹¹ Article 39, paragraphe 7, point b), du RPDUE: «L'analyse contient au moins [...] une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités [...]»

¹² Article 39, paragraphe 7, point c), du RPDUE: «L'analyse contient au moins [...] une évaluation des risques pour les droits et libertés des personnes concernées [...]» et article 39, paragraphe 7, point d), du RPDUE: «L'analyse contient au moins [...] les mesures envisagées pour faire face aux risques, y compris les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.»

conjoint du traitement;

- Mettre à jour les informations relatives aux principaux acteurs concernés au fur et à mesure de l'évolution du projet;
- Identifier clairement les sources des données et les citations des dispositions juridiques importantes mentionnées;
- Expliquer les notions utilisées dans la partie relative au type de données collectées, telles que [...];
- Expliquer quels sont les outils analytiques de tiers qui peuvent être utilisés, et préciser quels sont les rôles et responsabilités de ces mêmes tiers;
- Expliquer clairement ce qu'il advient des données après l'expiration de la période de conservation;
- Mieux expliquer comment est effectuée l'évaluation régulière de la nécessité de conserver certaines données sous une forme identifiable;
- Être en mesure de démontrer, chaque fois qu'il est possible pour l'[IUE] de procéder à une évaluation de la nécessité de la période de conservation de 10 ans, si une période de conservation aussi longue est effectivement nécessaire;
- Inclure si possible des références exactes aux protocoles et aux mémorandums d'accord sur les transferts de données;
- Préciser comment les données peuvent être alimentées à partir de bases de données ou de plateformes déjà contrôlées par l'[IUE];
- Décrire l'infrastructure en mettant l'accent en particulier sur la fonction de partage des données;
- Faire également référence à l'évaluation approfondie qui a été effectuée en ce qui concerne les risques liés à la sécurité de l'information;
- Consacrer un point distinct (8) à la nécessité et à la proportionnalité; ajouter une déclaration claire expliquant pourquoi l'[IUE] considère que les données sont proportionnées; et
- Consacrer un point distinct (9) à l'analyse des risques et à la mise en place de contrôles pour les risques identifiés; mieux expliquer la conception et l'efficacité des contrôles et des mesures d'atténuation liés aux risques n^{os} 12 et 13.

Autres suggestions d'amélioration

- Envisager d'utiliser un titre plus descriptif et expliquer la signification des acronymes; et
- Une fois l'AIPD terminée, envisager de la publier (ou au moins un résumé) sur le site web de l'IUE.

26 février 2021