Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la police fedpol
Domaine de direction Prévention de la criminalité et droit PCD

Loi fédérale sur le traitement des données relatives aux passagers aériens pour la lutte contre les infractions terroristes et les autres infractions pénales graves (Loi sur les données relatives aux passagers aériens, LDPa)

Rapport sur les résultats de la procédure de consultation

15 mai 2024

Table des matières

1 Objet de la consultation

Au moment de la réservation d'un billet d'avion, les entreprises de transport aérien collectent diverses données sur les passagers. Cet ensemble de données relatives aux passagers aériens, connu au niveau international sous le nom de dossier passager ou *Passenger Name Record* (PNR), comprend par exemple le nom et l'adresse des passagers, mais aussi d'autres informations relatives à leurs bagages ou aux modes de paiement. De nombreux États ont reconnu le potentiel du PNR et l'exploitent depuis des années pour lutter contre le terrorisme et les autres infractions pénales graves. La Suisse doit aussi avoir cette possibilité. La loi sur les données relatives aux passagers aériens (LDPa) constitue la base légale requise. En traitant de telles données, la Suisse s'engage pour davantage de sécurité tout en remplissant ses obligations internationales.

2 Déroulement de la procédure de consultation

Le Département fédéral de justice et police (DFJP) a mené, du 13 avril au 31 juillet 2022, une procédure de consultation relative à l'avant-projet de LDPa, conformément à l'art. 3, al. 2, de la loi du 18 mars 2005 sur la consultation (LCo)[1]. Les résultats de cette consultation sont résumés ci-après.

Cinquante-six participants à la consultation (ci-après participants) ont pris position sur la LDPa:

Cantons	25 (AG, AI, AR, BE, BL, BS, FR, GE, GL, GR, JU, LU, NE, NW, OW, SG, SH, SO, SZ, TG, TI, VD, VS, ZG, ZH)
Partis	6 (Le Centre, PLR, PS, UDC, Les Verts, Parti pirate)
Associations faîtières des communes, des villes et de l'économie	2 (economiesuisse, USS)
Autres organisations et institutions intéressées	14 (AEROSUISSE, AlgorithmWatch, ASA, CCDJP, CCPCS, CPS, easyjet, FSA, FST, privatim, Société numérique, SWISS, TAF, Zurich Aéroport)
Particuliers	2 (Law_firm, R.S.)
Renonciations explicites à prendre position	7 (UR, ACS, MPC, SSDP, TF, TPF, UPS)

Le présent rapport est un résumé des résultats de la procédure de consultation. Il indique quelles dispositions ont reçu un accueil favorable ou défavorable et si des modifications ont été proposées. S'agissant des participants qui, sans approuver ou rejeter explicitement le projet mis en consultation, se sont uniquement prononcés sur ses différentes dispositions, on peut partir du principe qu'ils l'acceptent dans ses grandes lignes et que leurs critiques ou leurs souhaits de modification se limitent aux dispositions qui font expressément l'objet de la prise de position

[1] RS **172.061**

relative à la consultation. Pour les motivations détaillées des participants, on se référera aux prises de position originales[2].

3 Évaluation générale

A) Approbation: 40

25 cantons (tous sauf UR)
2 partis (Le Centre, PLR)
13 organisations ou associations (AEROSUISSE, ASA, CCDJP, CCPCS, CPS, easyjet, economiesuisse, FSFP, FST, SWISS, TAF, USS, Zurich Aéroport)

Une nette majorité de 40 participants approuve le projet mis en consultation dans son ensemble. Ces participants préconisent l'introduction prévue du traitement systématique des données relatives aux passagers aériens pour que les autorités puissent plus facilement prévenir les infractions terroristes et les autres infractions pénales graves et mener des enquêtes et des poursuites en la matière. Ils considèrent que la création d'une nouvelle loi à cet effet est pertinente (AG, AR, BL, BS, FR, GE, GL, GR, JU, LU, NW, OW, SG, SH, SO, SZ, TG, TI, VD, VS, ZG, ZH, Le Centre, PLR, CCDJP, CCPCS, CPS, FST, FSFP, SWISS, USS).

Divers participants justifient leur approbation dans une démarche de solidarité avec le reste de l'Europe et de respect des obligations internationales de la Suisse. La mise en place d'une autorité légitime sur le plan national traitant les données PNR est indispensable si le pays entend soutenir la comparaison avec les autorités de poursuite pénale internationales (BS, VD, Le Centre, PLR, FST, FSFP, USS).

Plusieurs participants relèvent également que la formulation neutre d'un point de vue technologique de l'avant-projet de loi, qui permet de s'adapter aux évolutions futures sans devoir réviser la loi, est un élément positif (AR, GR, NW, OW, TI, CCPCS, CPS).

Plusieurs autres saluent le rattachement organisationnel prévu de l'UIP à fedpol (AR, BL, BS, GR, NW, OW, SH, SZ, TG, ZG, CCDJP, CCPCS).

Plusieurs participants soutiennent aussi le modèle de détachement selon lequel l'UIP se compose de collaborateurs de la Confédération et des cantons. Ce fonctionnement permet un transfert de compétences de l'UIP aux cantons qui peut être utile notamment pour l'établissement des profils de risque et des listes d'observation (AR, BL, BS, GR, NW, OW, SH, TG, CCDJP, CCPCS).

Les participants approuvant le projet mis en consultation abordent d'autres thèmes résumés ci-après (cf. ch. 4 et prises de position originales):

- **Dépenses supplémentaires en matière de personnel à la charge des cantons**

La majorité des cantons affirme que le projet mis en consultation entraîne des dépenses supplémentaires en matière de personnel à leur charge, dont le montant n'a pas encore pu être chiffré de manière définitive. De plus, il n'existe pas encore de répartition de ces charges entre les cantons. Par conséquent, la participation à parts égales de collaborateurs de la Confédération et des cantons au nouveau service fédéral fait l'objet de critiques et de rejets de la part des cantons (cf. ch. 4.18 relatif à l'art. 20).

[2] fedlex-data-admin-ch-eli-dl-proj-2021-80-cons_1-doc_6-de-pdf-a.pdf

- **Respect des normes techniques existantes et concertation avec le secteur de l'aviation**

Pour **PLR, AEROSUISSE, ASA, economiesuisse, FST, SWISS** et **Zurich Aéroport**, il est crucial que la Suisse se base sur les normes techniques existantes afin que les données requises puissent être générées sans trop de moyens supplémentaires par les systèmes déjà en service dans les entreprises de transport aérien et mises à la disposition des autorités. Les participants souhaitent que les modalités de collecte et de traitement des données définies au niveau de l'ordonnance soient élaborées en étroite collaboration avec les acteurs concernés du secteur de l'aviation et s'opposent à des charges disproportionnées qui aillent au-delà des normes internationales. Il faut éviter de créer de potentiels obstacles supplémentaires qui entravent la compétitivité de la Suisse dans le transport international de voyageurs.
Il n'est pas encore possible d'estimer les conséquences sur les entreprises de transport aérien avec pleine satisfaction. De même, la définition du devoir de diligence et des sanctions en cas de violation des obligations des entreprises de transport aérien n'est pas assez précise (ASA).

- **Protection des données**

Pour différents participants, l'AP-LDPa garantit dans l'ensemble la protection des données et des droits de la personnalité des passagers: seul le personnel de l'UIP est autorisé à accéder aux données relatives aux passagers aériens pour accomplir ses tâches. Dans le même temps, la protection des membres de l'équipage est renforcée et une compatibilité avec l'étranger, dont l'UE, est établie (USS). Le fait que la collecte et l'utilisation des données PNR soient réglées de sorte à satisfaire aux exigences de la directive PNR en matière de protection et de traitement des données est accueilli favorablement (BL). Les participants se félicitent également que le projet mis en consultation se base sur la nouvelle législation sur la protection des données. Le traitement des données est autorisé uniquement à des fins légales et, en cas de concordances obtenues après la comparaison automatique, il est obligatoire de vérifier manuellement la plausibilité de ces dernières. Ce procédé garantit une protection suffisante des données des voyageurs (Le Centre). **PLR** salue l'obligation d'informer incombant aux entreprises de transport aérien, qui doivent expliquer aux passagers que leurs données PNR seront collectées et traitées, ce qui contribue considérablement à protéger les droits de la personnalité. Néanmoins, l'UIP et les autorités de poursuite pénale doivent obligatoirement se fonder sur les principes de minimisation des données et de limitation de la conservation.
Les participants soulèvent la question d'un organisme indépendant de surveillance de l'activité de l'UIP dans le domaine du droit de la protection des données (Préposé fédéral à la protection des données et à la transparence [PFPDT] ou préposé cantonal à la protection des données), qui n'est réglée ni dans le projet mis en consultation, ni dans le rapport explicatif. Selon **SH**, la surveillance interne assumée en intégralité par le service de protection des données de fedpol est jugée insuffisante, car fedpol mène elle-même des enquêtes de police. Compte tenu de la quantité importante de données et des abus potentiels, il est approprié de fournir des instructions sur la sécurité des données déjà à l'étape du rapport explicatif (BE).

- **Conservation des données**

Les participants trouvent que la durée de conservation des données fixée à cinq ans (sous forme pseudonymisée en vertu de l'art. 16, al. 1) est relativement longue. Pour éviter tout reproche sur une conservation disproportionnée de données et toute contradiction avec la jurisprudence européenne, la durée de conservation des données devrait être adaptée à celle mentionnée dans l'arrêt rendu récemment par la Cour de justice de l'Union européenne (CJUE) et le droit d'accès prévu à l'art. 18, al. 1, en relation avec les art. 25 à 28 de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[3] devrait être maintenu (PLR).

[3] RS **235.1**; entrée en vigueur du nouveau droit sur la protection des données au 1er septembre 2023

- **Obligation d'informer de la levée de la pseudonymisation**

Dans sa teneur actuelle, l'AP-LDPa ne prévoit aucune obligation d'informer (a posteriori) la personne concernée de la levée de la pseudonymisation. À l'inverse, l'art. 33 de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[4] prévoit une obligation d'informer les personnes visées par une opération de surveillance impliquant des mesures de recherche soumises à autorisation. Selon les circonstances, cette surveillance peut faire l'objet d'un recours. À la lumière du droit international et de la jurisprudence du Tribunal fédéral relative aux art. 8 et 13 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)[5], il serait opportun de réfléchir à la nécessité d'introduire dans la LDPa une obligation analogue d'informer a posteriori assortie d'une possibilité de recours, d'autant plus que dans ces cas, le passager est également visé, à son insu, par une action de l'État soumise à autorisation et touchant parfois à ses données personnelles. Cette obligation devrait incomber à l'UIP (TAF).

- **Opérabilité de l'UIP**

Conformément aux catégories d'infractions, l'échange immédiat d'informations est considéré comme impératif dans la lutte contre le terrorisme et les infractions pénales graves. Les informations devraient pouvoir être obligatoirement échangées, traitées et analysées 24 heures sur 24, 7 jours sur 7. Il faut donc garantir l'opérabilité de l'UIP en tout temps (AG, PLR).

B) Réserves majeures: 1 (PS)

PS estime que le traitement systématique des données de tous les passagers aériens est délicat pour des raisons de minimisation des données, de proportionnalité et de protection des données. La sécurité des données et leur usage abusif présentent des risques. Des améliorations du projet mis en consultation sont demandées, notamment en ce qui concerne la transmission des données relatives aux passagers aériens aux autorités de poursuite pénale, la durée de conservation de ces données et les conditions pour les transmettre à des services étrangers.

C) Rejet: 8

(UDC, Les Verts, AlgorithmWatch, FSA, Parti pirate, Société numérique, Law_firm, R.S.)

Dans l'ensemble, les participants qui rejettent clairement le projet mis en consultation invoquent les arguments suivants:

La surveillance massive de tous les passagers aériens et la conservation de leurs données ne repose sur aucun motif ni aucun soupçon. Il s'agit d'une conservation disproportionnée de données personnelles, qui représente une grave atteinte aux droits fondamentaux des passagers (UDC, Les Verts, AlgorithmWatch, FSA, Parti pirate, Société numérique, Law_firm).

L'avant-projet de loi arrive au mauvais moment: en effet, une action de l'Allemagne est toujours pendante devant la CJUE. Parallèlement, la Suisse est encore en train d'élaborer une directive sur la gestion des données personnelles API. Elle risque ainsi d'adopter une loi qui pourrait subir d'importantes modifications dès que ladite directive aura abouti ou que la CJUE aura rendu un

[4] RS **121**
[5] RS **0.101**

nouvel arrêt. Il faut tenir dûment compte des réserves et des décisions de la CJUE et réexaminer l'avant-projet de loi en profondeur (UDC, Les Verts, FSA, Parti pirate, Law_firm).

La transmission de toutes les données relatives aux passagers aériens effectuée indépendamment de tout soupçon engendre une quantité énorme de données qui ne peut pas servir la lutte contre le terrorisme (AlgorithmWatch, Parti pirate, Société numérique).

L'évaluation de ces données devrait rester du ressort du Service de renseignement de la Confédération (SRC), qui l'effectue déjà aujourd'hui dans une moindre mesure. L'UIP devrait être uniquement mise en place afin de coordonner l'échange d'informations en Suisse et à l'étranger et pourrait être exploitée sans engendrer de charges de personnel trop importantes (UDC). Aucun nouveau mécanisme de surveillance opaque ne devrait voir le jour et l'utilisation des données PNR devrait être maintenue dans un cadre strict et efficace (Les Verts).

La conservation systématique de toutes les données personnelles pendant cinq ans, sous forme pseudonymisée après six mois, est une mesure inutile et trop onéreuse. Les périodes définies (six mois et cinq ans) sont trop longues sur le plan tant des finances que des aspects techniques de la protection des données (UDC, Les Verts, Parti pirate, Société numérique, Law_firm).

Les données personnelles devraient être échangées uniquement sur la base de soupçons et seulement avec des pays où l'on suppose que des menaces liées au terrorisme ou à la grande criminalité pourraient toucher des vols (UDC).

Le projet mis en consultation nuit également au secret des avocats ainsi qu'à d'autres secrets professionnels protégés par la loi (FSA).

L'AP-LDPa ne propose pas de protection des données forte, ni de droit d'accès, pourtant nécessaires (AlgorithmWatch, Parti pirate, Société numérique, Law_firm).

La base de données utilisée pour établir les profils de risque et les listes d'observation ne sont pas claires pour les justiciables, ni la manière dont leurs données sont traitées dans ce contexte (Les Verts, AlgorithmWatch, FSA, Parti pirate, Société numérique, Law_firm).

Les catégories d'infractions contre lesquelles le PNR entend lutter dépassent largement le domaine du terrorisme et des infractions pénales graves (Les Verts, AlgorithmWatch, FSA, Parti pirate, Société numérique).

4 AP-LDPa: prises de position article par article

4.1 Art. 1

S'agissant de la let. a, **AG** demande que le traitement des données de personnes fugitives condamnées par un jugement entré en force soit explicitement mentionné dans le texte de loi. Pour **ZH**, l'AP-LDPa devrait obligatoirement inclure l'aviation privée.

FSA demande de modifier l'ordre des let. a et b.

4.2 Art. 2

Al. 1

Parti pirate et **R.S.** soulignent que la CJUE limite considérablement la collecte de données pour les vols intra-UE à des cas particuliers, raison pour laquelle il convient de renoncer aux données de la plupart des vols internes à l'espace Schengen.

Al. 2

Les Verts, AlgorithmWatch, Société numérique et **R.S.** ne comprennent pas pourquoi les données doivent être transmises à deux moments différents. Pour eux, cette double transmission

ne fait que doubler la quantité de données. Ils demandent donc que les données ne soient pas transmises avant la fin de l'embarquement. **Parti pirate** ne comprend pas pourquoi la loi ne prévoit pas l'effacement des données des passagers qui n'ont pas embarqué sur le vol.

Al. 3
Parti pirate et **R.S.** notent qu'il manque une instance chargée de contrôler l'effacement éventuel de données sensibles.

FSA demande un renvoi à la LPD ("ne peuvent pas transmettre de données sensibles au sens de l'art. 5, let. c, de la loi fédérale du 25 septembre 2020 sur la protection des données [LPD[6]]").

Al. 4
GR, NE, SO et **TI** approuvent l'al. 4 en vertu duquel fedpol règle les modalités techniques relatives à la transmission des données. **BL** signale qu'il reste possible de réserver un vol sous un faux nom. Les entreprises de transport aérien devraient au moins pouvoir garantir que le nom indiqué lors de la réservation sera vérifié au moment de l'embarquement, lorsque les documents d'identité sont de toute façon contrôlés. Dans le cas contraire, la comparaison des données avec celles issues des systèmes de recherche conformément à l'art. 7 ne servirait à rien.

PS, Les Verts, AlgorithmWatch et **Société numérique** proposent de régler les principes de la transmission des données entre les entreprises de transport aérien et fedpol à l'art. 2, al. 4, et les modalités dans une ordonnance du Conseil fédéral. **Parti pirate** et **R.S.** sont d'avis que fedpol doit fixer les modalités techniques de la transmission des données avec le PFPDT, la décision finale devant incomber à ce dernier.

Pour **ASA**, il n'est pas possible d'estimer pleinement les conséquences sur les entreprises de transport aérien. Le devoir de diligence est considéré comme étant une notion extensible.

FSA demande l'ajout suivant: "La transmission est notamment protégée par un chiffrement de bout en bout. fedpol publie les modalités techniques définies de la transmission."

4.3 Art. 3

SO approuve cette disposition.

Pour **Les Verts, AlgorithmWatch** et **Société numérique**, la transmission des données à l'étranger devrait également être régie par l'AP-LDPa afin que leur sécurité soit garantie. De plus, ces participants demandent que la loi prévoie explicitement la conclusion d'un traité international uniquement avec les États garantissant un niveau de protection adéquat. En ce sens, **FSA** réclame l'ajout suivant: "et que la législation de l'État concerné garantisse une protection adéquate des données relatives aux passagers aériens."

4.4 Art. 5

Pour **ZH**, l'obligation d'informer prévue à l'art. 5 est superflue dans la mesure où il ressort de la loi que ces informations sont collectées et traitées.

Pour **Les Verts, AlgorithmWatch, Parti pirate, Société numérique** et **R.S.**, il est impératif qu'une information compréhensible et bien visible à propos de l'utilisation des données PNR soit communiquée spontanément avant la réservation des billets. Cette information doit énumérer toutes les données qui seront transmises. Le consentement des passagers doit être une décision délibérée. De plus, la Confédération doit clarifier les procédures et les sanctions si les entreprises de transport aérien ne respectent pas leur obligation d'informer. **FSA** demande le remplacement

[6] RS **235.1**

de "par écrit" par "de manière adéquate, compréhensible et sous une forme facilement accessible".

4.5 Art. 6

SO approuve cette disposition.

FSA estime que les annexes 1 et 2 peuvent être fusionnées en une seule annexe 1. Les catégories d'infractions ci-après contenues dans l'annexe 2 de l'avant-projet de loi devraient être retirées: 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26. **Société numérique** partage cet avis.

Al. 1
AG et **BL** demandent que le traitement des données de personnes fugitives condamnées par un jugement entré en force soit explicitement mentionné dans le texte de loi.

AlgorithmWatch et **Société numérique** demandent que la protection des données soit complétée et ainsi renforcée, au lieu d'être restreinte.

Parti pirate et **R.S.** font remarquer que la notion d'"infractions pénales graves" doit être clarifiée de manière univoque et que l'expression "autres infractions pénales graves" doit être supprimée.

Al. 2
BE, GE, ZH et **CPS** indiquent que la définition des infractions terroristes doit renvoyer à l'annexe 1a de l'ordonnance N-SIS du 8 mars 2013[7]. Pour **BE**, cette disposition devrait au moins reprendre l'art. 260^{sexies} du code pénal (CP)[8] et l'art. 2 de la loi fédérale du 12 décembre 2014 interdisant les groupes "Al-Qaïda" et "État islamique" et les organisations apparentées[9].

PS, Les Verts, AlgorithmWatch et **Société numérique** demandent que l'infraction d'émeute à motivation terroriste au sens de l'art. 260 CP soit supprimée des catégories d'infractions terroristes prévues à l'art. 6, al. 2.

Al. 3
Pour **AG**, l'expression "peine privative de liberté d'au moins trois ans" est sujette à interprétation et nécessite une précision dans le rapport explicatif.
BE, ZH et **CPS** estiment que la let. a est trop restrictive. Grâce au traitement des données relatives aux passagers aériens, les enquêteurs ont en leur possession un outil efficace pour identifier les activités de la criminalité organisée, ce que les catégories d'infractions ne prennent pas suffisamment en compte. Par conséquent, la définition des autres infractions pénales graves devrait renvoyer à la catégorie d'infractions de l'annexe 1b de l'ordonnance N-SIS. **BE, BL, GE, CPS** et **Parti pirate** demandent de prévoir une peine privative de liberté d'au moins trois ans tant à la let. a qu'à la let. b. **ZH** souhaite supprimer la let. b, car il n'est pas approprié de mettre sur un pied d'égalité des éléments constitutifs d'une infraction relevant du droit pénal administratif et la lutte contre le terrorisme et la grande criminalité. Si cette disposition devait demeurer inchangée, les catégories d'infractions devraient être réglées au niveau de la loi.

PS, Les Verts, AlgorithmWatch et **Société numérique** demandent que le piratage de produits soit retiré des catégories d'infractions pénales graves prévues par l'art. 6, al. 3, let. a.

GE remarque que l'espionnage politique (art. 272 CP) et militaire (art. 274 CP) ne sont pas pris en compte dans les catégories d'infractions malgré la catégorie 26 (espionnage industriel), ce qui est une lacune en matière de prévention et de détection du renseignement prohibé.

---

[7] RS **362.0**
[8] RS **311.0**
[9] RS **122**

Al. 4
Comme pour l'al. 3, let. b, **ZH** souhaite supprimer l'al. 4. Si cette disposition devait demeurer inchangée, les catégories d'infractions devraient être réglées au niveau de la loi.

Al. 6
BE souhaite une clarification des sanctions policières dans le rapport explicatif: en effet, des mesures de sécurité et de protection mises en place par la police dans le cadre de la gestion des menaces pourraient être très utiles à l'évaluation de l'UIP, d'où le besoin de clarification s'agissant de la transmission de telles informations.

Parti pirate soutient que l'al. 6 est en contradiction avec l'art. 2, al. 3, qui interdit aux entreprises de transport aérien de transmettre des données sensibles. De plus, il est connu que le Département américain de la sécurité intérieure souhaite consulter l'intégralité de ces données, raison pour laquelle il convient d'y renoncer ("minimisation des données") et de supprimer l'al. 6.

Pour **AlgorithmWatch** et **Société numérique**, la disposition doit explicitement mentionner que les poursuites et les sanctions pénales ne peuvent que concerner des infractions terroristes ou d'autres infractions pénales graves. Le traitement de poursuites ou de sanctions administratives doit être supprimé de la let. b.

FSA affirme que l'effacement de données sensibles constitue déjà un traitement en soi qu'il convient d'expliciter ("c. les données en vertu de l'art. 2, al. 3, AP-LDPa, dans le but de les effacer").

4.5 Art. 7

Al. 1
BE est d'avis qu'il faut clarifier la partie du rapport explicatif relative à l'art. 7 et y ajouter que le collaborateur de l'UIP détaché par le canton peut comparer des données avec celles contenues dans les systèmes d'information de son canton. Si les bases légales ne suffisent pas à cet effet, l'AP-LDPa doit y pourvoir. C'est la seule manière d'atteindre le but visé à l'art. 1, al. 1.

Les Verts, AlgorithmWatch, FSA et **Société numérique** proposent de supprimer l'expression "infractions [...] planifiées" (art. 7, al. 1, let. d), car son sens n'est pas clair. **FSA** avance comme autre solution de la définir.
AlgorithmWatch et **Société numérique** demandent que les buts visés aux let. a à d se limitent explicitement aux infractions terroristes ou autres infractions pénales graves.

Al. 2
Pour **LU**, l'al. 2, dispose certes que la comparaison automatique est faite "immédiatement après réception des données", mais dans la pratique, l'utilité de leur transmission dépend essentiellement du fait que les autorités de poursuite pénales les reçoivent rapidement.

PLR n'est pas satisfait du mot "immédiatement", qu'il juge vague. Il faudra définir dans l'ordonnance d'exécution le délai dans lequel les données devront être comparées et, le cas échant, les cas suspects annoncés aux autorités de poursuite pénale.

Al. 3
PS invite fedpol à établir suffisamment la plausibilité requise lors de l'exécution et à effacer systématiquement les données relatives aux passagers aériens concernées en l'absence de lien avec l'une des catégories d'infractions.

Pour **AlgorithmWatch** et **Société numérique**, il est difficile de savoir à quels systèmes d'information les systèmes "supplémentaires" se rapportent. Il convient de définir expressément

les systèmes d'information auxquels l'UIP a accès. De plus, la journalisation des accès doit être réglée au niveau de l'ordonnance.

FSA demande les ajouts suivants: "Avant que des concordances obtenues automatiquement soient transmises à l'autorité compétente, leur plausibilité doit être *immédiatement* vérifiée manuellement et [...] les motifs de diffusion de son signalement. *La vérification doit être documentée*." et "[…] doivent être vérifiées quant à leur exactitude. Le résultat de cette vérification doit être documenté".

4.6 Art. 8

FSA demande la suppression de l'art. 8, al. 1, let. b.
BE propose d'utiliser la désignation "autorités de police et de poursuite pénale" à l'al. 2, let. a. Les expressions "autorités de poursuite pénale" et "l'existence d'une infraction" sont trop restrictives et doivent être revues.
BL suggère de reformuler l'al. 1: "pour autant que leur vérification ait confirmé que les données servent à prévenir ou à poursuivre une infraction pénale au sens de [...]" à la place de "pour autant que leur vérification ait confirmé l'existence d'une infraction au sens de [...]".

SH qualifie de prometteuse la comparaison automatique des données relatives aux passagers aériens avec les données issues des systèmes d'information de police.

VD propose d'ajouter les services de renseignement cantonaux à l'al. 2.

Pour **ZH**, il faut régler expressément la possibilité de transmettre aussi des données biométriques pour faciliter la suite de la poursuite pénale.

AlgorithmWatch, FSA et **Société numérique** demandent que seule une autorité judiciaire, et non pas l'UIP, puisse vérifier l'existence d'une infraction.

4.7 Art. 9

BL est d'avis qu'il manque des prescriptions pour la comparaison de données avec les profils de risque et les listes d'observation établis par l'UIP. Cette comparaison doit être effectuée immédiatement une fois les données reçues et ne peut pas être répétée au gré de l'UIP tant que les données n'ont pas été pseudonymisées. De plus, la plausibilité des concordances doit être établie avant la transmission des données à d'autres autorités afin que les personnes concernées ne soient pas soupçonnées à tort. Ces restrictions ne doivent pas être déléguées au Conseil fédéral en vue de la réglementation au niveau de l'ordonnance, mais elles doivent être inscrites dans la loi.

LU estime que la possibilité d'établir des profils de risque et des listes d'observation et de pouvoir les comparer en continu avec les données relatives aux passagers aériens fournies est très utile. Toutefois, le rapport explicatif ne mentionne ni la forme sous laquelle la demande d'établissement de profils de risque et de listes d'observation doit parvenir, ni la manière dont l'UIP doit rendre sa décision en la matière, ni la personne compétente au sein de l'UIP pour rendre cette décision, ni les possibilités de recourir contre une décision négative. Ces aspects doivent être pris en compte lors de l'élaboration de l'ordonnance. Enfin, il convient d'examiner les profils de risque et les listes d'observation sous l'angle de la non-discrimination et de l'égalité de traitement des personnes concernées.

Les Verts, AlgorithmWatch, FSA et **Société numérique** demandent la suppression pure et simple de cet article. Cette disposition introduirait une recherche par quadrillage générale sans motif ni soupçon. Une telle recherche irait clairement au-delà de la comparaison déjà importante de données personnelles avec des systèmes d'information conformément à l'art. 7 et serait manifestement disproportionnée. Si l'art. 9 devait ne pas être supprimé, il faudrait régler

précisément la manière de procéder à ces analyses pour que les profils de risque et les listes d'observation soient établis avec transparence et qu'ils ne se fondent pas sur des éléments directement ou indirectement discriminatoires. De plus, les résultats de la vérification prévue à l'art. 9, al. 5, devraient être publiés et une surveillance efficace devrait être définie. **FSA** propose des adaptations textuelles précises si l'article n'est pas supprimé.
Parti pirate et **R.S.** veulent une définition plus précise des *analyses*, des *profils de risque* et des *listes d'observation*. S'il n'est pas possible de préciser ces définitions, la disposition doit être supprimée sans être remplacée. De plus, le recours à l'intelligence artificielle dans le cadre de systèmes auto-apprenants (*machine learning*) pour les comparaisons doit être expressément interdit.

SG suggère également de vérifier la plausibilité des résultats de la comparaison des données avec les profils de risque et les listes d'observation avant de transmettre ces données aux autorités compétentes.

4.8 Art. 10

PS approuve la réglementation relativement restrictive de la transmission des données relatives aux passagers aériens au SRC. Cette réglementation ne doit ainsi en aucun cas être assouplie. Un accès direct du SRC au système d'information PNR est notamment inconcevable.

Les Verts, AlgorithmWatch, FSA et **Société numérique** demandent la suppression pure et simple de l'art. 10. Si le Conseil fédéral décidait de le maintenir, la transparence exigerait que les trajets définis par le SRC soient au moins publiés et les passagers informés spontanément, avant la réservation, de la transmission générale de leurs données PNR au SRC. De plus, ce dernier doit immédiatement effacer les données si la comparaison n'a pas donné de concordance (et non pas 96 heures au plus après les avoir reçues).

Parti pirate et **R.S.** demandent que la Commission de gestion du Parlement approuve les trajets que le SRC souhaite surveiller. En outre, la loi doit clairement disposer que les données transmises sont effacées directement après une comparaison si cette dernière ne donne aucune concordance.

4.9 Art. 11

VD propose d'ajouter les services de renseignement cantonaux à cet article.

BE propose d'utiliser la désignation "autorités de police et de poursuite pénale" à la let. a. **BE, BL** et **CPS** demandent que le passage suivant soit retiré du rapport explicatif: "Les recherches d'ordre général, c'est-à-dire celles dont la teneur n'est pas spécifiée et qui produisent une multitude de résultats divers [...]" (p. 31). Cette restriction des possibilités de recherche ne repose sur aucune disposition de la loi. Il doit par exemple être possible de faire des recherches sur tous les passagers d'un certain vol.

LU critique le fait que ni la loi, ni le rapport explicatif ne mentionnent qui est compétent au sein de l'UIP pour statuer sur les demandes et s'il existe des voies de recours contre les décisions rendues. Il est préconisé de tenir également compte de cet aspect lors de l'élaboration de l'ordonnance.

ZH propose d'autoriser expressément les recherches dans les ensembles de données importants dans le cadre de la vérification de schémas comportementaux et de le mentionner en conséquence dans le message.

Parti pirate et **R.S.** demandent la suppression pure et simple de cette disposition. **FSA** souhaite que les demandes soient vérifiées et documentées et demande l'ajout d'un alinéa: "Les voies de droit sont régies par la loi qui règle l'activité de l'autorité concernée".

4.10 Art. 12

BE propose d'utiliser la désignation "autorités de police et de poursuite pénale" à l'al. 1 et de vérifier le qualificatif de "konkret" (concerne le texte allemand) s'agissant des soupçons.

Pour **ZH, PLR, PS, CPS** et **FSA**, l'expression "konkreter Verdacht" ("s'il y a lieu de soupçonner") ne doit pas être utilisée à l'al. 1 (proposition de reformulation de ZH: soupçon initial, soupçon suffisant, soupçon grave / PLR, CPS: supprimer "konkret" / PS: soupçon grave / FSA: soupçon suffisant). Des "indices" d'infraction pénale doivent suffire. Il convient de modifier la disposition en conséquence.

Les Verts, AlgorithmWatch, FSA et **Société numérique** demandent que l'on utilise l'expression de "soupçon suffisant". S'agissant de l'al. 2, ces participants demandent de préciser que les données sensibles dont il est question sont celles visées à l'art. 6, al. 6.

FSA indique que l'art. 12 devrait être placé entre l'art. 9 et l'art. 10 (actuel) pour des raisons de cohérence.

R.S. propose de supprimer l'expression "ou une autre infraction pénale grave".

4.11 Art. 13, al. 2

BL note que le Conseil fédéral doit fixer d'autres exigences en matière de protection des données compte tenu de la quantité de données et des abus potentiels.

PS est d'avis que seuls des employés de droit public doivent avoir accès au système d'information PNR pour des raisons de protection et de sécurité des données. Cette condition doit être inscrite dans la loi au présent alinéa.

AlgorithmWatch et **Société numérique** proposent de régler du point de vue organisationnel à l'al. 2, let. a, qui a accès à quelles données. De plus, il faut introduire un principe des quatre yeux si les données doivent être traitées manuellement. Ces deux participants, ainsi que **Parti pirate** et **R.S.** souhaitent en outre supprimer l'al. 2, let. b.

4.12 Art. 14

Pour **PS**, le fait que l'application de la présente loi entraîne la collecte des données de passagers aériens qui ne sont pas concernés par une infraction pénale est problématique. Par conséquent, le parti propose la modification suivante: "Le système d'information PNR pseudonymise automatiquement les données relatives aux passagers aériens trois mois après que les entreprises de transport aérien les ont transmises."

Les Verts veulent que les données soient immédiatement effacées après que l'UIP a procédé à la comparaison. Si le Conseil fédéral devait maintenir l'enregistrement, il faudrait au moins que la pseudonymisation ait lieu plus tôt, c'est-à-dire automatiquement dès la comparaison des données. **AlgorithmWatch, Société numérique** et **R.S.** estiment que le délai de six mois pour la pseudonymisation est trop long.

Pour **Parti pirate**, il est urgent de réduire considérablement la période d'enregistrement.

FSA demande une définition du terme "pseudonymisation" (proposition: "On entend par pseudonymisation le remplacement du nom et d'autres caractéristiques d'identification par un signe distinctif dans le but de compliquer considérablement l'identification des personnes concernées").

4.13 Art. 15

LU fait remarquer que, compte tenu de la grande pertinence escomptée des données relatives aux passagers aériens et du large éventail de catégories d'infractions, il faudra s'attendre à un nombre élevé de demandes de levée de la pseudonymisation rien que du côté des autorités de poursuite pénale (des données datant de plus de six mois peuvent souvent être pertinentes dans les enquêtes). Il faut donc accorder une importance particulière à cet aspect au vu des ressources dont le TAF aura besoin. **SH** remet en question la pertinence de la pseudonymisation prévue à l'art. 15. Les délais d'effacement devraient plutôt être aussi brefs que possible et inscrits formellement dans la loi.

Les Verts souhaitent qu'il soit possible de demander la levée de la pseudonymisation nécessaire pour garantir le droit d'accès (art. 15, al. 1).

TAF constate que le libellé de l'al. 5 ne permet pas de savoir si la procédure reste pendante devant le TAF le temps que le dossier soit complété ou que des éclaircissements soient apportés. Selon le cas de figure, il n'est pas possible de statuer dans un délai de cinq jours ouvrables.

FSA suggère l'ajout d'un al. 6 (*"Le TAF publie ses arrêts.").*

4.14 Art. 16

Pour **PS**, il est essentiel que l'État conserve les données collectées par les autorités uniquement pour la durée strictement nécessaire. Dans ce contexte, il convient de raccourcir considérablement la durée de conservation (proposition: "Les données relatives aux passagers aériens sont effacées automatiquement deux ans après leur introduction dans le système d'information PNR").

PLR relève que l'enregistrement des données au-delà de la durée habituelle en l'absence d'indice d'infraction pénale commise est une atteinte aux droits fondamentaux des passagers, notamment car le droit d'accès individuel ne pourrait plus être exercé si les données ont été pseudonymisées (art. 18, al. 2). Pour éviter tout reproche sur une conservation disproportionnée des données et toute contradiction avec la jurisprudence européenne, la durée de conservation des données devrait être adaptée à celle mentionnée dans l'arrêt rendu par la CJUE et le droit d'accès prévu à l'art. 18, al. 1, en relation avec les art. 25 à 28 LPD devrait être maintenu. **SG** renvoie également à cet arrêt en ce qui concerne la durée d'enregistrement.

Les Verts, AlgorithmWatch et **Société numérique** veulent que les données soient effacées dès que l'UIP a procédé à la comparaison. Ils demandent la suppression de la durée de conservation prévue à l'al. 1. Si le Conseil fédéral devait maintenir l'enregistrement, il faudrait au moins que la pseudonymisation ait lieu plus tôt, soit automatiquement dès la comparaison des données. De plus, il est indispensable que la durée de conservation des données résultant d'une comparaison prévue aux art. 7 et 9 soit aussi inscrite dans la loi (art. 16, al. 2). Il s'agit de données sensibles pouvant être traitées uniquement en vertu d'une base légale formelle.

FSA relève qu'il serait possible d'enregistrer certaines données relatives aux passagers aériens (pseudonymisées) après six mois si une concordance a résulté de la vérification prévue à l'art. 7, si la vérification par quadrillage au sens de l'art. 9 a donné lieu à une transmission ou si les données ont été transmises d'une autre manière (également sur demande). Cette réglementation pourrait figurer dans un nouvel alinéa (proposition: "[…] six mois après leur introduction […]"). En outre, il est suggéré de régler dans la loi la durée maximale de conservation de toutes les données et non pas uniquement de celles prévues à l'art. 16, al. 1.

Parti pirate et **R.S.** proposent que les données soient effacées dans un délai de 24 heures après l'atterrissage moyennant la mise en place d'un mécanisme de contrôle et de sanction.

4.15 Art. 17

LU constate que le service de protection des données de fedpol veille au respect des dispositions relatives à la protection des données en vertu du présent article. Pour remplir cette tâche avec efficacité, il doit recevoir l'accès à toutes les données traitées (cf. art. 6(7) de la directive (UE) 2016/681).
FSA propose l'ajout suivant: "Le service de protection des données de fedpol veille au respect du traitement des données personnelles conformément à la présente loi. Il publie un rapport de surveillance annuel."

4.16 Art. 18

BL et **PS** ne comprennent pas pourquoi les données pseudonymisées sont exclues du droit d'accès ou du droit d'accès aux données personnelles propres.
LU observe que le droit d'accès des personnes concernées devrait être étendu à toutes les données, y compris aux données pseudonymisées, et ne devrait être restreint qu'à titre exceptionnel.

Les Verts, AlgorithmWatch et **Société numérique** souhaitent que l'al. 2 soit supprimé, alors que **FSA** réclame également la suppression de l'al. 3.

Parti pirate et **R.S.** font remarquer que la pseudonymisation des données entraîne une importante discrimination de toutes les personnes concernées. Si les données ne sont pas effacées dans un délai de 24 heures après l'atterrissage, ces personnes doivent dans tous les cas pouvoir faire usage de leur droit d'accès durant toute la période d'enregistrement des données (pseudonymisées ou non).

4.17 Art. 19

ZH considère que la transmission immédiate des données par l'UIP est décisive, notamment dans le cadre de recherches. Par conséquent, l'UIP devrait être opérationnelle 24 heures sur 24, 7 jours sur 7.

4.18 Art. 20

AG salue le choix de composer le personnel de l'UIP à parts égales de collaborateurs de la Confédération et des cantons, ce qui garantit le transfert de connaissances aux cantons.
Pour **ZH**, il est important que tous les cantons participent de manière équitable aux coûts relatifs à l'engagement de leurs collaborateurs au sein de l'UIP, étant donné qu'ils bénéficieront tous d'un gain de sécurité.
SO est aussi favorable à une participation en personnel et rappelle l'obligation de détachement actuelle et la mise en œuvre du traitement des données dans les activités des polices cantonales, qui doivent être prises en compte dans la planification future des effectifs. La charge supplémentaire pour les cantons doit être considérée en regard de l'utilité de cette mesure.
BE exprime sa volonté de mettre du personnel à la disposition de l'UIP, rattachée à fedpol, et d'élaborer une convention en la matière, même si la charge opérationnelle effective pour le canton ne peut pas encore être chiffrée.
ZG signale que les cantons devraient avoir suffisamment de temps pour budgétiser les postes avant l'entrée en vigueur de la loi.

BL s'oppose à une participation en personnel à parts égales entre la Confédération et les cantons au sein du nouveau service fédéral, d'autant plus que le rapport explicatif ne comporte que des indications rudimentaires sur les conséquences financières pour eux. Compte tenu des informations actuellement disponibles, les cantons peuvent difficilement estimer les coûts qui seront à leur charge. Les indications relatives aux conséquences financières pour les cantons doivent donc être complétées et précisées.

FR se montre également critique envers la clé de répartition et est dans l'incertitude quant à son engagement futur dans la mise en œuvre de l'UIP.
TI, NE, VD et **VS** remettent également en question cette clé de participation, car elle sollicite bien trop les cantons.
NE espère que cette répartition prendra en considération l'utilisation réelle de l'UIP par les autorités cantonales et estime qu'un détachement limité à seulement une année est peu judicieux. Finalement, il apparaît particulièrement important que l'UIP représente toutes les entités utilisatrices concernées.
JU demande l'application d'une répartition d'un tiers à la charge des cantons et de deux tiers à la charge de la Confédération.
AI indique qu'il ne pourra pas détacher du personnel pour l'engagement au sein de l'UIP compte tenu de la taille de sa police cantonale.
AR, GR, SH et **TG** souhaitent que la Confédération prenne en charge l'intégralité des coûts relatifs à l'engagement des collaborateurs, comme c'est le cas pour les Centres de coopération policière et douanière de Genève et de Chiasso. C'est la seule manière de pouvoir détacher du personnel pour assumer des tâches de la Confédération, notamment pour les petits cantons et leur police. Par conséquent, il convient d'adapter l'art. 20, al. 4.
Pour **GL, NW** et **SZ**, il est essentiel que les cantons soient impliqués d'emblée dans les travaux de planification ultérieurs et notamment dans l'élaboration de la structure organisationnelle concrète. De plus, **SZ** souhaite que les ressources en personnel (étonnamment élevées malgré l'automatisation) soient examinées d'un œil critique.

Pour **GE**, une attention particulière doit être portée aux répercussions des mesures prévues par la loi et à l'emplacement de l'UIP dans les cas relevant de la compétence cantonale.

GE relève par ailleurs que le rapport explicatif ne précise pas si des UIP décentralisées sont aussi prévues dans les principaux aéroports suisses.

Compte tenu des ressources limitées des corps de police cantonaux, **FSFP** soutient une participation à parts égales de collaborateurs de la Confédération et des cantons à la seule condition que du personnel soit recruté.

Parti pirate se demande pourquoi les cantons ne prendraient pas simplement les coûts à leur charge au lieu de détacher la moitié du personnel. **R.S.** déclare que l'on souhaite introduire des processus compliqués.

S'agissant de l'al. 3, **BL** trouverait pertinent d'inscrire sans équivoque dans la loi l'obligation de garder le secret, qui doit également être respectée vis-à-vis de l'employeur contractuel des collaborateurs de l'UIP.

4.18 Art. 21

SO approuve cette disposition.

SH, Les Verts, AlgorithmWatch, Société numérique et **R.S.** demandent que la loi prévoie explicitement que la Suisse ne peut conclure des traités internationaux qu'avec les États qui garantissent une protection des données adéquate. **FSA** souhaite modifier à l'al. 1 l'expression "[…] une protection des données adéquate ou adaptée […]" et ajouter à l'al. 2: "[…], pour autant que leur droit interne garantisse une protection adéquate ou adaptée de ces données."

Parti pirate demande des précisions quant au terme "comparable", qui pourrait aussi signifier "un peu moins bonne".

4.19 Art. 22

LU recommande d'inscrire dans l'AP-LDPa la double incrimination telle que la prévoit l'art. 64 de la loi du 20 mars 1981 sur l'entraide pénale internationale[10], de façon que cette disposition s'applique également à la transmission de données relatives aux passagers aériens.

BE demande de vérifier le qualificatif de "begründet" ("motivée").

ZH propose de remplacer l'expression "begründeter Verdacht" ("s'il n'y a pas lieu de soupçonner") par "Anhaltspunkte" ("s'il n'existe pas d'indices").

BL note que l'al. 3 revient à vérifier matériellement qu'il y a "lieu de soupçonner" ("begründeter Verdacht"), puisque l'UIP doit avoir reçu une demande motivée conformément à l'al. 2 et que le service étranger qui fait la demande doit remplir les mêmes tâches qu'elle. Pour **CPS**, il convient d'adapter la version allemande en supprimant "begründeter" ("wenn gegen die betreffende Person kein Verdacht vorliegt"), de manière à la rapprocher de la version française, comme pour l'art. 12.
Pour **Parti pirate**, il est nécessaire de préciser, à l'al. 3, qui décide s'il y a lieu ou non de soupçonner que la personne concernée a commis ou planifie une infraction terroriste ou une autre infraction pénale grave. Le parti propose un organe composé de cinq juges fédéraux.

4.20 Art. 23

SO approuve cette disposition.

Al. 1
BL propose de sanctionner la violation de l'art. 3 et non pas celle de l'art. 4.

Al. 2
AEROSUISSE, economiesuisse et **SWISS** proposent de supprimer purement et simplement l'art. 23, al. 2, let. b. Les entreprises de transport aérien ne peuvent pas vérifier l'exactitude des données saisies par les passagers ou par les agences. De plus, il n'existe pas de normes en matière de données relatives aux passagers aériens fausses ou correctes; il s'agit d'informations que les entreprises de transport aérien saisissent pour pouvoir effectuer une réservation d'un point de vue commercial.

TAF signale que la let. d doit renvoyer à l'art. 15, al. 4.

Al. 5
Pour **ASA**, l'al. 5 s'accompagne de risques parfois difficiles à évaluer pour les entreprises de transport aérien, étant donné que la violation du devoir de diligence et de l'obligation d'informer prévus aux art. 4 et 5 est sanctionnée indépendamment du fait que l'entreprise en question prouve que la faute ne lui est pas imputable. Le ch. 6 "Aspects juridiques" du rapport explicatif n'aborde pas non plus ces risques.

4.20 Annexe 1

SO approuve l'annexe 1.

AG et **ZH** souhaitent que les données biométriques soient ajoutées à la liste.

AlgorithmWatch et **Société numérique** proposent que toutes les données visées à l'annexe 1 soient pseudonymisées.

[10] RS **351.1**

4.21 Annexe 2

SO approuve l'annexe 2.

BE, ZH, GE et **CPS** indiquent que la définition des infractions terroristes doit renvoyer à l'annexe 1a de l'ordonnance N-SIS.

Les Verts, AlgorithmWatch et **Société numérique** demandent que toutes les catégories d'infractions qui ne présentent aucun lien objectif indirect avec le transport de passagers aériens soient supprimées. Pour **FSA**, les catégories d'infractions ci-après contenues dans l'annexe 2 de l'avant-projet de loi devraient en être retirées: 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26.

Liste des cantons, partis et organisations ayant répondu à la consultation

(avec indication des abréviations utilisées dans le texte)

1. CANTONS

AG	Conseil d'État du canton d'Argovie
AI	Conseil d'État du canton d'Appenzell Rhodes-Intérieures
AR	Conseil d'État du canton d'Appenzell Rhodes-Extérieures
BE	Conseil-exécutif du canton de Berne
BL	Conseil d'État du canton de Bâle-Campagne
BS	Conseil d'État du canton de Bâle-Ville
FR	Conseil d'État du canton de Fribourg
GE	Conseil d'État du canton de Genève
GL	Conseil d'État du canton de Glaris
GR	Conseil d'État du canton des Grisons
JU	Gouvernement du canton du Jura
LU	Conseil d'État du canton de Lucerne
NE	Conseil d'État du canton de Neuchâtel
NW	Conseil d'État du canton de Nidwald
OW	Conseil d'État du canton d'Obwald
SG	Conseil d'État du canton de Saint-Gall
SH	Conseil d'État du canton de Schaffhouse
SO	Conseil d'État du canton de Soleure
SZ	Conseil d'État du canton de Schwyz
TG	Conseil d'État du canton de Thurgovie
TI	Conseil d'État du canton du Tessin
UR	Conseil d'État du canton d'Uri
VD	Conseil d'État du canton de Vaud
VS	Conseil d'État du canton du Valais
ZG	Conseil d'État du canton de Zoug
ZH	Conseil d'État du canton de Zurich

2. PARTIS POLITIQUES REPRÉSENTÉS À L'ASSEMBLÉE FÉDÉRALE

Le Centre	Le Centre
PLR	Parti libéral-radical suisse
PS	Parti socialiste suisse
UDC	Union démocratique du centre
Les Verts	Parti écologiste suisse

3. ASSOCIATIONS FAÎTIÈRES DES COMMUNES, DES VILLES ET DES RÉGIONS DE MONTAGNE ŒUVRANT AU NIVEAU NATIONAL

ACS	Association des communes suisses

4. ASSOCIATIONS FAÎTIÈRES DE L'ÉCONOMIE ŒUVRANT AU NIVEAU NATIONAL

economiesuisse	Fédération des entreprises suisses
UPS	Union patronale suisse
usam	Union suisse des arts et métiers
USS	Union syndicale suisse

5. AUTRES ORGANISATIONS ET INSTITUTIONS

AEROSUISSE	AEROSUISSE
AlgorithmWatch	AlgorithmWatch CH
ASA	Association suisse des aérodromes
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des commandants des polices cantonales de Suisse
CPS	Conférence des procureurs de Suisse
easyjet	easyjet
FSA	Fédération suisse des avocats
FSFP	Fédération Suisse des Fonctionnaires de Police
FST	Fédération suisse du tourisme
MPC	Ministère public de la Confédération
Parti pirate	Parti pirate Suisse
privatim	Conférence des préposé(e)s suisses à la protection des données
Société numérique	Société numérique
SSDP	Société suisse de droit pénal
SWISS	SWISS
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TPF	Tribunal pénal fédéral
Zurich Aéroport	Zurich Aéroport

PERSONNES PRIVÉES

Law_firm	Sylvain Métille, professeur ass., Dr en droit, avocat
R.S.	Rolf Sommer