Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 41/2025 du 12 juin 2025

Objet: Demande d'avis concernant un projet de Traité bilatéral relatif à l'entraide judiciaire en matière pénale entre le Royaume de Belgique et la République du Kosovo (CO-A-2025-026)

Mots-clés : Transferts de données hors UE – Traité international – Coopération judiciaire en matière pénale – Kosovo – Directive 2016/680 - Titre II LTD

Version originale

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier ses articles 23 et 26 (ci-après « LCA ») ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD ») ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD ») ;

Vu la demande d'avis de Madame Annelies Verlinden, Ministre de la Justice (ci-après « la demanderesse »), reçue le 28 mars 2025 ;

Vu le courriel de l'Organe de contrôle de l'information policière du 17 avril 2025, indiquant qu'il ne rendrait pas d'avis au sujet de ce projet ;

Émet, le 12 juin 2025, l'avis suivant :

Pour les textes normatifs émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale et de la Commission communautaire commune, les avis sont en principe disponibles en français et en néerlandais sur le site Internet de l'Autorité. La « Version originale » est la version qui a été validée.

I. OBJET DE LA DEMANDE D'AVIS

1. La demanderesse a sollicité l'avis de l'Autorité concernant l'art. 7 du projet de Traité relatif à l'entraide judiciaire en matière pénale (ci-après "le Projet").

2. A l'occasion de l'introduction de la demande d'avis, le fonctionnaire délégué a précisé que la demande était introduite préalablement à la signature du projet de Traité par le Ministre compétent. L'Autorité en prend acte et[1] reconnait qu'en matière de traités internationaux impliquant des traitements de données à caractère personnel, la consultation de l'Autorité préalablement à la signature dudit traité est davantage de nature à permettre une protection effective des droits des personnes concernées[2]. Par conséquent, sans préjudice de la nécessité de soumettre le projet de loi d'assentiment à l'avis de l'Autorité, l'Autorité accepte (lorsqu'elle est dans les conditions matérielles pour le faire) de se prononcer sur un projet de traité international susceptible de lier la Belgique, préalablement à sa signature par les Parties.

3. Le Projet entend permettre aux Parties de se prêter mutuellement assistance judiciaire dans le cadre d'une enquête ou d'une procédure pénale et plus spécifiquement dans l'exécution d'actes d'enquête (interrogatoires, perquisitions, saisies, demandes de renseignements), l'exécution d'actes de procédure liés à une procédure pénale (significations), l'échange de casiers judiciaires et l'échange spontané d'informations[3].

4. Le formulaire accompagnant la demande d'avis précise que, sous certaines conditions, la coopération entre le Kosovo et la Belgique, dans le cadre de l'entraide judiciaire en matière pénale, est déjà possible sur la base du traité de [1971][4] relatif à l'entraide judiciaire et à l'extradition entre la République socialiste fédérative de Yougoslavie et le Royaume de Belgique pour ce qui concerne l'entraide judiciaire, des traités multilatéraux des Nations-Unies et de la réciprocité[5].

---

[1] Nonobstant l'art. 46, §1er du Règlement d'Ordre Intérieur de l'Autorité, qui dispose que « *le* [SAA] *examine uniquement les demandes d'avis sur les projets normatifs* (…) *dans leur stade final de rédaction* ».

[2] En ce sens, voy. l'avis 119/2022 du 15 juin 2022, point 7 ; voy. également le point 48 des lignes directrices 01/2023 de l'EDPB relatives à l'art. 37 de la directive police-justice, qui dispose que « *in any case, Member States are in all circumstances encouraged to* ***engage with the national SA before the conclusion of the legally binding agreement*** *to allow for a timely, constructive and meaningful exchange in order to verify that the appropriate safeguards are in place, in line with the requirements of Article 37(1)(a) LED. In that context, the SA should be provided with all relevant information regarding the third country or international organisations, including the respective assessments made, when available*".

[3] Art. 10 et sv. du projet.

[4] Le formulaire accompagnant la demande d'avis mentionne « 1970 ».

[5] A noter, en ce qui concerne les données policières, que le Kosovo n'est pas membre d'Interpol (voy. https://www.kosovo-online.com/en/news/politics/dacic-it-serbias-interest-kosovo-does-not-join-interpol-13-5-2025)

5. Le contexte répressif entourant les traitements de données à caractère personnel envisagés emporte l'application du Chapitre V de la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil* (ci-après "Directive police-justice"), telle que transposée en droit belge par le Chapitre V du Titre 2 de la LTD.

6. A ce jour, le Kosovo n'a pas fait l'objet d'une reconnaissance de protection adéquate par la Commission européenne[6]. Il ne peut donc se voir transférer des données à caractère personnel que[7] s'il assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet, comme le prévoit l'article 66, §1er LTD.

7. L'Autorité vérifie ci-après si le Projet répond aux conditions pour être considéré comme un instrument juridiquement contraignant fournissant des garanties appropriées pour la protection des données à caractère personnel pouvant faire l'objet d'un transfert vers les pays tiers en dehors de l'Union européenne, conformément à l'article 68, § 1er, 1° de la LTD[8].

8. A noter que le Kosovo – qui a déclaré unilatéralement son indépendance en février 2008 - est un candidat potentiel à l'adhésion à l'Union Européenne. L'art. 36 de la Constitution du Kosovo protège la vie privée et garantit la protection des données à caractère personnel[9]. Une législation spécifique relative à la protection des données (qui « *transpose* » les dispositions du RGPD[10]) y est applicable depuis le 13 février 2019[11] et le Kosovo dispose d'une autorité de protection des données indépendante[12]. Cette autorité siège par ailleurs à l'EDPB en qualité d'observateur[13].

---

[6] L'art. 36 de la Directive (UE) 2016/680 du Parlement et du Conseil du 27 avril 2016 confère à la Commission le pouvoir de constater par voie de décision qu'un pays tiers assure un niveau de protection adéquat (voy. également l'art. 67 LTD et, bien entendu l'art. 45.1. du RGPD).

[7] Outre, en matière répressive, la nécessité « *aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* » (art. 27 LTD).

[8] Ainsi qu'à l'art. 37 de la directive police-justice précitée.

[9] Voy. https://qzk.rks-gov.net/ActDetail.aspx?Ac-tID=3702

[10] Cependant, les dispositions applicables aux procédures judiciaires et au casier judiciaire figurent principalement dans la loi No.05/L-053 *ON SPECIALIST CHAMBERS AND SPECIALIST PROSECUTOR'S OFFICE* et la loi No. 08/L-194 *ON CENTRAL CRIMINAL RECORDS SYSTEM OF KOSOVO*

[11] Voy. https://www.dlapiperdataprotection.com/?t=law&c=XK

[12] Qui ne comptait que 19 employés en 2019 (voy. Hajdari, P., Nimani, P., Hebibi, D., & Maloku, A. (2022). Implementation of the right to privacy in the Republic of Kosovo. *International Journal of Health Sciences*, *6*(S8), p. 5037 (https://doi.org/10.53730/ijhs.v6nS8.13358) et 32 en 2024 (voy. le rapport annuel 2024 de l'AIP du Kosovo, p. 15)

[13] Voy. https://idp.al/en/2024/10/11/information-and-privacy-agency-of-kosovo-member-of-the-european-data-protection-board/

9. L'Autorité en profite pour signaler qu'à ce jour, le législateur belge reste en défaut d'identifier l'autorité compétente pour contrôler les traitements de données à caractère personnel réalisés par les cours et tribunaux, ainsi que par le ministère public dans le cadre de leur fonction juridictionnelle.

10. Enfin, à toutes fins utiles, l'Autorité signale qu'un autre Etat de l'Union (la Suède) a récemment signé un traité relatif à l'extradition, un traité relatif à l'assistance mutuelle en matière répressive et un traité relatif au transfert de personnes condamnées avec le Kosovo[14].

II. EXAMEN DU PROJET

11. L' art. 7 en projet porte sur la « *protection des données à caractère personnel* »[15]. A l'occasion de l'introduction de la demande d'avis, le fonctionnaire délégué a demandé à l'Autorité de limiter son examen à cette seule disposition. Toutefois, comme il sera davantage expliqué *infra*, d'autres dispositions du Projet impliquent manifestement des traitements de données à caractère personnel.

12. L'Autorité rappelle que l'EDPB a adopté des lignes directrices[16] relatives à l'art. 37 de la directive police-justice (article transposé à l'art. 68 LTD), destinées – notamment – à guider les Etats membres, lors de la négociation de nouveaux instruments internationaux. L'Autorité développe ci-dessous les principaux enseignements de ces lignes directrices, tout en y renvoyant la demanderesse pour tout ce qui ne figure pas dans le présent avis.

---

[14] Voy. https://kosovapress.com/kosova-e-suedia-finalizojne-tri-marreveshje-per-bashkepunim-juridik

[15] Et est libellé comme suit :

*1. Les Parties veillent à ce que les données à caractère personnel soient transférées d'une Partie à l'autre, et qu'elles ne soient utilisées qu'**aux fins de l'exécution d'une demande**, conformément au présent Traité. Aucune donnée à caractère personnel ne sera utilisée à d'autres fins, ni transférée à un pays tiers sans l'accord préalable de la Partie qui a transféré les données.*

*2. Les Parties garantissent l'**exactitude** des données à caractère personnel transférées en vertu du présent Traité et veillent à ce que des mesures appropriées soient prises pour **protéger** les données transmises contre la destruction accidentelle ou non autorisée ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés.*

*3. Les données à caractère personnel transférées sont conservées pendant une **durée n'excédant pas celle nécessaire aux finalités** pour lesquelles elles sont traitées, conformément au présent Traité. Les Parties **se consultent sur la nécessité de rectifier** des données inexactes, incomplètes ou non fiables ou sur le désir ou la nécessité d'effacer des données à caractère personnel ou de limiter leur utilisation.*

*4. Les Parties veillent à ce que les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques ou les données à caractère personnel concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne fassent l'objet de **garanties appropriées**.*

*5. La personne condamnée **peut recevoir des informations** sur les catégories de données transférées et la finalité du transfert de données.*

*6. La personne condamnée a le **droit de déposer une plainte** lorsqu'elle estime que ses droits concernant le traitement de ses données à caractère personnel sur la base du présent Traité ont été violés.*

[16] Lignes directrices 01/2023, adoptées le 19 juin 2024

1. Mentions dans l'exposé des motifs de la loi d'assentiment

13. L'Autorité, tout comme l'EDPB, estime que l'exposé des motifs de la loi d'assentiment doit préciser sur quels éléments les négociateurs belges se sont basés pour **évaluer l'état de la situation en matière de droits humains et de respect de l'état de droit** dans le pays destinataire[17].

2. Mise en évidence des dispositions applicables aux données à caractère personnel

14. L'art. 7 en projet porte spécifiquement sur la protection des données à caractère personnel, ce que l'Autorité accueille favorablement.

15. Cependant, les mesures dont il est question aux art. 11 et sv. en projet (production de documents, registres, informations, casiers judiciaires, etc.) sont également susceptibles d'impliquer des traitements de données à caractère personnel.

16. Sur ce point, l'EDPB estime que lorsque des dispositions ne figurant pas dans le chapitre « *protection des données à caractère personnel* » impliquent le traitement d' « *informations* », il est essentiel d'indiquer clairement si ces informations sont susceptibles de comporter des données à caractère personnel et, dans l'affirmative, de les **distinguer des dispositions portant sur des informations autres que des données à caractère personnel**[18].

17. L'Autorité estime qu'il convient de revoir les dispositions du Projet à la lumière de ce qui précède.

3. Effectivité de la protection des données

18. L'adoption d'une loi relative à la protection des données par le pays tiers est un élément essentiel, mais qui doit s'accompagner d'une analyse du caractère **effectif de son implémentation**[19]. Une telle analyse doit également permettre de démontrer que les exceptions dont les autorités répressives peuvent se prévaloir sont bien limitées à ce qui est proportionné et nécessaire[20].

---

[17] *Ibidem*, point 44

[18] *Ibidem*, point 49

[19] Voy. par exemple l'analyse réalisée par la plateforme Civikos, pp. 28 et sv. (https://civikos.net/wp-content/uploads/2023/12/Raporti-NED-eng_compressed.pdf)

[20] *Ibidem*, point 45 ; A noter que l'AIP du Kosovo et la police kosovare ont signé un Memorandum of Understanding (voy. https://aip.rks-gov.net/en/the-information-and-privacy-agency-signed-a-memorandum-of-understanding-on-support-and-cooperation-with-the-kosovo-police/)

19. Par conséquent, l'Autorité estime que l'exposé des motifs de la loi d'assentiment doit mentionner les rapports consultés et justifier du caractère nécessaire et proportionné de chacune des exceptions dont les autorités compétentes peuvent se prévaloir.

4. Points d'attention lors de la reformulation des dispositions relatives à la protection des données

20. Les concepts doivent être compris de la même manière par les Parties, de sorte qu'il ne soit pas possible de les **interpréter** d'une manière ne correspondant pas aux principes généraux et garanties prévalant dans l'Union européenne[21], tels qu'appliqués à l'entraide judiciaire en matière pénale. A cette égard, l'Autorité estime que l'art. 7 en projet présente de sérieuses lacunes, notamment en ce qui concerne les finalités des traitements de données (7.1.), les mesures de protection des données et les garanties « appropriées » (7.2. et 7.4.), la durée de conservation « nécessaire » (7.3.), la condition de consultation sur la nécessité de rectifier (7.3.), la « possibilité » de recevoir des informations (7.5.) et le « droit » de déposer une plainte (7.6.).

21. Une bonne pratique consiste à **détailler** les dispositions relatives notamment aux mesures spécifiques de protection des données, aux catégories de personnes concernées, aux catégories de données, aux canaux de communication et aux procédures d'urgence, dans une **annexe** faisant partie intégrante de la convention[22].

22. Il convient par ailleurs d'indiquer expressément que les autorités des Parties impliquées dans les traitements de données à caractère personnel visés par le traité (c'est-à-dire pas uniquement l'autorité centrale désignée), sont **exclusivement des autorités compétentes** aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, au sens de l'art. 1.1. de la directive police-justice[23].

23. Les **références à d'autres cadres normatifs**, qu'ils soient nationaux (telles que celles figurant à l'art. 5.1. du Projet) ou internationaux, ne peuvent être des références générales, mais doivent au contraire identifier des dispositions spécifiques, comportant des garanties spécifiques et uniquement à condition d'être en mesure de démontrer que l'analyse de la législation du pays tiers

---

[21] *Ibidem*, points 46, 53 et 54; Sur cette question, voy. également les recommandations 01/2021 de l'EDPB sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, adoptées le 2 février 2021

[22] *Ibidem*, point 50

[23] *Ibidem*, points 52 et 59, iii; L'énumération des autorités compétentes pour chacune des Parties peut figurer dans une annexe ou une déclaration ultérieure.

ne permet pas de craindre que le niveau de protection requis par la directive police-justice s'en trouve amoindri[24].

24. Les **dispositions du traité** doivent en outre[25] (1) déterminer son champ d'application et déterminer quelles catégories de données sont concernées, (2) soumettre les traitements de données ultérieurs à des conditions, (3) assortir l'obligation de respect du principe d'exactitude des données d'obligations concrètes, (4) prévoir une durée de conservation maximale des données, (5) imposer des mesures de sécurité des données, (6) imposer une obligation de confidentialité à tout membre du personnel traitant des données à caractère personnel et imposer des obligations précises en cas de *data breach*, (7) identifier les autorités auprès desquelles les personnes concernées peuvent exercer leurs droits, (8) limiter les dérogations aux droits des personnes concernées, (9) prévoir que les conditions auxquelles la convention soumet le traitement des données transférées restent applicables à ces données nonobstant la résiliation de la convention et imposer une obligation d'information en cas de modification législative susceptible d'affecter significativement la convention.

4.1. Détermination du champ d'application du traité et détermination des catégories de données concernées

25. La détermination du champ d'application du traité peut se faire via une liste d'infractions ou de critères basés sur des taux de peines.

26. En ce qui concerne la détermination des catégories de données, il y a tout d'abord lieu d'y inclure les données à caractère personnel relatives aux membres du personnel des autorités compétentes (dont le traitement est nécessaire et proportionné)[26].

27. Pour les données relatives à des infractions (en ce compris les données figurant dans les casiers judiciaires), en raison de leur caractère sensible, il convient de viser les données susceptibles d'être transférées et non uniquement les catégories auxquelles elles appartiennent. En outre, il convient de préciser que ces données ne peuvent être traitées que pour autant que cela soit nécessaire et de prévoir expressément des garanties supplémentaires.

28. L'Autorité estime enfin qu'il convient d'exclure tout profilage de la personne concernée, sur base d'un traitement de données appartenant à des catégories particulières de données susceptibles d'engendrer une discrimination.

---

[24] *Ibidem*, point 55

[25] Ibidem, point 59

[26] Par exemple leurs données d'identification et/ou de contact.

4.2. Soumettre les traitements ultérieurs à des conditions

29. L'art. 7.1. du Projet soumet les traitements ultérieurs de données à l'accord préalable de la Partie transférante.

30. L'Autorité estime cependant qu'il serait souhaitable d'aller plus loin en exigeant une demande motivée de la Partie demanderesse, en plus de l'accord préalable et écrit de la Partie à qui le transfert des données est demandé.

31. Par ailleurs, l'Autorité estime que, sauf à interdire purement et simplement les traitements ultérieurs des données transférées, l'art. 7.1. gagnerait à être reformulé en précisant qu'un tel traitement ultérieur (en ce compris la communication à d'autres autorités de la Partie réceptrice[27]) ne peut se concevoir que pour une finalité compatible avec la finalité du transfert et relevant elle aussi du champ d'application de la directive police-justice (sauf urgence motivée par la prévention d'une menace grave et immédiate à la sécurité publique).

32. Le cas échéant, il conviendra également de préciser que « *les données à caractère personnel traitées doivent être pertinentes, adéquates et limitées à ce qui est nécessaire pour atteindre la finalité du transfert et du traitement ultérieur* ».

4.3. Principe d'exactitude

33. L'art. 7.2. du Projet dispose que les Parties garantissent l'exactitude des données transférées.

34. A cet égard, l'Autorité estime (tout comme l'EDPB), qu'il convient d'assortir l'obligation de respect du principe d'exactitude des données d'obligations concrètes, telles que des obligations de notification et de rectification ou encore d'effacement.

4.4. Durée de conservation maximale

35. L'art. 7.3. du projet dispose que « *les données à caractère personnel transférées sont conservées pendant une* ***durée n'excédant pas celle nécessaire aux finalités*** *pour lesquelles elles sont traitées, conformément au présent Traité* ». Cette formulation n'est pas d'une précision suffisante

[27] Un tel accès devrait être interdit par principe, sauf accord express (le cas échéant assorti de conditions additionnelles par rapport à celles figurant dans le traité) donné dans un délai à déterminer suivant la communication d'informations écrites identifiant l'autorité compétente réceptrice (relevant elle aussi de la directive police-justice), mentionnant les motifs de la demande d'accès et les catégories de données concernées.

pour permettre à une personne concernée d'apprécier si c'est à bon droit que les données sont toujours susceptible d'être traitées.

36. Il convient donc de reformuler cette disposition, en indiquant – par catégorie de données et par finalité –la durée de conservation maximale des données et le point de départ de sa computation.

37. A noter qu'une bonne pratique consiste à appliquer des règles d'accès plus ou moins restreints en fonction des durées de conservation (en d'autres termes, de prévoir un accès large durant X années, suivi d'un accès limité à une certaine catégorie de membres du personnel durant les X années suivantes et enfin un accès limité aux finalités d'archivages après les dernières années de conservation). Bien entendu, le caractère nécessaire et proportionné de ces durées de conservation et des accès correspondants devra être dûment justifié dans l'exposé des motifs du projet de loi d'assentiment.

4.5. Mesures de sécurité

38. L'art. 7.2. du Projet évoque des « *mesures appropriées* » pour protéger les données « *transmise*s ».

39. Comme indiqué *supra*, l'Autorité estime qu'il y a lieu de mentionner des mesures concrètes, telles que le chiffrement, un contrôle des accès basé sur le principe du « *need-to-know* », un audit régulier des journaux, etc…

40. En outre, il y a lieu de préciser que ces mesures doivent être appliquées tant au transfert des données qu'à leur traitement par leur destinataire.

41. L'Autorité constate par ailleurs que l'art. 2.2. du Projet prévoit la transmission des communications « *par des **moyens électroniques** ou tout autre moyen permettant d'apporter une preuve écrite* (…) ».

42. A cet égard, l'Autorité considère que la communication de données à caractère personnel sensibles par courriel est en principe à proscrire[28]. Or, en l'espèce, il est question de telles données dès lors que sont notamment en cause des données relatives à des infractions visées à l'article 10 du RGPD.

[28] Voir en ce sens l'avis de l'Autorité n° 223/2021 du 3 décembre 2021 concernant un projet d'arrêté portant modification de l'arrêté du Collège réuni de la COCOM du 10 mars 2016 portant exécution de l'ordonnance du 21 juin 2012 relative à la promotion de la santé dans la pratique du sport, à l'interdiction du dopage et à sa prévention, considérant n° 17, et l'avis de l'Autorité n° 14/2022 du 21 janvier 2022 concernant un projet d'arrêté du Gouvernement wallon déterminant la composition et le fonctionnement du Comité wallon pour la protection des animaux d'expérience, considérants nos 21 à 22.

43. En outre, sauf à utiliser un service de messagerie électronique (sécurisé) propre au responsable du traitement (et n'impliquant donc ni sous-traitance, ni co-responsabilité de traitement), la communication électronique impliquera très probablement un transfert de données à caractère personnel vers un pays tiers et vers un responsable du traitement autre qu'une autorité compétente visée par l'instrument international en projet[29]. Il convient donc d'imposer la mise en place de procédures et d'un canal de communication offrant un niveau de sécurité adapté à la nature des données transmises.

44. En l'occurrence, les données relatives à des infractions exigent un haut niveau de confidentialité. Parallèlement aux mesures générales listées dans les normes relatives à la sécurité de l'information (par exemple, NIST CSF, ISO 27001, 27002, 27701), on pourra plus spécifiquement, afin d'atteindre un niveau correct de confidentialité dans la communication électronique, mettre en place des mesures concernant tant le canal de transmission que le message (et éventuelles pièces jointes) lui-même, au moyen et à titre d'exemples (non exhaustif) :

• De l'utilisation d'une plateforme d'échange en ligne présentant des standards de sécurité conformes à l'état de la technique. Sur internet, l'emploi du protocole TLS dans une version égale ou supérieure à la version 1.2 fait partie des bonnes pratiques ;
• D'un logiciel de chiffrement rendant l'information incompréhensible à toute personne ne disposant pas de l'information nécessaire au déchiffrement (la clef), tel l'outil gratuit de compression « 7-zip » où l'on choisira le standard de chiffrement AES-256. On notera la nécessité d'utiliser deux canaux de communication distincts pour l'envoi du message chiffré et de la clef de déchiffrement correspondante (par exemple : courriel puis application) ;
• Si l'on veut s'assurer que les informations n'ont pas subi d'altérations lors de la transmission, de l'utilisation d'une technique de hachage. Tout comme pour le chiffrement, on veillera à n'utiliser que des algorithmes reconnus et sûrs (ex., SHA-512 et SHA-3). La fonction de hachage doit être appliquée au texte clair et ajoutée au texte clair avant le chiffrement (pas au texte chiffré).

45. Parallèlement à ces mesures, on conseillera également, pour tout système donnant accès à des données sensibles (y compris donc celles relatives à des infractions) :

• D'imposer d'avoir recours à l'authentification à au moins deux facteurs - l'authentification auprès de la plate-forme par un nom d'utilisateur et un mot de passe n'est pas suffisante ;
• D'imposer une politique de mot de passe stricte (un mot de passe aléatoire composé de lettres d'une longueur d'au moins 17 caractères ou un mot de passe aléatoire composé de caractères alphanumériques (a-z, A-Z, 0-9,...) d'au moins 14 caractères) ;

[29] Sur cette question voy. les avis 15/2015 (cons. 18 et 19) et 04/2017 de la CPVP, prédécesseur de l'Autorité.

- D'exiger des éventuels sous-traitants et sous-sous-traitants le respect des mêmes exigences de sécurité.

46. Comme indiqué supra, ces éléments peuvent toutefois figurer dans une annexe au traité.

47. L'Autorité recommande par ailleurs d'imposer la tenue d'un registre des échanges écrits d'informations[30] et la publication périodique de statistiques (anonymisées).

4.6. Obligation de confidentialité et mesures en cas de data breach

48. L'art. 6.1. du Projet impose à la partie requise de transmettre des données, de garantir la confidentialité des faits et du contenu de la demande de transmission de données reçue « conformément à sa législation ».

49. Outre la problématique (évoquée *supra*) du renvoi général vers une norme nationale, l'Autorité estime qu'il serait préférable de prévoir qu'**il appartient à l'autorité destinataire des données d'assurer le niveau de confidentialité** (et donc d'accès) **attaché aux informations par l'autorité transférante**. Les règles détaillées peuvent également être déterminées dans une annexe, par exemple si les Parties conviennent d'appliquer les niveaux de confidentialité utilisés par Interpol[31].

50. L'Autorité constate par ailleurs que la Partie destinataire des données ne se voit imposer aucune obligation précise en cas de survenance d'une **fuite de données**. L'Autorité estime qu'il convient d'adapter le Projet sur ce point.

4.7. Autorité de contrôle

51. L'art. 7.6. du Projet dispose que « *la personne condamnée a le droit de déposer une plainte lorsqu'elle estime que ses droits concernant le traitement de ses données à caractère personnel sur la base du présent Traité ont été violés* ».

52. Le choix de ce libellé s'explique vraisemblablement par l'absence de désignation légale, dans l'ordre juridique belge, d'une autorité compétente pour contrôler les traitements de données effectués par les juridictions dans le cadre de l'exercice de leur fonction juridictionnelle. Il n'en demeure pas

[30] Et en particulier des demandes d'autorisation, des autorisations données, des notifications, etc.

[31] Voy. art. 112, p. 41 ; même si le Kosovo n'est pas membre d'Interpol.

moins qu'il convient de **préciser quelle est l'autorité** - indépendante et disposant des moyens nécessaires pour accomplir ses missions - habilitée à recevoir pareille plainte[32].

53. Toutefois, le choix de ce libellé est également susceptible de témoigner de la volonté des Parties de **prévoir des voies de recours** administratives et judiciaires. A cet égard, l'Autorité insiste pour qu'il soit veillé à ce que ces recours soient **effectifs** et qu'ils permettent, à ce titre, à toute personne concernée (en ce compris les personnes ayant quitté le territoire, incarcérées, ne maîtrisant pas la langue nationale ou ne disposant pas de moyens financiers ou de connaissances juridiques particulières) d'avoir accès à ces recours ainsi que, le cas échéant, d'être indemnisée pour le préjudice subi.

54. Une bonne pratique consiste à prévoir un **échange d'informations** (en ce compris des statistiques) entre Parties au sujet de l'exercice de ces recours.

55. L'Autorité estime également qu'il convient de veiller à ce qu'une Partie n'ait pas la possibilité d'**échapper à sa responsabilité** envers les personnes concernées en invoquant le fait qu'une autre Partie aurait communiqué des données inexactes ou non à jour.

4.8. Dérogations aux droit de la personne concernée

56. En ce qui concerne les droits des personnes concernées, l'art. 7.5. du Projet mentionne « *possibilité* » de recevoir des informations sur les catégories de données transférées et les finalités de leur transfert. En se référant à une « possibilité » plutôt qu'à un « droit », cette disposition est susceptible d'être interprétée comme conférant un pouvoir d'appréciation discrétionnaire à l'autorité compétente. En outre, ce libellé (en ce qu'il ne précise pas les obligations du responsable du traitement confronté à une demande d'exercice de ses droits par la personne concernée) ne permet pas à la personne concerné d'évaluer le caractère nécessaire et proportionné d'un éventuel refus.

57. Par conséquent, l'Autorité estime qu'il convient de revoir cette formulation en précisant clairement quelles autorités ont l'obligation de répondre à une demande d'accès et dans quelles **circonstances précises** il leur est permis de ne pas réserver une suite favorable à une telle demande.

58. Concrètement, l'Autorité estime que ces **dérogations devraient être expressément limitées** aux motifs visés à l'art. 16.4 de la directive police-justice. Le cas échéant, il pourrait être envisagé d'imposer une **restriction au transfert** des données à caractère personnel (conformément à l'art. 16 de la directive police-justice) tant que leur exactitude est à l'examen.

[32] Ou à tout le moins imposer que cette information soit publique et facilement accessible.

59. A noter qu'une bonne pratique consiste à imposer la réalisation et la publication de **statistiques** au sujet des demandes d'exercice de leurs droits par les personnes concernées.

4.9. Maintien des effets du traité et obligation d'information

60. L'Autorité recommande de prévoir que les conditions auxquelles la convention soumet le traitement des données transférées restent applicables à ces données nonobstant la résiliation de la convention. A cet égard, une bonne pratique consiste à prévoir une **durée de conservation abrégée en cas de résiliation et à interdire tout transfert ultérieur** des données.

61. Enfin, l'Autorité recommande d'imposer une obligation d'information envers l'autre Partie en cas de **modification législative** susceptible d'affecter significativement la convention[33].

5. Recours à la vidéoconférence

62. L'art. 17 du Projet encadre la possibilité de procéder à une audition par vidéoconférence « *dans la mesure du possible et dans le respect des principes fondamentaux du droit de la Partie requise* ».

63. L'Autorité rappelle qu'il convient de justifier du caractère nécessaire et proportionné de la mesure dans l'exposé des motifs de la loi d'assentiment. Si, à cette occasion, la nécessité de modifier l'art. 17 du Projet devait apparaitre, l'Autorité invite la demanderesse à prendre connaissance des observations formulées par l'Autorité dans son avis 63/2023[34] ainsi que dans l'avis 3/2023[35] de l'Institut fédéral pour la protection et la promotion des droits humains, en vue de la reformulation de cette disposition.

[33] *Op. cit.*, point 60, vii

[34] Emis le 9 mars 2023

[35] Emis le 31 janvier 2023

PAR CES MOTIFS,

L'Autorité

accueille favorablement le fait d'avoir été consultée préalablement à la signature du projet de traité par les Parties ;

est d'avis que le Projet doit être fondamentalement revu à la lumière des observations formulées ci-avant ;

rappelle que le présent avis ne dispense pas la demanderesse de soumettre le projet de loi d'assentiment accompagné du projet de traité adapté à l'Autorité, pour avis ;

attire l'attention de la demanderesse sur l'existence des lignes directrices 01/2023 de l'EDPB relatives à l'art. 37 de la directive police-justice.

Pour le Service d'Autorisation et d'Avis,
(sé.) Alexandra Jaspar, Directrice