COM(2021) 784 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2021/2022

Reçu à la Présidence de l'Assemblée nationale
le 28 janvier 2022

Enregistré à la Présidence du Sénat
le 28 janvier 2022

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Règlement du Parlement européen et du Conseil relatif à l’échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil

E 16404

COMMISSION
EUROPÉENNE

Bruxelles, le 8.12.2021
COM(2021) 784 final

2021/0410 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil

{SEC(2021) 421 final} - {SWD(2021) 378 final} - {SWD(2021) 379 final}

EXPOSÉ DES MOTIFS

CONTEXTE DE LA PROPOSITION

• Justification de la proposition

La criminalité en Europe nuit à la sécurité et au bien-être des citoyens de l'Union européenne. Les services répressifs ont besoin d'outils solides et performants pour lutter efficacement contre la criminalité. La coopération et le partage d'informations sont les outils les plus efficaces pour lutter contre la criminalité et le terrorisme et rendre la justice[1]. En 2021, plus de 70 % des organisations criminelles étaient présentes dans plus de trois États membres[2]. Même la criminalité d'apparence très locale peut avoir des liens avec d'autres endroits en Europe où le même auteur a commis ses actes criminels. De même, les liens entre la criminalité présumée locale et les structures et activités de la criminalité organisée ne sont souvent pas évidents. Par conséquent, afin de pouvoir lutter efficacement contre la criminalité, les services répressifs doivent être en mesure d'échanger des données en temps utile. L'Union a déjà fourni aux services répressifs une panoplie d'instruments pour faciliter l'échange d'informations, dont l'importance s'est révélée cruciale pour mettre au jour les activités criminelles et les réseaux criminels[3], mais il subsiste toujours des lacunes en matière d'information qu'il convient de combler. En outre, les données étant stockées séparément dans divers systèmes d'information nationaux ainsi que dans des systèmes d'information à grande échelle au niveau de l'Union, il est nécessaire de veiller à ce que ces systèmes puissent communiquer entre eux.

Dans l'espace sans contrôles aux frontières intérieures qu'est l'espace Schengen, l'échange de données entre les services répressifs continue de se heurter aux frontières et à des obstacles[4], ce qui crée des angles morts et des failles exploités par de nombreux criminels et terroristes qui agissent dans plusieurs États membres. La présente initiative ainsi que la proposition, adoptée en parallèle, de directive relative à l'échange d'informations entre les services répressifs des États membres[5] visent à renforcer l'échange d'informations entre les États membres et, partant, à fournir aux services répressifs de l'Union des outils améliorés pour lutter contre la criminalité et le terrorisme[6].

Depuis plus de dix ans, le cadre Prüm permet aux services répressifs de l'Union d'échanger des informations. Adoptées en 2008 dans le but de soutenir la coopération policière et judiciaire transfrontalière en matière pénale, les décisions Prüm[7] prévoient l'échange automatisé de données spécifiques (profils ADN, empreintes digitales et données relatives à l'immatriculation des véhicules) entre les autorités chargées de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière. Le cadre Prüm contribue avec succès à la lutte contre la criminalité et le terrorisme dans l'Union, mais il subsiste encore des lacunes dans le domaine de l'échange d'informations et des améliorations peuvent par conséquent être apportées.

---

[1] Stratégie de l'UE pour l'union de la sécurité 2020 – COM(2020) 605 final du 24.7.2020.

[2] Évaluation 2021 de la menace que représente la grande criminalité organisée dans l'Union.

[3] Stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025), COM(2021) 170 final du 14.4.2021.

[4] Comme les modalités d'échange de certaines catégories de données, le canal utilisé pour ces échanges, les délais applicables, etc.

[5] [Référence].

[6] Communication intitulée «Stratégie pour un espace Schengen pleinement opérationnel et résilient», COM(2021) 277 final du 2.6.2021.

[7] Décision 2008/615/JAI du Conseil relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière; et décision 2008/616/JAI du Conseil concernant la mise en œuvre de la décision 2008/615/JAI. Les décisions du Conseil reposent sur le traité de Prüm de 2005.

Dans ses conclusions sur la mise en œuvre des décisions Prüm dix ans après leur adoption, le Conseil a souligné l'importance de la consultation et de la comparaison automatisées de profils ADN, de données dactyloscopiques et de données relatives à l'immatriculation des véhicules pour lutter contre le terrorisme et la criminalité transfrontière. Le Conseil a également demandé à la Commission d'envisager de réviser les décisions Prüm en vue d'en élargir le champ d'application et de mettre à jour les exigences techniques et juridiques nécessaires[8].

Le mécanisme de Prüm II repose sur le cadre Prüm actuellement en place, en le renforçant et en le modernisant, et en permettant l'interopérabilité avec d'autres systèmes d'information de l'Union. Il garantira que toutes les données pertinentes dont disposent les services répressifs d'un État membre peuvent être utilisées par les services répressifs des autres États membres. Il permettra également à Europol d'apporter son soutien aux États membres au titre du cadre Prüm. La présente initiative prévoit la création d'une nouvelle architecture qui permette un échange de données plus facile et plus rapide entre les États membres et qui garantisse un niveau élevé de protection des droits fondamentaux.

- **Objectifs de la proposition**

L'objectif général de la présente proposition résulte de l'objectif fondé sur le traité visant à contribuer à la sécurité intérieure de l'Union européenne. Parmi les mesures à prendre à cette fin figurent la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes[9]. Par conséquent, l'objectif général du présent instrument est d'améliorer, de rationaliser et de faciliter l'échange d'informations aux fins de la prévention et de la détection des infractions pénales et terroristes ainsi que des enquêtes en la matière entre les services répressifs des États membres, mais aussi avec Europol en tant que plateforme centrale d'information sur la criminalité dans l'Union.

La présente proposition poursuit les objectifs stratégiques spécifiques suivants:

(a) fournir une solution technique pour un échange automatisé efficace de données entre les services répressifs afin de les informer des données pertinentes disponibles dans la base de données nationale d'un autre État membre;

(b) faire en sorte qu'un plus grand nombre de données pertinentes (en ce qui concerne les catégories de données) provenant des bases de données nationales des autres États membres soient mises à la disposition de l'ensemble des services répressifs compétents;

(c) faire en sorte que les données pertinentes (en ce qui concerne les sources de données) provenant des bases de données d'Europol soient mises à la disposition des services répressifs;

(d) fournir aux services répressifs un accès efficace aux données réelles correspondant à une «concordance» qui sont disponibles dans la base de données nationale d'un autre État membre.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

Dans sa récente stratégie Schengen[10], la Commission a annoncé plusieurs mesures visant à approfondir la coopération policière et l'échange d'informations entre les services répressifs afin de renforcer la sécurité dans un espace sans frontières intérieures, intrinsèquement interdépendant. Conjuguée à la proposition de directive relative à l'échange d'informations entre les services répressifs des États membres, la présente proposition contribue à la réalisation des objectifs de cette stratégie en

[8] Conclusions du Conseil sur la mise en œuvre des «DÉCISIONS PRÜM» dix ans après leur adoption (document 11227/18) (https://data.consilium.europa.eu/doc/document/ST-11227-2018-INIT/fr/pdf).

[9] Article 87, paragraphe 2, point a), du traité sur le fonctionnement de l'Union européenne.

[10] Communication de la Commission au Parlement européen et au Conseil intitulée «Stratégie pour un espace Schengen pleinement opérationnel et résilient», COM(2021) 277 final du 2.6.2021.

garantissant que les services répressifs d'un État membre ont accès aux mêmes informations que celles dont disposent leurs homologues d'un autre État membre.

La proposition s'inscrit dans le paysage plus large des systèmes d'information de l'Union à grande échelle qui a considérablement évolué depuis l'adoption du cadre Prüm. Il s'agit des trois systèmes d'information centraux de l'Union qui sont en service, à savoir le système d'information Schengen (SIS), le système d'information sur les visas (VIS) et le système Eurodac[11]. En outre, trois nouveaux systèmes sont actuellement en phase de développement: le système d'entrée/de sortie (EES), le système européen d'information et d'autorisation concernant les voyages (ETIAS) et le système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN)[12]. Tous ces systèmes actuels et futurs sont reliés par le cadre pour l'interopérabilité des systèmes d'information de l'Union[13] pour la sécurité, les frontières et la gestion des migrations, qui a été adopté en 2019 et dont la mise en place est en cours. Les modifications incluses dans la présente proposition visent à aligner le cadre Prüm sur le cadre pour l'interopérabilité, notamment en ce qui concerne l'échange de données et l'architecture globale prévue par l'interopérabilité des systèmes d'information de l'Union. Cet alignement permettrait un accès rapide et contrôlé aux informations dont les agents des services répressifs ont besoin pour s'acquitter de leurs tâches et pour lesquelles ils disposent de droits d'accès.

Le SIS contient déjà des signalements sur les personnes disparues et permet des recherches à partir des empreintes digitales. Le SIS est un système d'information «hit/no hit» (de concordance/non-concordance) centralisé, exploitable, directement accessible à un grand nombre d'utilisateurs finaux de première ligne, qui contient des signalements et fournit une réponse immédiate sur place, tout en indiquant des actions à prendre en rapport avec le sujet du signalement. Le SIS est principalement utilisé lors des contrôles de police, de frontière et de douane, ainsi que par les autorités chargées des visas et de l'immigration dans le cadre de leurs procédures et contrôles de routine.

En revanche, le cadre Prüm ne dispose d'aucune composante ou base de données centrale au niveau de l'Union et il n'est utilisé que dans le cadre d'enquêtes en matière pénale. Il permet aux autres États membres d'accéder aux sous-ensembles dépersonnalisés des bases de données nationales de profils ADN et d'empreintes digitales des services répressifs de tous les États membres connectés. Cet accès est accordé uniquement aux points de contact nationaux. Alors que la réponse comportant le résultat (concordance ou non-concordance) est fournie en quelques secondes ou minutes, il peut s'écouler des semaines, voire des mois, avant de recevoir les données à caractère personnel correspondantes liées à la concordance.

[11] Le SIS aide les autorités compétentes de l'Union à maintenir la sécurité intérieure en l'absence de contrôles aux frontières intérieures, et le VIS permet aux États Schengen d'échanger des données sur les visas. Le système Eurodac est une base de données de l'Union contenant les empreintes digitales des demandeurs d'asile. Il permet aux États membres de comparer ces empreintes afin de déterminer si les demandeurs d'asile ont déjà demandé l'asile ou s'ils sont entrés dans l'Union de manière irrégulière en franchissant la frontière d'un autre État membre.

[12] L'EES et l'ETIAS contribueront à renforcer les contrôles de sécurité des voyageurs exemptés de l'obligation de visa, en permettant de procéder à des vérifications préalables en matière d'immigration irrégulière et de sécurité. L'ECRIS-TCN comblera les lacunes recensées dans l'échange d'informations entre les États membres sur les ressortissants de pays tiers condamnés.

[13] Règlement (UE) 2019/817 et règlement (UE) 2019/818.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La base juridique de la présente proposition est constituée des dispositions suivantes du traité sur le fonctionnement de l'Union européenne (TFUE): l'article 16, paragraphe 2, l'article 87, paragraphe 2, point a), et l'article 88, paragraphe 2.

En vertu de l'article 16, paragraphe 2, l'Union dispose du pouvoir d'adopter des mesures relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et les règles relatives à la libre circulation de ces données. En vertu de l'article 87, paragraphe 2, point a), l'Union a le pouvoir d'adopter des mesures portant sur la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes afin de garantir la coopération policière entre les autorités compétentes des États membres, y compris les services de police, les services des douanes et autres services répressifs spécialisés dans les domaines de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière. En vertu de l'article 88, paragraphe 2, le Parlement européen et le Conseil peuvent déterminer la structure, le fonctionnement, le domaine d'action et les tâches d'Europol.

• Subsidiarité

L'amélioration de l'échange d'informations entre les services de police et les services répressifs au sein de l'Union ne peut être réalisée de manière suffisante par les États membres agissant isolément, en raison du caractère transnational de la lutte contre la criminalité et des questions de sécurité. Les États membres doivent compter les uns sur les autres dans ces matières.

Par l'intermédiaire de plusieurs projets de mise en œuvre à l'échelon de l'Union[14], les États membres ont tenté de prendre des mesures afin de remédier aux lacunes du cadre Prüm actuellement en place[15]. Malgré toutes ces mesures, de nombreuses lacunes sont restées les mêmes que celles décrites dans le rapport de 2012 sur la mise en œuvre de la décision Prüm[16]. Les mesures mises en œuvre isolément par les États membres s'étant révélées insuffisantes pour remédier aux limites du cadre Prüm actuellement en place, une action de l'Union est nécessaire.

En outre, des règles, normes et exigences communes au niveau de l'Union facilitent les échanges d'informations, tout en garantissant la compatibilité entre les différents systèmes nationaux. Cela permet un certain niveau d'automatisation dans les flux d'échange d'informations qui libèrent les agents des services répressifs d'activités manuelles à forte intensité de main-d'œuvre.

---

[14] Par exemple, le projet «Mobile Competence Team» (2011-2014) avait été lancé par l'Allemagne et financé par le programme «Prévenir et combattre la criminalité» de la Commission. Ce projet visait à fournir des connaissances spécialisées et un soutien aux États membres de l'Union qui n'étaient pas encore opérationnels pour l'échange de données relatives aux profils ADN et aux empreintes digitales.

[15] Dans le cadre d'un projet dirigé par la Finlande, les États membres ont analysé les procédures nationales appliquées à la suite d'une concordance. Les auteurs du projet ont recommandé une série de bonnes pratiques et de pratiques non obligatoires afin de rationaliser l'échange d'informations à la suite d'une concordance dans toute l'Union (voir document 14310/2/16 REV2, non public).
En outre, Europol a soutenu en 2012-2013 l'élaboration de formulaires types à utiliser pour l'échange d'informations de suivi, indépendamment du canal de communication utilisé (voir document 9383/13 pour de plus amples informations). La mesure dans laquelle les points de contact nationaux utilisent ces formulaires n'est toutefois pas connue.

[16] COM (2012) 732 final.

- **Proportionnalité**

Comme l'explique de manière très détaillée l'analyse d'impact qui accompagne la présente proposition de règlement, les choix opérés dans la présente proposition sont considérés comme proportionnés. En effet, ils n'excèdent pas ce qui est nécessaire à la réalisation des objectifs fixés.

La proposition prévoit la création de **routeurs centraux** [le routeur Prüm II et le système d'index européen des registres de la police (EPRIS)] qui feraient chacun office de point de connexion entre les États membres. Il s'agit d'une approche hybride entre une solution décentralisée et une solution centralisée, sans qu'aucune donnée ne soit stockée au niveau central. Une telle approche impliquera que les bases de données nationales de chaque État membre seront toutes connectées au routeur central au lieu d'être connectées les unes aux autres. Ces routeurs serviraient de courtiers de messages qui transmettraient les opérations de recherche et les réponses aux systèmes nationaux, sans créer de nouveaux processus de traitement de données, élargir les droits d'accès ou remplacer les bases de données nationales. Cette approche permettrait aux services répressifs de disposer d'un accès rapide et contrôlé aux informations dont ils ont besoin pour s'acquitter de leurs tâches, conformément à leurs droits d'accès. Le routeur faciliterait la mise en œuvre par les États membres des échanges de données existants et futurs au titre du cadre Prüm.

L'**échange automatisé de catégories de données supplémentaires**, telles que des images faciales et des registres de la police, est crucial pour l'efficacité des enquêtes en matière pénale et pour l'identification des criminels. L'introduction de ces catégories de données supplémentaires n'entraînerait pas le stockage de nouvelles catégories de données, car les États membres les collectent déjà en vertu du droit national et les stockent dans des bases de données nationales. L'échange de ces nouvelles catégories de données constituerait un nouveau traitement de données. Il serait toutefois limité à la mesure nécessaire pour réaliser son objectif et il ne permettrait de comparer les données qu'au cas par cas. La proposition prévoit également un ensemble de garanties (par exemple, le partage de données complètes uniquement en cas de concordance à la suite d'une requête).

Grâce à la présente proposition, **Europol** fera partie intégrante du cadre Prüm, en premier lieu en permettant aux États membres de vérifier automatiquement les données biométriques obtenues auprès de pays tiers et détenues par Europol. En second lieu, Europol pourrait également vérifier les données obtenues auprès de pays tiers par rapport aux bases de données nationales des États membres. Ces deux aspects de la contribution d'Europol prévus dans le nouveau cadre Prüm, conformément aux missions d'Europol telles que définies dans le règlement (UE) 2016/794, garantiraient qu'aucune faille n'apparaisse en ce qui concerne les données relatives à la grande criminalité et au terrorisme reçues de pays tiers. Dans une société ouverte à l'ère de la mondialisation, les données fournies par les pays tiers sur les criminels et les terroristes sont cruciales. Elles permettraient l'identification potentielle de criminels connus de pays extérieurs à l'Union et bénéficieraient de solides garanties en matière de protection de la vie privée et des droits et libertés fondamentaux des personnes, établies dans les accords de coopération d'Europol avec des pays tiers.

La révision du **processus d'échange d'informations à la suite d'une concordance** contribuerait à la sécurité intérieure de l'Union européenne en simplifiant et en rationalisant l'échange d'informations en matière répressive. Par rapport à la situation actuelle où l'échange d'informations à la suite d'une concordance est régi par le droit national et est par conséquent soumis à des règles et procédures différentes, des règles communes harmonisant cette deuxième étape du processus de Prüm conféreraient une certaine prévisibilité à l'ensemble des utilisateurs, car tous sauraient quelles données ils obtiendraient à cette étape. L'échange de données serait facilité par une automatisation partielle, ce qui signifie qu'une intervention humaine serait encore nécessaire avant que tout échange de données de

suivi complet puisse avoir lieu. Les États membres conserveraient la propriété/le contrôle de leurs données.

- **Choix de l'instrument**

Un règlement du Parlement européen et du Conseil est proposé. La législation proposée repose sur un cadre existant de décisions du Conseil contribuant à la coopération transfrontière entre les États membres de l'Union dans les domaines de la justice et des affaires intérieures[17].

Compte tenu de la nécessité de rendre les mesures proposées directement applicables et de les appliquer uniformément dans tous les États membres, ainsi que de renforcer l'échange d'informations, un règlement est l'instrument juridique approprié.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluation ex post de la législation existante**

Dans l'ensemble, l'évaluation du cadre Prüm[18] a montré que la consultation et la comparaison des données relatives aux profils ADN, aux empreintes digitales et à l'immatriculation des véhicules figurant dans les bases de données des autres États membres, à des fins de prévention des infractions pénales et d'enquêtes en la matière, revêtent une importance capitale pour la préservation de la sécurité intérieure de l'Union et de la sûreté de ses citoyens. L'évaluation a également permis de démontrer que les décisions Prüm ont contribué à établir des règles, des normes et des exigences communes au niveau de l'Union, à faciliter l'échange d'informations et à garantir la compatibilité entre les différents systèmes nationaux.

Toutefois, depuis l'expiration du délai de mise en œuvre du cadre Prüm il y a dix ans, l'Union a adopté plusieurs autres mesures visant à faciliter l'échange d'informations entre les services répressifs[19], dont le cadre pour l'interopérabilité[20]. En outre, les dispositions relatives aux spécifications techniques des requêtes, aux mesures de sécurité et à la communication n'ont pas été mises à jour depuis l'adoption des décisions Prüm en 2008[21]. Certaines de ces règles sont devenues obsolètes, car la science et la technologie médico-légales ont considérablement évolué au cours de la dernière décennie.

Il ressort également de l'évaluation que la mise en œuvre des décisions Prüm au cours des dix dernières années a été lente et que tous les États membres n'ont pas pris les mesures nécessaires pour appliquer

---

17 Décision 2008/615/JAI du Conseil relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière; et décision 2008/616/JAI du Conseil concernant la mise en œuvre de la décision 2008/615/JAI.

18 Annexe 4 du document de travail des services de la Commission qui accompagne la présente proposition [référence de l'analyse d'impact du mécanisme de Prüm].

19 Comme le système d'information Europol (SIE), les systèmes d'information d'Interpol et le système d'information Schengen (SIS).

20 Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil;
règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816.

21 Contenues dans la décision 2008/616/JAI du Conseil.

lesdites décisions[22]. En conséquence, un certain nombre de connexions bilatérales n'ont pas été établies et il est impossible d'interroger les bases de données de certains États membres. Les résultats de l'évaluation ont également montré que la suite donnée aux concordances repose sur le droit national et ne relève par conséquent pas du champ d'application des décisions Prüm. Les différences entre les règles et procédures nationales peuvent entraîner, dans plusieurs cas, des délais importants avant que les autorités compétentes ne reçoivent des informations à la suite d'une concordance. Cet état de fait nuit au fonctionnement du mécanisme de Prüm ainsi qu'à l'échange efficace d'informations entre les États membres en diminuant la possibilité d'identifier les criminels et de détecter les liens transfrontaliers entre les infractions.

Les résultats de l'évaluation ont permis d'élaborer l'analyse d'impact et la présente proposition.

- **Consultation des parties intéressées**

L'élaboration de la présente proposition a nécessité des consultations ciblées des parties intéressées concernées, y compris des utilisateurs finaux du système, à savoir les autorités des États membres qui utilisent l'échange automatisé de données dans le cadre du mécanisme de Prüm, qu'il s'agisse des services répressifs et judiciaires, des autorités nationales chargées de l'immatriculation des véhicules, des dépositaires des bases de données nationales ou des laboratoires de police scientifique. L'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) ont également été consultées en raison de leur expertise respective et de leur rôle potentiel dans le nouveau cadre Prüm.

L'Agence des droits fondamentaux de l'Union européenne (FRA), ainsi que des organisations non gouvernementales telles qu'EDRi (European Digital Rights) et des organisations intergouvernementales (Eucaris; système d'information européen concernant les véhicules et les permis de conduire) ont également apporté une contribution en fonction de leur expertise.

Les activités de consultation menées dans le cadre de la réalisation de l'analyse d'impact qui sous-tend la présente proposition ont permis de recueillir les avis des parties intéressées dans divers forums. Ces activités comprenaient notamment une analyse d'impact initiale, une consultation publique et une série d'ateliers techniques. Une étude de faisabilité a été réalisée sur la base de recherches documentaires, d'entretiens avec des experts en la matière, de questionnaires et de trois ateliers d'experts. Elle portait sur la possibilité d'améliorer l'échange d'informations dans le cadre des décisions Prüm.

Des discussions régulières sur l'échange d'informations entre les services répressifs et plus particulièrement sur les décisions Prüm au sein des groupes de travail DAPIX et IXIM[23] du Conseil ont également contribué à l'élaboration de la présente proposition.

Une **analyse d'impact initiale** a été publiée en vue de recueillir les avis des parties intéressées entre août et octobre 2020. Au total, six contributions ont été reçues[24].

---

[22] La Commission a lancé des procédures d'infraction à l'encontre de cinq États membres en 2016. En octobre 2021, deux de ces procédures d'infraction étaient toujours en cours.

[23] Groupe de travail «Protection des données» (DAPIX) du Conseil et, à partir du 1er janvier 2020, groupe de travail sur l'échange d'informations dans le domaine de la justice et des affaires intérieures (IXIM).

[24] L'analyse d'impact initiale et les contributions sont disponibles ici.

Une **consultation publique** annoncée sur le site internet de la Commission européenne ciblait le grand public. Les réponses ont confirmé l'utilité du cadre Prüm actuellement en place pour la prévention des infractions pénales et les enquêtes en la matière et le fait que ledit cadre a également permis d'améliorer l'échange de données entre les services répressifs des États membres. En évitant de devoir interroger chaque État membre de manière bilatérale, l'échange automatisé de données au titre du cadre Prüm a également permis de gagner en efficacité. Les réponses ont en outre confirmé la cohérence du cadre avec les actions menées dans ce domaine au niveau de l'Union et au niveau international, ainsi que sa valeur ajoutée par rapport à ce que les États membres pourraient réaliser dans le domaine de l'échange d'informations en matière répressive en l'absence du cadre Prüm. En ce qui concerne le renforcement du cadre actuel, la plupart des répondants ont convenu que le fait que certaines catégories de données ne soient pas couvertes par ledit cadre et soient par conséquent échangées par l'envoi de requêtes manuelles constitue une faiblesse.

Les services de la Commission ont également organisé une série d'**ateliers techniques** informels ciblés avec des experts des États membres et des pays associés à l'espace Schengen. Ces ateliers visaient à réunir les utilisateurs finaux pour un échange de vues sur les options envisagées et évaluées afin de renforcer le cadre Prüm sur le plan technique.

L'analyse d'impact qui accompagne la présente proposition contient une description plus détaillée de la consultation des parties intéressées (annexe 2).

- **Analyse d'impact**

La présente proposition s'appuie sur une analyse d'impact, présentée dans le document de travail des services de la Commission qui l'accompagne [référence de l'analyse d'impact du mécanisme de Prüm]. Le comité d'examen de la réglementation a examiné le projet d'analyse d'impact lors de sa réunion du 14 juillet 2021 et a émis un avis favorable le 16 juillet 2021.

L'analyse d'impact a conclu ce qui suit:

(1) pour réaliser l'objectif visant à fournir une solution technique permettant un échange automatisé efficace de données, il convient d'appliquer une solution hybride entre une approche décentralisée et une approche centralisée, sans qu'aucune donnée ne soit stockée au niveau central;

(2) pour réaliser l'objectif visant à faire en sorte que les services répressifs disposent d'un plus grand nombre de données pertinentes (sur le plan des catégories de données), il convient d'introduire l'échange d'images faciales et de registres de la police;

(3) pour réaliser l'objectif visant à faire en sorte que les données pertinentes provenant des bases de données d'Europol soient mises à la disposition des services répressifs, les États membres devraient être en mesure de vérifier automatiquement les données biométriques obtenues auprès de pays tiers au sein d'Europol, au titre du cadre Prüm. Europol devrait également être en mesure de vérifier les données obtenues auprès de pays tiers par rapport aux bases de données nationales des États membres;

(4) pour réaliser l'objectif visant à fournir un accès efficace aux données réelles correspondant à une concordance qui sont disponibles dans la base de données nationale d'un autre État membre ou au sein d'Europol, le processus de suivi devrait être réglementé au niveau de l'Union par un échange semi-automatique des données réelles correspondant à une concordance.

L'incidence positive majeure de la présente proposition sera de répondre efficacement aux problèmes cernés et de renforcer le cadre Prüm actuellement en place avec des capacités supplémentaires ciblées et solides afin d'intensifier son soutien aux États membres dans le renforcement de l'échange d'informations, l'objectif final étant de prévenir les infractions pénales et terroristes et d'enquêter sur celles-ci, dans le plein respect des droits fondamentaux.

Les bénéficiaires ultimes de toutes les options privilégiées sont les citoyens, qui profiteront directement et indirectement d'une meilleure lutte contre la criminalité et d'une baisse des taux de criminalité. Sur le plan de l'efficience, les principaux bénéficiaires sont les services répressifs nationaux.

Les incidences financières et économiques immédiates de la proposition nécessiteront des investissements tant au niveau de l'Union qu'au niveau des États membres. Les coûts d'investissement prévus devraient être compensés par des avantages et des économies, notamment au niveau des États membres. Malgré les investissements initiaux, la création du routeur central Prüm permettra aux États membres de réaliser des économies, car celui-ci n'obligera pas chaque État membre à créer (et à maintenir) autant de connexions qu'il y a d'États membres et de catégories de données.

- **Droits fondamentaux**

Conformément à la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), que les institutions de l'Union et les États membres doivent respecter lorsqu'ils appliquent le droit de l'Union (article 51, paragraphe 1, de la charte), et au principe de non-discrimination, les possibilités offertes par les options présentées doivent être mises en balance avec l'obligation de garantir que les atteintes aux droits fondamentaux qui peuvent découler de celles-ci se limitent à ce qui est strictement nécessaire afin d'atteindre effectivement les objectifs d'intérêt général poursuivis, sous réserve du principe de proportionnalité (article 52, paragraphe 1, de la charte).

Les solutions proposées donnent la possibilité d'adopter des mesures préventives ciblées afin d'améliorer la sécurité. Elles peuvent ainsi contribuer à la poursuite de l'objectif légitime visant à faciliter la lutte contre la criminalité, qui implique également que les autorités ont l'obligation positive d'adopter des mesures opérationnelles préventives afin de protéger toute personne dont la vie serait en péril, si elles ont ou devraient avoir connaissance de l'existence d'un risque immédiat[25].

- **Protection des données à caractère personnel**

L'échange d'informations a une incidence sur le droit à la protection des données à caractère personnel. L'article 8 de la charte, l'article 16 du traité sur le fonctionnement de l'Union européenne et l'article 8 de la convention européenne des droits de l'homme ont consacré ce droit. Ainsi que l'a souligné la Cour de justice de l'Union européenne[26], le droit à la protection des données à caractère personnel n'apparaît pas comme une prérogative absolue, mais doit être pris en considération par rapport à sa fonction dans la société. La protection des données est étroitement liée au respect de la vie privée et familiale, protégé par l'article 7 de la charte.

En ce qui concerne le mécanisme de Prüm, la législation applicable en matière de protection des données est la directive (UE) 2016/680. En effet, le cadre Prüm prévoit le traitement de données à

[25] Cour européenne des droits de l'homme, Osman c. Royaume-Uni, nº 87/1997/871/1083, 28 octobre 1998, point 116.

[26] Arrêt de la Cour de justice de l'Union européenne du 9 novembre 2010 dans les affaires jointes C-92/09 et C93/09, Volker und Markus Schecke et Eifert, [2010] Recueil I-0000.

caractère personnel effectué dans le cadre de l'échange d'informations entre les services répressifs chargés de la prévention des infractions pénales et des enquêtes en la matière.

La libre circulation des données au sein de l'Union ne doit pas être limitée pour des motifs liés à la protection des données. Une série de principes doivent toutefois être respectés. En effet, pour être légale, toute limitation de l'exercice des droits fondamentaux protégés par la charte doit être conforme aux critères suivants, prévus par l'article 52, paragraphe 1, de la charte:

(1) elle doit être prévue par la loi;

(2) elle doit respecter le contenu essentiel des droits;

(3) elle doit répondre effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui;

(4) elle doit être nécessaire; et

(5) elle doit être proportionnée.

La présente proposition est conforme à toutes ces règles en matière de protection des données, comme l'explique en détail l'analyse d'impact qui l'accompagne. La proposition est fondée sur les principes de la protection des données dès la conception et par défaut. Elle inclut toutes les dispositions appropriées limitant le traitement des données à ce qui est nécessaire à son objectif spécifique et n'accordant l'accès aux données qu'aux entités qui ont «besoin d'en connaître». L'accès aux données est exclusivement réservé aux membres du personnel dûment autorisés des autorités des États membres ou des organes de l'Union compétents aux fins spécifiques du cadre Prüm révisé et sa portée est limitée aux informations nécessaires pour l'exécution des missions conformément à ces fins.

Au moment de la publication du rapport évaluant les effets donnés à la [recommandation du Conseil relative à la coopération policière opérationnelle] par les États membres, visé au point 9) d) de ladite recommandation, la Commission décidera s'il est nécessaire d'adopter une législation de l'UE en matière de coopération policière opérationnelle transfrontière. Si une telle législation s'avérait nécessaire, la Commission présentera une proposition législative relative à la coopération policière opérationnelle transfrontière, qui assurera également l'alignement des dispositions de la décision 2008/615/JAI et de la décision 2008/616/JAI non couvertes par la présente proposition sur la directive 2016/680, conformément aux résultats de l'évaluation au titre de l'article 62, paragraphe 6, de la directive 2016/680. Si une législation de l'UE en matière de coopération policière opérationnelle transfrontière n'est pas nécessaire, la Commission présentera une proposition législative visant à assurer ce même alignement, conformément aux résultats de l'évaluation au titre de l'article 62, paragraphe 6, de la directive 2016/680.

4. INCIDENCE BUDGÉTAIRE

La présente initiative législative aurait une incidence sur le budget et les besoins en personnel de l'eu-LISA et d'Europol.

S'agissant de l'eu-LISA, selon les estimations, un budget supplémentaire d'environ 16 millions d'EUR et approximativement 10 postes supplémentaires seraient nécessaires pour l'ensemble de la période du cadre financier pluriannuel (CFP) afin de s'assurer que l'Agence dispose des ressources nécessaires pour exécuter les tâches qui lui sont attribuées dans la présente proposition de règlement. Le budget alloué à l'eu-LISA sera déduit de l'IGFV.

S'agissant d'Europol, selon les estimations, un budget supplémentaire d'environ 7 millions d'EUR et approximativement 5 postes supplémentaires seraient nécessaires pour l'ensemble de la période du CFP afin de s'assurer que l'Agence dispose des ressources nécessaires pour exécuter les tâches qui lui sont attribuées dans la présente proposition de règlement. Le budget alloué à Europol sera déduit du FSI.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

La Commission veillera à ce que les dispositions nécessaires soient en place pour contrôler le fonctionnement des mesures proposées et les évaluer au regard des principaux objectifs stratégiques. Deux ans après la création et la mise en service des nouvelles fonctionnalités, puis tous les deux ans par la suite, les agences de l'Union devraient présenter au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique des nouvelles mesures proposées. De plus, trois ans après la création et la mise en service des nouvelles fonctionnalités, puis tous les quatre ans par la suite, la Commission devrait produire une évaluation globale des mesures, notamment en ce qui concerne l'incidence directe ou indirecte sur les droits fondamentaux. Cette évaluation devrait examiner les résultats obtenus par rapport aux objectifs, déterminer si les principes de base restent valables et en tirer toutes les conséquences pour les options futures. La Commission devrait présenter les rapports d'évaluation au Parlement européen et au Conseil.

- **Explication détaillée des différentes dispositions de la proposition**

Le chapitre 1 énonce les dispositions générales du présent règlement, notamment son objet, son but et son champ d'application. Il fournit une liste de définitions et rappelle que le traitement des données à caractère personnel aux fins du présent règlement respecte le principe de non-discrimination et d'autres droits fondamentaux.

Le chapitre 2 énonce les dispositions relatives à l'échange des catégories de données au titre du présent règlement, à savoir l'échange de profils ADN, de données dactyloscopiques, de données relatives à l'immatriculation des véhicules, d'images faciales et de registres de la police. Les principes régissant l'échange, la consultation automatisée de données ainsi que les règles relatives aux demandes et aux réponses sont détaillés dans une section distincte pour chaque catégorie de données respectivement. Le chapitre 2 contient également des dispositions communes relatives à l'échange de données, à la création de points de contact nationaux et à la mesure d'exécution.

Le chapitre 3 présente les détails de la nouvelle architecture (technique) de l'échange de données. La première section de ce chapitre comprend des dispositions décrivant le routeur central, l'utilisation du routeur et le lancement des requêtes. Des actes d'exécution seront nécessaires pour préciser les procédures techniques de ces requêtes. Cette section comprend également des dispositions sur l'interopérabilité entre le routeur et le répertoire commun de données d'identité aux fins de l'accès des services répressifs, la tenue de registres pour toutes les opérations de traitement de données dans le routeur, le contrôle de la qualité et les procédures de notification en cas d'impossibilité technique d'utiliser le routeur. Une seconde section fournit des précisions sur l'utilisation du système d'index européen des registres de la police (EPRIS) pour l'échange de registres de la police. Cette section comprend également des dispositions relatives à la tenue de registres pour toutes les opérations de traitement de données effectuées dans l'EPRIS et aux procédures de notification en cas d'impossibilité technique d'utiliser l'EPRIS.

Le chapitre 4 présente les processus d'échange de données à la suite d'une correspondance. Il comprend une disposition relative à l'échange automatisé de données de base, les données étant limitées à ce qui est nécessaire pour permettre l'identification de la personne concernée, et une

disposition relative à l'échange de données à tout stade du processus au titre du présent règlement qui n'est pas explicitement décrit dans le présent règlement.

Le chapitre 5 contient des dispositions sur l'accès des États membres aux données biométriques obtenues auprès de pays tiers et stockées par Europol et sur l'accès d'Europol aux données stockées dans les bases de données des États membres.

Le chapitre 6 sur la protection des données contient des dispositions garantissant que les données relevant du présent règlement sont traitées de manière légale et appropriée, conformément aux dispositions 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[27]. Il explique qui sera le sous-traitant pour le traitement des données en vertu du présent règlement. Il énonce les mesures que l'eu-LISA et les autorités des États membres doivent prendre pour garantir la sécurité du traitement des données, le traitement approprié des incidents de sécurité et le contrôle du respect des mesures prévues par le présent règlement. Ce chapitre établit également des dispositions concernant le contrôle et l'audit en lien avec la protection des données. Il souligne le principe selon lequel les données traitées en vertu du présent règlement ne doivent pas être transférées ou mises à la disposition d'un pays tiers ou d'une organisation internationale de manière automatisée.

Le chapitre 7 détaille les responsabilités respectives des États membres, d'Europol et de l'eu-LISA dans la mise en œuvre des mesures prévues par le présent règlement.

Le chapitre 8 porte sur les modifications apportées aux autres instruments existants, à savoir les décisions 2008/615/JAI et 2008/616/JAI, le règlement (UE) 2018/1726, le règlement (UE) 2019/817 et le règlement (UE) 2019/818.

Le chapitre 9, relatif aux dispositions finales, porte sur l'établissement de rapports et de statistiques, les coûts, les notifications, les dispositions transitoires et les dérogations. Il définit également les exigences relatives à la mise en œuvre initiale des mesures proposées par le présent règlement. Le chapitre prévoit également la création d'un comité et l'adoption d'un manuel pratique pour soutenir la mise en œuvre et la gestion du présent règlement. Il comprend également une disposition sur le suivi et l'évaluation et une disposition sur l'entrée en vigueur et l'applicabilité du présent règlement. Le présent règlement remplace notamment les articles 2 à 6 et les sections 2 et 3 du chapitre 2 de la décision 2008/615/JAI du Conseil, ainsi que les chapitres 2 à 5 et les articles 18, 20 et 21 de la décision 2008/616/JAI du Conseil, qui seront donc supprimés de ces décisions du Conseil à compter de la date d'application du présent règlement. Ces modifications auront pour effet que les dispositions remplacées et supprimées ne s'appliquent plus à aucun État membre.

[27] À la suite des conclusions de la Commission dans sa communication du 24 juin 2020 sur la marche à suivre en ce qui concerne la mise en conformité de l'acquis de l'ancien troisième pilier avec les règles en matière de protection des données [COM(2020) 262 final].

2021/0410 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16, paragraphe 2, son article 87, paragraphe 2, point a), et son article 88, paragraphe 2,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[28],

vu l'avis du Comité des régions[29],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) L'Union s'est donné pour objectif d'offrir à ses citoyens un espace de liberté, de sécurité et de justice sans frontières intérieures, au sein duquel est assurée la libre circulation des personnes. Cet objectif devrait être réalisé au moyen, entre autres, de mesures appropriées visant à prévenir et à lutter contre la criminalité, y compris la criminalité organisée et le terrorisme.

(2) Cet objectif exige que les services répressifs échangent des données, de manière efficace et en temps utile, afin de lutter efficacement contre la criminalité.

(3) Par conséquent, l'objectif du présent règlement est d'améliorer, de rationaliser et de faciliter l'échange d'informations en matière pénale entre les services répressifs des États membres, mais aussi avec l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) instituée par le règlement (UE) 2016/794 du Parlement européen et du Conseil[30] en tant que plateforme centrale d'information sur la criminalité dans l'Union.

(4) En prévoyant le transfert automatisé des profils ADN, des données dactyloscopiques et de certaines données relatives à l'immatriculation des véhicules, les décisions 2008/615/JAI[31]

[28] JO C du , p. .

[29] JO C du , p. .

[30] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

[31] Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 1).

et 2008/616/JAI[32] du Conseil établissant des règles relatives à l'échange d'informations entre les services chargés de la prévention des infractions pénales et des enquêtes en la matière se sont avérées importantes pour lutter contre le terrorisme et la criminalité transfrontalière.

(5) Le présent règlement devrait fixer les conditions et les procédures de transfert automatisé des profils ADN, des données dactyloscopiques, des données relatives à l'immatriculation des véhicules, des images faciales et des registres de la police. Cela devrait être sans préjudice du traitement de ces données dans le système d'information Schengen (SIS) ou de l'échange d'informations supplémentaires les concernant par l'intermédiaire des bureaux Sirene ou des droits des personnes dont les données sont traitées dans ce système.

(6) Le traitement de données à caractère personnel et l'échange de données à caractère personnel aux fins du présent règlement ne devraient donner lieu à aucune discrimination à l'encontre des personnes, quel qu'en soit le motif. Ils devraient respecter pleinement la dignité humaine, l'intégrité des personnes et d'autres droits fondamentaux, notamment le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, conformément à la charte des droits fondamentaux de l'Union européenne.

(7) En prévoyant la consultation ou la comparaison automatisée de profils ADN, de données dactyloscopiques, de données relatives à l'immatriculation des véhicules, d'images faciales et de registres de la police, le présent règlement a également pour objet de permettre la recherche de personnes disparues et de restes humains non identifiés. Cela devrait être sans préjudice de l'introduction dans le SIS de signalements de personnes disparues et de l'échange d'informations supplémentaires sur ces signalements en vertu du règlement (UE) 2018/1862 du Parlement européen et du Conseil[33].

(8) La directive (UE) .../... [*relative à l'échange d'informations entre les services répressifs des États membres*] fournit un cadre juridique cohérent de l'Union afin de garantir que les services répressifs disposent d'un accès équivalent aux informations détenues par les autres États membres lorsqu'ils en ont besoin pour lutter contre la criminalité et le terrorisme. Afin que l'échange d'informations soit intensifié, cette directive formalise les procédures de partage d'informations entre États membres, notamment à des fins d'enquêtes, y compris le rôle du «point de contact unique» pour cet échange, en faisant pleinement usage de l'application de réseau d'échange sécurisé d'informations d'Europol, SIENA. Tout échange d'informations allant au-delà de ce qui est prévu par le présent règlement devrait être régi par la directive (UE) .../... [*relative à l'échange d'informations entre les services répressifs des États membres*].

(9) En ce qui concerne la consultation automatisée de données relatives à l'immatriculation des véhicules, les États membres devraient utiliser le système d'information européen concernant les véhicules et les permis de conduire (Eucaris) créé par le traité sur un système d'information européen concernant les véhicules et les permis de conduire (traité EUCARIS) et conçu à cet effet. Eucaris devrait connecter tous les États membres participants dans un réseau. Aucun

[32] Décision 2008/616/JAI du Conseil du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 12).

[33] Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

élément central n'est nécessaire pour établir la communication, chaque État membre communiquant directement avec les autres États membres connectés.

(10) L'identification d'un criminel est essentielle pour mener à bien des enquêtes et des poursuites en matière pénale. La consultation automatisée d'images faciales de suspects et de criminels reconnus coupables devrait fournir des informations supplémentaires permettant d'identifier les criminels et de lutter contre la criminalité.

(11) La consultation ou la comparaison automatisée de données biométriques (profils ADN, données dactyloscopiques et images faciales) entre les autorités chargées de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière en vertu du présent règlement ne devrait concerner que les données contenues dans les bases de données établies aux fins de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière.

(12) La participation à l'échange de registres de la police devrait rester volontaire. Lorsque les États membres décident de participer, dans un esprit de réciprocité, il ne devrait pas leur être possible d'interroger les bases de données des autres États membres s'ils ne mettent pas leurs propres données à la disposition de ceux-ci.

(13) Ces dernières années, Europol a reçu de plusieurs pays tiers un grand nombre de données biométriques de terroristes et de criminels présumés ou reconnus coupables. L'intégration dans le cadre Prüm des données obtenues auprès de pays tiers et stockées au sein d'Europol, et, partant, la mise à disposition des services répressifs de ces données sont nécessaires pour améliorer la prévention des infractions pénales et les enquêtes en la matière. Elles contribuent également à créer des synergies entre les différents outils de répression.

(14) Europol devrait pouvoir consulter les bases de données des États membres au titre du cadre Prüm à partir des données reçues de pays tiers afin d'établir des liens transfrontaliers entre les affaires pénales. La possibilité d'utiliser les données au titre du cadre Prüm, parallèlement à d'autres bases de données dont dispose Europol, devrait permettre d'établir une analyse plus complète et plus éclairée en matière d'enquêtes pénales et permettre à Europol d'apporter un meilleur soutien aux services répressifs des États membres. En cas de correspondance entre les données utilisées pour la consultation et les données détenues dans les bases de données des États membres, ces derniers peuvent fournir à Europol les informations nécessaires à l'accomplissement de ses missions.

(15) Les décisions 2008/615/JAI et 2008/616/JAI prévoient un réseau de connexions bilatérales entre les bases de données nationales des États membres. En conséquence de cette architecture technique, chaque État membre devrait établir au moins 26 connexions, c'est-à-dire une connexion avec chaque État membre, par catégorie de données. Le routeur et le système d'index européen des registres de la police (EPRIS) établis par le présent règlement devraient simplifier l'architecture technique du cadre Prüm et servir de points de connexion entre tous les États membres. Le routeur devrait exiger une connexion unique par État membre en ce qui concerne les données biométriques, et l'EPRIS devrait exiger une connexion unique par État membre en ce qui concerne les registres de la police.

(16) Le routeur devrait être connecté au portail de recherche européen créé par l'article 6 du règlement (UE) 2019/817 du Parlement européen et du Conseil[34] et l'article 6 du

[34] Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les

règlement (UE) 2019/818 du Parlement européen et du Conseil[35] afin de permettre aux autorités des États membres et à Europol d'interroger les bases de données nationales au titre du présent règlement simultanément aux requêtes introduites dans le répertoire commun de données d'identité établi par l'article 17 du règlement (UE) 2019/817 et l'article 17 du règlement (UE) 2019/818 à des fins répressives.

(17) En cas de correspondance entre les données utilisées pour la consultation ou la comparaison et les données détenues dans la base de données nationale de l'État membre ou des États membres requis, et après confirmation de cette correspondance par l'État membre requérant, l'État membre requis devrait renvoyer un ensemble limité de données de base par l'intermédiaire du routeur dans les 24 heures. Ce délai garantirait un échange rapide de communications entre les autorités des États membres. Les États membres devraient conserver le contrôle de la communication de cet ensemble limité de données de base. Un certain degré d'intervention humaine devrait être maintenu aux points clés du processus, y compris pour la décision de communiquer des données à caractère personnel à l'État membre requérant, afin de garantir qu'il n'y aurait pas d'échange automatisé de données de base.

(18) Tout échange entre les autorités des États membres ou avec Europol à un stade quelconque de l'un des processus décrits dans le présent règlement, qui n'est pas explicitement décrit dans le présent règlement, devrait avoir lieu par l'intermédiaire de l'application SIENA afin de garantir que l'ensemble des États membres utilisent un canal de communication commun, sûr et fiable.

(19) La norme de format universel pour les messages (UMF) devrait être utilisée pour le développement du routeur et de l'EPRIS. Tout échange automatisé de données conformément au présent règlement devrait utiliser la norme UMF. Les autorités des États membres et Europol sont encouragés à également utiliser la norme UMF pour tout autre échange de données entre eux dans le cadre du mécanisme de Prüm II. La norme UMF devrait servir en tant que norme pour l'échange d'informations transfrontière structuré entre les systèmes d'information, les autorités ou les organismes dans le domaine de la justice et des affaires intérieures.

(20) Seules les informations non classifiées devraient être échangées dans le cadre du mécanisme de Prüm II.

(21) Certains aspects du mécanisme de Prüm II ne peuvent pas être couverts de manière exhaustive par le présent règlement en raison de leur nature technique, de leur niveau élevé de précision et de leur nature sujette à de fréquents changements. Ces aspects comprennent, par exemple, les dispositions et spécifications techniques pour les procédures de consultation automatisée, les normes d'échange de données et les éléments de données à échanger. Afin de garantir des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil[36].

---

règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil (JO L 135 du 22.5.2019, p. 27).

[35] Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 (JO L 135 du 22.5.2019, p. 85).

[36] Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(22) Étant donné que le présent règlement prévoit l'établissement du nouveau cadre Prüm, il convient de supprimer les dispositions pertinentes des décisions 2008/615/JAI et 2008/616/JAI. Il convient dès lors de modifier lesdites décisions en conséquence.

(23) Étant donné que le routeur devrait être développé et géré par l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) instituée par le règlement (UE) 2018/1726 du Parlement européen et du Conseil[37], il est nécessaire de modifier ledit règlement en ajoutant ces deux missions au mandat de l'eu-LISA. Afin de permettre la connexion du routeur au portail de recherche européen pour pouvoir consulter simultanément le routeur et le répertoire commun de données d'identité, il est donc nécessaire de modifier le règlement (UE) 2019/817. Afin de permettre la connexion du routeur au portail de recherche européen pour pouvoir consulter simultanément le routeur et le répertoire commun de données d'identité et afin de stocker les rapports et les statistiques du routeur dans le répertoire commun des rapports et statistiques, il est donc nécessaire de modifier le règlement (UE) 2019/818. Il convient dès lors de modifier lesdits règlements en conséquence.

(24) Conformément aux articles 1er et 2 du protocole nº 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption du présent règlement et n'est pas lié par celle-ci ni soumis à son application.

(25) [Conformément à l'article 3 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande a notifié son souhait de participer à l'adoption et à l'application du présent règlement.] OU [Conformément aux articles 1er et 2 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande ne participe pas à l'adoption du présent règlement et n'est pas liée par celui-ci ni soumise à son application.]

(26) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil[38] et a rendu un avis le [XX][39],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE 1

DISPOSITIONS GÉNÉRALES

---

[37] Règlement (UE) 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), modifiant le règlement (CE) nº 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) nº 1077/2011 (JO L 295 du 21.11.2018, p. 99).

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

[39] [JO C …].

Article premier

Objet

Le présent règlement établit un cadre pour l'échange d'informations entre les autorités chargées de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière (mécanisme de Prüm II).

Le présent règlement fixe les conditions et les procédures applicables à la consultation automatisée de profils ADN, de données dactyloscopiques, d'images faciales, de registres de la police et de certaines données relatives à l'immatriculation des véhicules, ainsi que les règles relatives à l'échange de données de base à la suite d'une correspondance.

Article 2

Objectif

Le mécanisme de Prüm II a pour objet d'approfondir la coopération transfrontière dans les matières relevant de la partie III, titre V, chapitre 5, du traité sur le fonctionnement de l'Union européenne, notamment l'échange d'informations entre les autorités chargées de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière.

Le mécanisme de Prüm II a également pour objet de permettre la recherche de personnes disparues et de restes humains non identifiés par les autorités chargées de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière.

Article 3

Champ d'application

Le présent règlement s'applique aux bases de données nationales utilisées pour le transfert automatisé des catégories de profils ADN, de données dactyloscopiques, d'images faciales, de registres de la police et de certaines données relatives à l'immatriculation des véhicules.

Article 4

Définitions

Aux fins du présent règlement, on entend par:

(1) «loci»: la structure moléculaire particulière issue de divers segments d'ADN;

(2) «profil ADN: un code alphanumérique qui représente un ensemble de caractéristiques d'identification de la partie non codante d'un échantillon d'ADN humain analysé, c'est-à-dire la structure moléculaire particulière issue de divers segments d'ADN (loci);

(3) «partie non codante de l'ADN»: les régions chromosomiques non génétiquement exprimées, c'est-à-dire non connues pour fournir des propriétés fonctionnelles d'un organisme;

(4) «données indexées ADN»: un profil ADN et la référence visée à l'article 9;

(5) «profil ADN de référence»: le profil ADN d'une personne identifiée;

(6) «profil ADN non identifié»: le profil ADN obtenu à partir de traces recueillies lors d'une enquête pénale et appartenant à une personne non encore identifiée;

(7) «données dactyloscopiques»: les images d'empreintes digitales, images d'empreintes digitales latentes, d'empreintes de paumes de mains, d'empreintes de paumes de mains latentes, ainsi

que des modèles de telles images (points caractéristiques codés), lorsqu'ils sont stockés et traités dans une base de données automatisée;

(8) «données indexées dactyloscopiques»: les données dactyloscopiques et la référence visée à l'article 14;

(9) «cas par cas»: un dossier d'enquête unique;

(10) «image faciale»: une image numérique du visage;

(11) «données biométriques»: les profils ADN, les données dactyloscopiques ou les images faciales;

(12) «correspondance»: l'existence d'une correspondance résultant d'une comparaison automatisée entre les données à caractère personnel enregistrées ou en cours d'enregistrement dans un système d'information ou dans une base de données;

(13) «candidat»: les données avec lesquelles une correspondance a été établie;

(14) «État membre requérant»: l'État membre qui effectue une consultation par l'intermédiaire du mécanisme de Prüm II;

(15) «État membre requis»: l'État membre dont les bases de données sont consultées par l'État membre requérant par l'intermédiaire du mécanisme de Prüm II;

(16) «registres de la police»: toutes les informations disponibles dans le ou les registres nationaux qui contiennent les données des autorités compétentes à des fins de prévention et de détection des infractions pénales ainsi que d'enquêtes en la matière;

(17) «pseudonymisation»: le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

(18) «données d'Europol»: toutes les données à caractère personnel traitées par Europol conformément au règlement (UE) 2016/794;

(19) «autorité de contrôle»: une autorité publique indépendante instituée par un État membre en vertu de l'article 41 de la directive (UE) 2016/680 du Parlement européen et du Conseil[40];

(20) «application SIENA»: l'application de réseau d'échange sécurisé d'informations, gérée par Europol, destinée à faciliter l'échange d'informations entre les États membres et Europol;

(21) «incident important»: tout incident, sauf s'il a une incidence limitée et s'il est susceptible d'être déjà bien appréhendé en ce qui concerne la méthode ou la technologie à employer;

(22) «menace informatique importante»: une menace informatique ayant l'intention, la possibilité et la capacité de provoquer un incident important;

[40] 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 (JO L 119 du 4.5.2016, p. 89).

(23) «vulnérabilité importante»: une vulnérabilité qui entraînera probablement un incident important si elle est exploitée;

(24) «incident»: un incident au sens de l'article 4, paragraphe 5, de la directive (UE) .../... du Parlement européen et du Conseil[41] [*proposition SRI 2*].

CHAPITRE 2

ÉCHANGE DE DONNÉES

SECTION 1

Profils ADN

Article 5

Création de fichiers nationaux d'analyses ADN

1. Les États membres créent et conservent des fichiers nationaux d'analyses ADN aux fins des enquêtes en matière d'infractions pénales.

Le traitement des données conservées dans ces fichiers en vertu du présent règlement s'effectue conformément au droit national des États membres applicable au traitement de ces données.

2. Les États membres s'assurent de la disponibilité des données indexées ADN provenant de leurs fichiers nationaux d'analyses ADN visés au paragraphe 1.

Les données indexées ADN ne contiennent aucune donnée permettant l'identification directe de la personne concernée.

Les données indexées ADN qui ne peuvent être rattachées à aucune personne (profils ADN non identifiés) doivent être reconnaissables en tant que telles.

Article 6

Consultation automatisée de profils ADN

1. Les États membres autorisent les points de contact nationaux visés à l'article 29 et Europol à accéder aux données indexées ADN contenues dans leurs fichiers d'analyses ADN, afin qu'ils puissent procéder à des consultations automatisées par comparaison de profils ADN aux fins d'enquêtes en matière d'infractions pénales.

La consultation n'est possible que cas par cas et dans le respect du droit national de l'État membre requérant.

2. Si une consultation automatisée révèle une correspondance entre un profil ADN transmis et les profils ADN enregistrés dans le fichier consulté de l'État membre requis, le point de contact national de l'État membre requérant reçoit de manière automatisée les données indexées ADN pour lesquelles une correspondance a été mise en évidence.

[41] Directive (UE) .../... du Parlement européen et du Conseil du … (JO...).

S’il n’y a pas de correspondance, l’État membre requérant en est informé de manière automatisée.

3. Le point de contact national de l’État membre requérant confirme l’existence d’une correspondance entre les données de profils ADN et les données indexées ADN détenues par l’État membre requis après la transmission automatisée des données indexées ADN nécessaires à la confirmation d’une correspondance.

Article 7

Comparaison automatisée de profils ADN non identifiés

1. Aux fins d’enquêtes en matière d’infractions pénales, les États membres peuvent, par l’intermédiaire de leurs points de contact nationaux, comparer les profils ADN non identifiés avec tous les profils ADN provenant des autres fichiers nationaux d’analyses ADN. La transmission et la comparaison des profils se font de manière automatisée.

2. Si la comparaison visée au paragraphe 1 permet à un État membre requis de mettre en évidence une correspondance entre des profils ADN transmis et le contenu de ses propres fichiers d’analyses ADN, ledit État membre communique sans délai au point de contact national de l’État membre requérant les données indexées ADN pour lesquelles une correspondance a été mise en évidence.

3. La confirmation de l’existence d’une correspondance entre les données de profils ADN et les données indexées ADN détenues par l’État membre requis est établie par le point de contact national de l’État membre requérant après la transmission automatisée des données indexées ADN nécessaires à la confirmation d’une correspondance.

Article 8

Notification de fichiers d’analyses ADN

Chaque État membre informe la Commission et l’eu-LISA des fichiers nationaux d’analyses ADN auxquels s’appliquent les articles 5, 6 et 7, conformément à l’article 73.

Article 9

Références des profils ADN

Les références des profils ADN consistent en la combinaison des éléments suivants:

(a) un numéro de référence permettant aux États membres, en cas de correspondance, d’extraire des données à caractère personnel supplémentaires et d’autres informations de leurs bases de données visées à l’article 5 afin de les transmettre à un, à plusieurs ou à tous les autres États membres, conformément aux articles 47 et 48;

(b) un code indiquant l’État membre qui détient le profil ADN;

(c) un code indiquant le type de profil ADN (profils ADN de référence ou profils ADN non identifiés).

Article 10

Principes régissant l’échange de données indexées ADN

1. Des mesures appropriées sont prises pour assurer la confidentialité et l’intégrité des données indexées ADN transmises aux autres États membres, notamment en matière de cryptage.

2. Les États membres prennent les mesures nécessaires pour garantir l'intégrité des profils ADN mis à la disposition des autres États membres ou transmis pour comparaison aux autres États membres et pour faire en sorte que ces mesures soient conformes aux normes internationales applicables à l'échange de données ADN.

3. La Commission adopte des actes d'exécution afin de préciser les normes internationales applicables qui doivent être utilisées par les États membres pour l'échange de données indexées ADN. Ces actes d'exécution sont adoptés en conformité avec la procédure visée à l'article 76, paragraphe 2.

Article 11

Règles applicables aux demandes et aux réponses relatives aux profils ADN

1. Une demande de consultation ou de comparaison automatisée inclut uniquement les informations suivantes:

(a) le code de l'État membre requérant;

(b) la date, l'heure et le numéro de référence de la demande;

(c) les profils ADN et leurs références visées à l'article 9;

(d) les types de profils ADN transmis (profils ADN non identifiés ou profils ADN de référence).

2. La réponse apportée à la demande visée au paragraphe 1 inclut uniquement les informations suivantes:

(a) une indication précisant s'il y a eu une ou plusieurs correspondances ou aucune correspondance;

(b) la date, l'heure et le numéro de référence de la demande;

(c) la date, l'heure et le numéro de référence de la réponse;

(d) les codes de l'État membre requérant et de l'État membre requis;

(e) les références des profils ADN obtenus de l'État membre requérant et de l'État membre requis;

(f) les types de profils ADN transmis (profils ADN non identifiés ou profils ADN de référence);

(g) les profils ADN pour lesquels une correspondance est établie.

3. La notification automatisée d'une correspondance est effectuée uniquement si la consultation ou la comparaison automatisée a mis en évidence une correspondance fondée sur un nombre minimal de loci. La Commission adopte des actes d'exécution afin de préciser ce nombre minimal de loci, conformément à la procédure visée à l'article 76, paragraphe 2.

4. Lorsqu'une consultation ou une comparaison avec des profils ADN non identifiés met en évidence une correspondance, chaque État membre requis disposant de données correspondantes peut insérer dans sa base de données nationale une marque indiquant que ce profil ADN a déjà fait l'objet d'une correspondance à la suite d'une consultation ou d'une comparaison effectuée par un autre État membre.

5. Les États membres veillent à ce que les demandes soient cohérentes avec les déclarations transmises en vertu de l'article 8. Ces déclarations figurent dans le manuel pratique visé à l'article 78.

SECTION 2

Données dactyloscopiques

Article 12

Données indexées dactyloscopiques

1. Les États membres s'assurent de la disponibilité des données indexées dactyloscopiques provenant du fichier regroupant les systèmes automatisés nationaux d'identification par empreintes digitales créés aux fins de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière.

2. Les données indexées dactyloscopiques ne contiennent aucune donnée permettant l'identification directe de la personne concernée.

3. Les données indexées dactyloscopiques qui ne peuvent être rattachées à aucune personne («données dactyloscopiques non identifiées») doivent être reconnaissables en tant que telles.

Article 13

Consultation automatisée de données dactyloscopiques

1. Aux fins de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière, les États membres autorisent les points de contact nationaux des autres États membres et Europol à accéder aux données indexées dactyloscopiques des systèmes automatisés d'identification par empreintes digitales qu'ils ont créés à cet effet, afin de procéder à des consultations automatisées par comparaison de données indexées dactyloscopiques.

La consultation n'est possible que cas par cas et dans le respect du droit national de l'État membre requérant.

2. Le point de contact national de l'État membre requérant confirme l'existence d'une correspondance entre les données dactyloscopiques et les données indexées dactyloscopiques détenues par l'État membre requis après la transmission automatisée des données indexées dactyloscopiques nécessaires à la confirmation d'une correspondance.

Article 14

Référence des données dactyloscopiques

Les références des profils dactyloscopiques consistent en la combinaison des éléments suivants:

(a) un numéro de référence permettant aux États membres, en cas de correspondance, d'extraire des données à caractère personnel supplémentaires et d'autres informations de leurs bases de données visées à l'article 12 afin de les transmettre à un, à plusieurs ou à tous les autres États membres, conformément aux articles 47 et 48;

(b) un code indiquant l'État membre qui détient les données dactyloscopiques.

Article 15

Principes régissant l'échange de données dactyloscopiques

1. La numérisation des données dactyloscopiques et leur transmission aux autres États membres s'effectuent selon un format de données uniforme. La Commission adopte des actes d'exécution afin de préciser le format de données uniforme, conformément à la procédure visée à l'article 76, paragraphe 2.

2. Chaque État membre s'assure que les données dactyloscopiques qu'il transmet sont d'une qualité suffisante en vue d'une comparaison par les systèmes automatisés d'identification par empreintes digitales.

3. Les États membres prennent des mesures appropriées pour assurer la confidentialité et l'intégrité des données dactyloscopiques transmises aux autres États membres, notamment en matière de cryptage.

4. La Commission adopte des actes d'exécution afin de préciser les normes existantes applicables à l'échange de données dactyloscopiques qui doivent être utilisées par les États membres. Ces actes d'exécution sont adoptés en conformité avec la procédure visée à l'article 76, paragraphe 2.

Article 16

Capacités de consultation pour les données dactyloscopiques

1. Chaque État membre veille à ce que ses demandes de consultation ne dépassent pas les capacités de consultation indiquées par l'État membre requis.

Les États membres informent la Commission et l'eu-LISA, conformément à l'article 79, paragraphes 8 et 10, de leurs capacités maximales de consultation journalières pour les données dactyloscopiques de personnes identifiées et pour les données dactyloscopiques de personnes non encore identifiées.

2. La Commission adopte des actes d'exécution afin de préciser les nombres maximaux de candidats admis pour comparaison par transmission, conformément à la procédure visée à l'article 76, paragraphe 2.

Article 17

Règles applicables aux demandes et aux réponses relatives aux données dactyloscopiques

1. Une demande de consultation automatisée inclut uniquement les informations suivantes:

(a) le code de l'État membre requérant;

(b) la date, l'heure et le numéro de référence de la demande;

(c) les données dactyloscopiques et leurs références visées à l'article 14.

2. La réponse apportée à la demande visée au paragraphe 1 inclut uniquement les informations suivantes:

(a) une indication précisant s'il y a eu une ou plusieurs correspondances ou aucune correspondance;

(b) la date, l'heure et le numéro de référence de la demande;

(c) la date, l'heure et le numéro de référence de la réponse;

(d) les codes de l'État membre requérant et de l'État membre requis;

(e) les références des données dactyloscopiques obtenues de l'État membre requérant et de l'État membre requis;

(f) les données dactyloscopiques pour lesquelles une correspondance est établie.

SECTION 3

Données relatives à l'immatriculation des véhicules

Article 18

Consultation automatisée de données relatives à l'immatriculation des véhicules

1. Aux fins de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière, les États membres autorisent les points de contact nationaux des autres États membres et Europol à accéder aux données nationales suivantes relatives à l'immatriculation des véhicules, afin de procéder, cas par cas, à une consultation automatisée:

(a) les données relatives aux propriétaires ou aux détenteurs, et

(b) les données relatives aux véhicules.

2. La consultation nécessite un numéro de châssis complet ou un numéro d'immatriculation complet.

3. La consultation n'est possible que dans le respect du droit national de l'État membre requérant.

Article 19

Principes régissant la consultation automatisée de données relatives à l'immatriculation des véhicules

1. Aux fins de la consultation automatisée de données relatives à l'immatriculation des véhicules, les États membres utilisent le système d'information européen concernant les véhicules et les permis de conduire (Eucaris).

2. Les informations échangées par l'intermédiaire d'Eucaris sont transmises sous une forme cryptée.

3. La Commission adopte des actes d'exécution afin de préciser les éléments des données relatives à l'immatriculation des véhicules qui doivent être échangés. Ces actes d'exécution sont adoptés en conformité avec la procédure visée à l'article 76, paragraphe 2.

Article 20

Tenue de registres

1. Chaque État membre tient des registres des requêtes introduites par le personnel de ses autorités dûment autorisé à échanger des données relatives à l'immatriculation des véhicules, ainsi que des registres des requêtes demandées par les autres États membres. Europol tient des registres des requêtes introduites par son personnel dûment autorisé.

Chaque État membre et Europol tiennent des registres de toutes les opérations de traitement de données relatives à l'immatriculation des véhicules. Ces registres contiennent les informations suivantes:

(a) l'État membre ou l'agence de l'Union qui lance la demande de requête;

(b) la date et l'heure de la demande;

(c) la date et l'heure de la réponse;

(d) les bases de données nationales auxquelles une demande de requête a été envoyée;

(e) les bases de données nationales qui ont fourni une réponse positive.

2. Les registres visés au paragraphe 1 ne peuvent être utilisés que pour collecter des statistiques et contrôler la protection des données, y compris vérifier l'admissibilité d'une requête et la licéité du traitement des données, et pour assurer la sécurité et l'intégrité des données.

Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création. Cependant, s'ils sont nécessaires à des procédures de contrôle qui ont déjà été engagées, ils sont effacés dès qu'ils ne sont plus nécessaires aux procédures de contrôle.

3. Aux fins du contrôle de la protection des données, y compris de la vérification de l'admissibilité d'une requête et de la licéité du traitement des données, les responsables du traitement ont accès aux registres en vue de l'autocontrôle visé à l'article 56.

SECTION 4

Images faciales

Article 21

Images faciales

1. Les États membres s'assurent de la disponibilité des images faciales provenant de leurs bases de données nationales établies aux fins de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière. Ces données ne contiennent que des images faciales et les références visées à l'article 23, et indiquent si les images faciales sont rattachées à une personne ou non.

Dans ce contexte, les États membres ne mettent à disposition aucune donnée permettant l'identification directe de la personne concernée.

2. Les images faciales qui ne peuvent être rattachées à aucune personne (images faciales non identifiées) doivent être reconnaissables en tant que telles.

Article 22

Consultation automatisée d'images faciales

1. Aux fins de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière, les États membres autorisent les points de contact nationaux des autres États membres et Europol à accéder aux images faciales stockées dans leurs bases de données nationales, afin de procéder à des consultations automatisées.

La consultation n'est possible que cas par cas et dans le respect du droit national de l'État membre requérant.

2. L'État membre requérant reçoit une liste des correspondances concernant les candidats probables. Ledit État membre examine cette liste afin de déterminer l'existence d'une correspondance confirmée.

3. Une norme de qualité minimale est établie pour permettre la consultation et la comparaison d'images faciales. La Commission adopte des actes d'exécution afin de préciser cette norme de qualité minimale. Ces actes d'exécution sont adoptés en conformité avec la procédure visée à l'article 76, paragraphe 2.

Article 23

Références des images faciales

Les références des images faciales consistent en la combinaison des éléments suivants:

(a) un numéro de référence permettant aux États membres, en cas de correspondance, d'extraire des données à caractère personnel supplémentaires et d'autres informations de leurs bases de données visées à l'article 21 afin de les transmettre à un, à plusieurs ou à tous les autres États membres, conformément aux articles 47 et 48;

(b) un code indiquant l'État membre qui détient les images faciales.

Article 24

Règles applicables aux demandes et aux réponses relatives aux images faciales

1. Une demande de consultation automatisée inclut uniquement les informations suivantes:

(a) le code de l'État membre requérant;

(b) la date, l'heure et le numéro de référence de la demande;

(c) les images faciales et leurs références visées à l'article 23.

2. La réponse apportée à la demande visée au paragraphe 1 inclut uniquement les informations suivantes:

(a) une indication précisant s'il y a eu une ou plusieurs correspondances ou aucune correspondance;

(b) la date, l'heure et le numéro de référence de la demande;

(c) la date, l'heure et le numéro de référence de la réponse;

(d) les codes de l'État membre requérant et de l'État membre requis;

(e) les références des images faciales obtenues de l'État membre requérant et de l'État membre requis;

(f) les images faciales pour lesquelles une correspondance est établie.

SECTION 5

Registres de la police

Article 25

Registres de la police

1. Les États membres peuvent décider de participer à l'échange automatisé de registres de la police. Les États membres qui participent à l'échange automatisé de registres de la police s'assurent de la disponibilité des données biographiques des suspects et des criminels dans leurs index nationaux de registres de la police créés aux fins d'enquêtes en matière d'infractions pénales. Cet ensemble de données, s'il est disponible, contient les données suivantes:

(a) le(s) prénom(s);

(b) le(s) nom(s) de famille;

(c) le(s) pseudonyme(s);

(d) la date de naissance;

(e) la (les) nationalité(s);

(f) le lieu et le pays de naissance;

(g) le sexe.

2. Les données visées au paragraphe 1, points a), b), c), e) et f), sont pseudonymisées.

Article 26

Consultation automatisée de registres de la police

1. Aux fins d'enquêtes en matière d'infractions pénales, les États membres autorisent les points de contact nationaux des autres États membres et Europol à accéder aux données provenant de leurs index nationaux de registres de la police, afin de procéder à des consultations automatisées.

La consultation n'est possible que cas par cas et dans le respect du droit national de l'État membre requérant.

2. L'État membre requérant reçoit la liste des correspondances, avec une indication de la qualité de celles-ci.

L'État membre requérant est également informé de l'État membre dont la base de données contient les données qui ont mis en évidence la correspondance.

Article 27

Références des registres de la police

Les références des registres de la police consistent en la combinaison des éléments suivants:

(a) un numéro de référence permettant aux États membres, en cas de correspondance, d'extraire des données à caractère personnel et d'autres informations de leurs index visés à l'article 25 afin de les transmettre à un, à plusieurs ou à tous les autres États membres, conformément aux articles 47 et 48;

(b) un code indiquant l'État membre qui détient les registres de la police.

Article 28

Règles applicables aux demandes et aux réponses relatives aux registres de la police

1. Une demande de consultation automatisée inclut uniquement les informations suivantes:

(a) le code de l'État membre requérant;

(b) la date, l'heure et le numéro de référence de la demande;

(c) les registres de la police et leurs références visées à l'article 27.

2. La réponse apportée à la demande visée au paragraphe 1 inclut uniquement les informations suivantes:

(a) une indication précisant s'il y a eu une ou plusieurs correspondances ou aucune correspondance;

(b) la date, l'heure et le numéro de référence de la demande;

(c) la date, l'heure et le numéro de référence de la réponse;

(d) les codes de l'État membre requérant et de l'État membre requis;

(e) les références des registres de la police obtenus des États membres requis.

SECTION 6

Dispositions communes

Article 29

Points de contact nationaux

Chaque État membre désigne un point de contact national.

Les points de contact nationaux sont chargés de fournir les données visées aux articles 6, 7, 13, 18, 22 et 26.

Article 30

Mesures d'exécution

La Commission adopte des actes d'exécution afin de préciser les modalités techniques des procédures énoncées aux articles 6, 7, 13, 18, 22 et 26. Ces actes d'exécution sont adoptés en conformité avec la procédure visée à l'article 76, paragraphe 2.

Article 31

Spécifications techniques

Les États membres et Europol observent les spécifications techniques communes dans le cadre de toutes les demandes et réponses liées aux consultations et comparaisons de profils ADN, de données dactyloscopiques, de données relatives à l'immatriculation des véhicules, d'images faciales et de registres de la police. La Commission adopte des actes d'exécution afin de préciser ces spécifications techniques, conformément à la procédure visée à l'article 76, paragraphe 2.

Article 32

Disponibilité de l'échange automatisé de données au niveau national

1. Les États membres prennent toutes les mesures nécessaires pour que la consultation ou la comparaison automatisée de données ADN, de données dactyloscopiques, de données relatives à l'immatriculation de véhicules, d'images faciales et de registres de la police soit possible 24 heures sur 24 et sept jours sur sept.

2. Les points de contact nationaux s'informent immédiatement les uns les autres de la défaillance technique entraînant l'indisponibilité de l'échange automatisé de données; ils en informent également la Commission, Europol et l'eu-LISA.

Les points de contact nationaux conviennent d'autres modalités temporaires d'échange d'informations, conformément au droit de l'Union et à la législation nationale applicables.

3. Les points de contact nationaux rétablissent sans délai l'échange automatisé de données.

Article 33

Justification du traitement des données

1. Chaque État membre conserve une justification des requêtes effectuées par ses autorités compétentes.

Europol conserve une justification des requêtes qu'elle effectue.

2. La justification visée au paragraphe 1 comprend:

(a) l'objet de la requête, y compris une référence à l'affaire ou à l'enquête spécifique;

(b) une indication permettant de déterminer si la requête concerne un suspect ou un auteur d'une infraction pénale;

(c) une indication permettant de déterminer si la requête vise à identifier une personne inconnue ou à obtenir plus de données sur une personne connue.

3. Les justifications visées au paragraphe 2 ne peuvent être utilisées que pour contrôler la protection des données, y compris vérifier l'admissibilité d'une requête et la licéité du traitement des données, et pour garantir la sécurité et l'intégrité des données.

Ces justifications sont protégées par des mesures appropriées empêchant tout accès non autorisé et sont effacées un an après leur création. Cependant, si elles sont nécessaires à des procédures de contrôle qui ont déjà été engagées, elles sont effacées dès qu'elles ne sont plus nécessaires à ces procédures.

4. Aux fins du contrôle de la protection des données, y compris de la vérification de l'admissibilité d'une requête et de la licéité du traitement des données, les responsables du traitement ont accès à ces justifications en vue de l'autocontrôle visé à l'article 56.

Article 34

Utilisation du format universel pour les messages

1. La norme de format universel pour les messages (UMF) est utilisée pour le développement du routeur visé à l'article 35 et de l'EPRIS.

2. Tout échange automatisé de données conformément au présent règlement utilise la norme UMF.

CHAPITRE 3

ARCHITECTURE

SECTION 1

Routeur

Article 35

Routeur

1. Un routeur est créé afin de faciliter l'établissement de connexions entre les États membres et avec Europol aux fins de l'interrogation, de l'extraction et de la notation de données biométriques conformément au présent règlement.

2. Le routeur se compose des éléments suivants:

(a) une infrastructure centrale, comprenant un outil de recherche permettant l'interrogation simultanée des bases de données des États membres visées aux articles 5, 12 et 21 ainsi que des données d'Europol;

(b) un canal de communication sécurisé entre l'infrastructure centrale, les États membres et les agences de l'Union qui sont autorisées à utiliser le routeur;

(c) une infrastructure de communication sécurisée entre l'infrastructure centrale et le portail de recherche européen aux fins de l'article 39.

Article 36

Utilisation du routeur

L'utilisation du routeur est réservée aux autorités des États membres qui ont accès à l'échange de profils ADN, de données dactyloscopiques et d'images faciales, ainsi qu'à Europol, conformément au présent règlement et au règlement (UE) 2016/794.

Article 37

Requêtes

1. Les utilisateurs du routeur visés à l'article 36 demandent une requête en soumettant des données biométriques au routeur. Le routeur envoie la demande de requête aux bases de données des États membres et aux données d'Europol en même temps que les données soumises par l'utilisateur et conformément à ses droits d'accès.

2. Dès réception de la demande de requête en provenance du routeur, chaque État membre requis et Europol interrogent leurs bases de données de manière automatisée et sans délai.

3. Toute correspondance mise en évidence par interrogation des bases de données de chaque État membre et des données d'Europol est renvoyée de manière automatisée au routeur.

4. Le routeur classe les réponses en fonction de la note de la correspondance entre les données biométriques utilisées pour la requête et les données biométriques stockées dans les bases de données des États membres et les données d'Europol.

5. La liste des données biométriques pour lesquelles une correspondance a été établie et leurs notes sont renvoyées à l'utilisateur du routeur par ce dernier.

6. La Commission adopte des actes d'exécution afin de préciser la procédure technique permettant au routeur d'interroger les bases de données des États membres et les données d'Europol, le format des réponses du routeur ainsi que les règles techniques de notation de la correspondance entre les données biométriques. Ces actes d'exécution sont adoptés en conformité avec la procédure visée à l'article 76, paragraphe 2.

Article 38

Contrôle de la qualité

L'État membre requis contrôle, par un procédé entièrement automatisé, la qualité des données transmises.

Au cas où les données ne se prêtent pas à une comparaison automatisée, l'État membre requis en informe sans tarder l'État membre requérant par l'intermédiaire du routeur.

Article 39

Interopérabilité entre le routeur et le répertoire commun de données d'identité aux fins de l'accès des services répressifs

1. Les utilisateurs du routeur visés à l'article 36 peuvent interroger les bases de données des États membres et les données d'Europol simultanément à une requête effectuée dans le répertoire commun de données d'identité lorsque les conditions applicables prévues par le droit de l'Union sont remplies et dans le respect de leurs droits d'accès. À cette fin, le routeur interroge le répertoire commun de données d'identité par l'intermédiaire du portail de recherche européen.

2. Les requêtes introduites dans le répertoire commun de données d'identité à des fins répressives sont effectuées conformément à l'article 22 du règlement (UE) 2019/817 et à l'article 22 du

règlement (UE) 2019/818. Tout résultat issu des requêtes est transmis par l'intermédiaire du portail de recherche européen.

Seules les autorités désignées définies à l'article 4, point 20), du règlement (UE) 2019/817 et à l'article 4, point 20), du règlement (UE) 2019/818 peuvent lancer ces requêtes simultanées.

Des requêtes simultanées dans les bases de données des États membres et les données d'Europol et dans le répertoire commun de données d'identité ne peuvent être lancées que dans les cas où il est probable que des données sur un suspect, un auteur ou une victime d'une infraction terroriste ou d'autres infractions pénales graves, telles que définies respectivement à l'article 4, points 21) et 22), du règlement (UE) 2019/817 et à l'article 4, points 21) et 22), du règlement (UE) 2019/818, sont stockées dans le répertoire commun de données d'identité.

Article 40

Tenue de registres

1. L'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le routeur. Ces registres contiennent les informations suivantes:

(a) l'État membre ou l'agence de l'Union qui lance la demande de requête;

(b) la date et l'heure de la demande;

(c) la date et l'heure de la réponse;

(d) les bases de données nationales ou les données d'Europol auxquelles une demande de requête a été envoyée;

(e) les bases de données nationales ou les données d'Europol qui ont fourni une réponse;

(f) le cas échéant, le fait qu'une requête a été introduite simultanément dans le répertoire commun de données d'identité.

2. Chaque État membre tient des registres des requêtes introduites par ses autorités compétentes et le personnel de ces autorités dûment autorisé à utiliser le routeur, ainsi que des registres des requêtes demandées par les autres États membres.

Europol tient des registres des requêtes introduites par son personnel dûment autorisé.

3. Les registres visés aux paragraphes 1 et 2 ne peuvent être utilisés que pour collecter des statistiques et contrôler la protection des données, y compris vérifier l'admissibilité d'une requête et la licéité du traitement des données, et pour garantir la sécurité et l'intégrité des données.

Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création. Cependant, s'ils sont nécessaires à des procédures de contrôle qui ont déjà été engagées, ils sont effacés dès qu'ils ne sont plus nécessaires aux procédures de contrôle.

4. Aux fins du contrôle de la protection des données, y compris de la vérification de l'admissibilité d'une requête et de la licéité du traitement des données, les responsables du traitement ont accès aux registres en vue de l'autocontrôle visé à l'article 56.

Article 41

Procédures de notification en cas d'impossibilité technique d'utiliser le routeur

1. Lorsqu'il est techniquement impossible d'utiliser le routeur pour interroger une ou plusieurs bases de données nationales ou les données d'Europol en raison d'une défaillance du routeur, les utilisateurs du

routeur sont informés de manière automatisée par l'eu-LISA. Cette dernière prend les mesures nécessaires pour remédier sans délai à l'impossibilité technique d'utiliser le routeur.

2. Lorsqu'il est techniquement impossible d'utiliser le routeur pour interroger une ou plusieurs bases de données nationales ou les données d'Europol en raison d'une défaillance de l'infrastructure nationale d'un État membre, cet État membre le notifie, de manière automatisée, aux autres États membres, à l'eu-LISA et à la Commission. Les États membres prennent les mesures nécessaires pour remédier sans délai à l'impossibilité technique d'utiliser le routeur.

3. Lorsqu'il est techniquement impossible d'utiliser le routeur pour interroger une ou plusieurs bases de données nationales ou les données d'Europol en raison d'une défaillance de l'infrastructure d'Europol, cette dernière le notifie, de manière automatisée, aux États membres, à l'eu-LISA et à la Commission. Europol prend les mesures nécessaires pour remédier sans délai à l'impossibilité technique d'utiliser le routeur.

SECTION 2

EPRIS

Article 42

EPRIS

1. Aux fins de la consultation automatisée des registres de la police visée à l'article 26, les États membres et Europol utilisent le système d'index européen des registres de la police (EPRIS).

2. L'EPRIS se compose des éléments suivants:

(a) une infrastructure centrale, comprenant un outil de recherche permettant l'interrogation simultanée des bases de données des États membres;

(b) un canal de communication sécurisé entre l'infrastructure centrale de l'EPRIS, les États membres et Europol.

Article 43

Utilisation de l'EPRIS

1. Aux fins de la consultation de registres de la police par l'intermédiaire de l'EPRIS, les ensembles de données suivants sont utilisés:

(a) le(s) prénom(s);

(b) le(s) nom(s) de famille;

(c) la date de naissance.

2. Lorsqu'ils sont disponibles, les ensembles de données suivants peuvent également être utilisés:

(a) le(s) pseudonyme(s);

(b) la (les) nationalité(s);

(c) le lieu et le pays de naissance;

(d) le sexe.

3. Les données visées au paragraphe 1, points a) et b), et au paragraphe 2, points a), b) et c), utilisées pour les requêtes, sont pseudonymisées.

Article 44

Requêtes

1. Les États membres et Europol demandent une requête en soumettant les données visées à l'article 43.

L'EPRIS envoie la demande de requête aux bases de données des États membres avec les données soumises par l'État membre requérant et conformément au présent règlement.

2. Dès réception de la demande de requête en provenance de l'EPRIS, chaque État membre requis interroge son index national de registres de la police de manière automatisée et sans délai.

3. Toute correspondance mise en évidence par interrogation de la base de données de chaque État membre est renvoyée de manière automatisée à l'EPRIS.

4. La liste des correspondances est renvoyée à l'État membre requérant par l'intermédiaire de l'EPRIS. La liste des correspondances indique la qualité de la correspondance ainsi que l'État membre dont la base de données contient les données qui ont mis en évidence la correspondance.

5. Dès réception de la liste des correspondances, l'État membre requérant décide des correspondances pour lesquelles un suivi est nécessaire et envoie une demande de suivi motivée contenant toute information complémentaire pertinente à l'État membre ou aux États membres requis au moyen de l'application SIENA.

6. L'État membre ou les États membres requis traitent ces demandes sans délai afin de décider de partager ou non les données stockées dans leurs bases de données.

Après confirmation, le ou les États membres requis partagent les données visées à l'article 43 lorsqu'elles sont disponibles. Cet échange d'informations est effectué au moyen de l'application SIENA.

7. La Commission adopte des actes d'exécution afin de préciser la procédure technique permettant à l'EPRIS d'interroger les bases de données des États membres et le format des réponses. Ces actes d'exécution sont adoptés en conformité avec la procédure visée à l'article 76, paragraphe 2.

Article 45

Tenue de registres

1. Europol tient des registres de toutes les opérations de traitement de données effectuées dans l'EPRIS. Ces registres contiennent les informations suivantes:

(a) l'État membre ou l'agence de l'Union qui lance la demande de requête;

(b) la date et l'heure de la demande;

(c) la date et l'heure de la réponse;

(d) les bases de données nationales auxquelles une demande de requête a été envoyée;

(e) les bases de données nationales qui ont fourni une réponse.

2. Chaque État membre tient des registres des demandes de requêtes effectuées par ses autorités compétentes et le personnel de ces autorités dûment autorisé à utiliser l'EPRIS. Europol tient des registres des demandes de requêtes effectuées par son personnel dûment autorisé.

3. Les registres visés aux paragraphes 1 et 2 ne peuvent être utilisés que pour contrôler la protection des données, y compris vérifier l'admissibilité d'une requête et la licéité du traitement des données, et pour garantir la sécurité et l'intégrité des données.

Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création.

Cependant, s'ils sont nécessaires à des procédures de contrôle qui ont déjà été engagées, ils sont effacés dès qu'ils ne sont plus nécessaires aux procédures de contrôle.

4. Aux fins du contrôle de la protection des données, y compris de la vérification de l'admissibilité d'une requête et de la licéité du traitement des données, les responsables du traitement ont accès aux registres en vue de l'autocontrôle visé à l'article 56.

Article 46

Procédures de notification en cas d'impossibilité technique d'utiliser l'EPRIS

1. Lorsqu'il est techniquement impossible d'utiliser l'EPRIS pour interroger une ou plusieurs bases de données nationales en raison d'une défaillance de l'infrastructure d'Europol, cette dernière le notifie, de manière automatisée, aux États membres. Europol prend les mesures nécessaires pour remédier sans délai à l'impossibilité technique d'utiliser l'EPRIS.

2. Lorsqu'il est techniquement impossible d'utiliser l'EPRIS pour interroger une ou plusieurs bases de données nationales en raison d'une défaillance de l'infrastructure nationale d'un État membre, cet État membre le notifie, de manière automatisée, à Europol et à la Commission. Les États membres prennent les mesures nécessaires pour remédier sans délai à l'impossibilité technique d'utiliser l'EPRIS.

CHAPITRE 4

ÉCHANGE DE DONNÉES À LA SUITE D'UNE CORRESPONDANCE

Article 47

Échange de données de base

Lorsque les procédures visées aux articles 6, 7, 13 ou 22 révèlent une correspondance entre les données utilisées aux fins de la consultation ou de la comparaison et les données détenues dans la base de données de l'État membre ou des États membres requis, et après confirmation de cette correspondance par l'État membre requérant, l'État membre requis renvoie un ensemble de données de base par l'intermédiaire du routeur dans les 24 heures. Cet ensemble de données de base, s'il est disponible, contient les données suivantes:

(a) le(s) prénom(s);

(b) le(s) nom(s) de famille;

(c) la date de naissance;

(d) la (les) nationalité(s);

(e) le lieu et le pays de naissance;

(f) le sexe.

Article 48

Utilisation de l'application SIENA

Tout échange qui n'est pas explicitement prévu par le présent règlement entre les autorités compétentes des États membres ou avec Europol, à n'importe quel stade de l'une des procédures prévues par le présent règlement, se fait au moyen de l'application SIENA.

CHAPITRE 5

EUROPOL

Article 49

Accès des États membres aux données biométriques obtenues auprès de pays tiers et stockées par Europol

1. Conformément au règlement (UE) 2016/794, les États membres ont accès aux données biométriques qui ont été fournies à Europol par des pays tiers aux fins de l'article 18, paragraphe 2, points a), b) et c), du règlement (UE) 2016/794, et peuvent les consulter par l'intermédiaire du routeur.

2. Lorsque cette procédure met en évidence une correspondance entre les données utilisées aux fins de la consultation et les données d'Europol, le suivi se fait conformément au règlement (UE) 2016/794.

Article 50

Accès d'Europol aux données stockées dans les bases de données des États membres

1. Conformément au règlement (UE) 2016/794, Europol a accès aux données qui sont stockées par les États membres dans leurs bases de données nationales conformément au présent règlement.

2. Les requêtes d'Europol ayant des données biométriques pour critère de recherche sont réalisées à l'aide du routeur.

3. Les requêtes d'Europol ayant des données relatives à l'immatriculation des véhicules pour critère de recherche sont réalisées à l'aide d'Eucaris.

4. Les requêtes d'Europol ayant des registres de la police pour critère de recherche sont réalisées à l'aide de l'EPRIS.

5. Europol effectue les recherches conformément au paragraphe 1 uniquement dans le cadre de l'exécution de ses missions visées par le règlement (UE) 2016/794.

6. Lorsque les procédures visées aux articles 6, 7, 13 ou 22 révèlent une correspondance entre les données utilisées aux fins de la consultation ou de la comparaison et les données détenues dans la base de données nationale du ou des États membres requis, et après confirmation de cette correspondance par Europol, l'État membre requis décide de renvoyer ou non un ensemble de données de base par l'intermédiaire du routeur dans les 24 heures. Cet ensemble de données de base, s'il est disponible, contient les données suivantes:

(a) le(s) prénom(s);

(b) le(s) nom(s) de famille;

(c) la date de naissance;

(d) la (les) nationalité(s);

(e) le lieu et le pays de naissance;

(f) le sexe.

7. L'utilisation par Europol des informations obtenues à la suite d'une consultation effectuée conformément au paragraphe 1 et de l'échange de données de base conformément au paragraphe 6 est soumise au consentement de l'État membre dans la base de données duquel la correspondance a été mise en évidence. Si ledit État membre autorise l'utilisation de ces informations, leur traitement par Europol est régi par le règlement (UE) 2016/794.

CHAPITRE 6

PROTECTION DES DONNÉES

Article 51

Objet des données

1. L'État membre requérant ou Europol ne peut traiter les données à caractère personnel qu'aux fins pour lesquelles les données lui ont été transmises par l'État membre requis en vertu du présent règlement. Le traitement à d'autres fins n'est autorisé qu'avec l'autorisation préalable de l'État membre requis.

2. L'État membre effectuant la consultation ou la comparaison des données ne peut procéder à un traitement des données transmises en vertu des articles 6, 7, 13, 18 ou 22 qu'aux fins suivantes:

(a) établir une correspondance entre les profils ADN, les données dactyloscopiques, les données relatives à l'immatriculation des véhicules, les images faciales et les registres de la police.

(b) établir et soumettre une demande d'entraide judiciaire, en cas de correspondance de ces données;

(c) tenir des registres conformément aux articles 40 et 45.

3. L'État membre requérant ne peut traiter les données qui lui sont transmises conformément aux articles 6, 7, 13 ou 22 que lorsqu'un tel traitement est nécessaire aux fins du présent règlement. Les données transmises sont effacées immédiatement après la comparaison ou la réponse automatisée, à moins que la poursuite du traitement par l'État membre requérant ne soit nécessaire aux fins de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière.

4. Les données transmises conformément à l'article 18 ne peuvent être utilisées par l'État membre requérant que si une telle utilisation est nécessaire aux fins du présent règlement. Les données transmises sont effacées immédiatement après l'obtention de la réponse automatisée, à moins que la poursuite du traitement en vue de la journalisation prévue à l'article 20 ne soit nécessaire. L'État membre requérant n'utilise les données obtenues dans le cadre de la réponse qu'aux fins de la procédure pour laquelle la consultation a été effectuée.

Article 52

Exactitude, pertinence et conservation des données

1. Les États membres s'assurent de l'exactitude et de l'actualité des données à caractère personnel. Si un État membre requis se rend compte que des données inexactes ou qui n'auraient pas dû être transmises ont été fournies, les États membres requérants en sont informés sans délai. Tous les États membres requérants concernés sont tenus de rectifier ou de supprimer les données en conséquence. En outre, les données à caractère personnel transmises sont corrigées si elles se révèlent inexactes. Si l'État

membre requérant a des raisons de penser que des données transmises sont inexactes ou devraient être effacées, l'État membre requis en est informé.

2. Lorsqu'une personne concernée conteste l'exactitude des données en possession d'un État membre, lorsque l'exactitude ne peut être établie de manière fiable par l'État membre concerné et lorsque la personne concernée le demande, les données concernées sont marquées. Les États membres peuvent lever un tel marquage uniquement avec le consentement de la personne concernée ou sur décision de la juridiction compétente ou de l'autorité indépendante compétente en matière de protection des données.

3. Les données transmises sont effacées lorsqu'elles n'auraient pas dû être transmises ou reçues. Les données légalement transmises et reçues sont effacées:

(a) lorsqu'elles ne sont pas ou plus nécessaires au regard des finalités pour lesquelles elles ont été transmises;

(b) à l'expiration de la période maximale de conservation des données prévue par le droit national de l'État membre requis, lorsque celui-ci a informé l'État membre requérant de cette période maximale au moment de la transmission.

Lorsqu'il y a des raisons de penser que l'effacement des données porterait atteinte aux intérêts de la personne concernée, les données sont verrouillées au lieu d'être effacées. Des données verrouillées ne peuvent être utilisées ou transmises qu'aux fins qui ont empêché leur effacement.

Article 53

Sous-traitant

1. L'eu-LISA est le sous-traitant au sens de l'article 3, point 12), du règlement (UE) 2018/1725 pour le traitement des données à caractère personnel par l'intermédiaire du routeur.

2. Europol est le sous-traitant pour le traitement des données à caractère personnel par l'intermédiaire de l'EPRIS.

Article 54

Sécurité du traitement

1. Europol, l'eu-LISA et les autorités des États membres veillent à la sécurité du traitement des données à caractère personnel qui est effectué en application du présent règlement. Europol, l'eu-LISA et les autorités des États membres coopèrent pour les tâches liées à la sécurité.

2. Sans préjudice de l'article 33 du règlement (UE) 2018/1725 et de l'article 32 du règlement (UE) 2016/794, l'eu-LISA et Europol prennent les mesures nécessaires pour garantir la sécurité du routeur et de l'EPRIS respectivement et de leurs infrastructures de communication connexes.

3. En particulier, l'eu-LISA et Europol adoptent les mesures nécessaires concernant le routeur et l'EPRIS respectivement, y compris un plan de sécurité, un plan de continuité des activités et un plan de rétablissement après sinistre, afin:

(a) de garantir la protection physique des données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques;

(b) d'interdire à toute personne non autorisée d'accéder aux équipements et aux installations utilisés pour le traitement de données;

(c) d’empêcher toute lecture, copie ou modification ou tout retrait non autorisés de supports de données;

(d) d’empêcher l’introduction non autorisée de données et le contrôle, la modification ou l’effacement non autorisés de données à caractère personnel enregistrées;

(e) d’empêcher le traitement non autorisé de données ainsi que toute copie, toute modification ou tout effacement non autorisés de données;

(f) d’empêcher l’utilisation de systèmes de traitement automatisé de données par des personnes non autorisées au moyen de matériel de transmission de données;

(g) de garantir que les personnes autorisées à avoir accès au routeur et à l’EPRIS n’aient accès qu’aux données couvertes par leur autorisation d’accès, uniquement grâce à l’attribution d’identifiants individuels et à des modes d’accès confidentiels;

(h) de garantir la possibilité de vérifier et d’établir à quels organismes les données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données;

(i) de garantir la possibilité de vérifier et d’établir quelles données ont été traitées dans le routeur et l’EPRIS, à quel moment, par qui et dans quel but;

(j) d’empêcher toute lecture, copie, modification ou tout effacement non autorisés de données à caractère personnel pendant leur transmission à partir du routeur et de l’EPRIS ou vers ceux-ci, ou durant le transport de supports de données, en particulier par des techniques de cryptage adaptées;

(k) de garantir le rétablissement des systèmes installés en cas d’interruption;

(l) de garantir la fiabilité en veillant à ce que toute erreur survenant dans le fonctionnement du routeur et de l’EPRIS soit dûment signalée;

(m) de contrôler l’efficacité des mesures de sécurité visées au présent paragraphe et de prendre les mesures organisationnelles nécessaires en matière de contrôle interne pour assurer le respect du présent règlement et d’évaluer ces mesures de sécurité à la lumière des nouvelles évolutions technologiques.

Article 55

Incidents de sécurité

1. Tout événement ayant ou pouvant avoir une incidence sur la sécurité du routeur ou de l’EPRIS et susceptible de causer aux données qui y sont stockées des dommages ou des pertes est considéré comme un incident de sécurité, en particulier lorsque des données peuvent avoir été consultées sans autorisation ou que la disponibilité, l’intégrité et la confidentialité des données ont été ou peuvent avoir été compromises.

2. Les incidents de sécurité sont gérés de telle sorte qu’une réponse rapide, efficace et idoine y soit apportée.

3. Les États membres notifient à leurs autorités de contrôle compétentes tout incident de sécurité dans les meilleurs délais.

Sans préjudice de l’article 34 du règlement (UE) 2016/794, Europol notifie à l’équipe d’intervention en cas d’urgence informatique pour les institutions, organes et agences de l’Union européenne (CERT-UE) les menaces informatiques importantes, les vulnérabilités importantes et les incidents importants

dans les meilleurs délais et, en tout état de cause, au plus tard 24 heures après en avoir pris connaissance. Les détails techniques appropriés et exploitables concernant les menaces informatiques, les vulnérabilités et les incidents qui permettent une détection proactive, une réponse aux incidents ou des mesures d'atténuation sont divulgués à la CERT-UE dans les meilleurs délais.

En cas d'incident de sécurité lié à l'infrastructure centrale du routeur, l'eu-LISA notifie à la CERT-EU les menaces informatiques importantes, les vulnérabilités importantes et les incidents importants dans les meilleurs délais et, en tout état de cause, au plus tard 24 heures après en avoir pris connaissance. Les détails techniques appropriés et exploitables concernant les menaces informatiques, les vulnérabilités et les incidents qui permettent une détection proactive, une réponse aux incidents ou des mesures d'atténuation sont divulgués à la CERT-UE dans les meilleurs délais.

4. Les informations relatives à un incident de sécurité ayant ou pouvant avoir une incidence sur le fonctionnement du routeur ou sur la disponibilité, l'intégrité et la confidentialité des données sont communiquées sans délai par les États membres et les agences de l'Union concernés aux États membres et à Europol et consignées conformément au plan de gestion des incidents qui doit être élaboré par l'eu-LISA.

5. Les informations relatives à un incident de sécurité ayant ou pouvant avoir une incidence sur le fonctionnement de l'EPRIS ou sur la disponibilité, l'intégrité et la confidentialité des données sont communiquées sans délai par les États membres et les agences de l'Union concernés aux États membres et consignées conformément au plan de gestion des incidents qui doit être élaboré par Europol.

Article 56

Autocontrôle

1. Les États membres et les agences de l'Union concernées veillent à ce que chaque autorité habilitée à utiliser le mécanisme de Prüm II prenne les mesures nécessaires afin de vérifier qu'elle respecte le présent règlement et coopère, au besoin, avec l'autorité de contrôle.

2. Les responsables du traitement prennent les mesures nécessaires afin de contrôler la conformité des opérations de traitement des données au regard du présent règlement, notamment en vérifiant fréquemment les registres visés aux articles 40 et 45, et coopèrent, au besoin, avec les autorités de contrôle et avec le Contrôleur européen de la protection des données.

Article 57

Sanctions

Les États membres veillent à ce que toute utilisation abusive, tout traitement ou tout échange de données contraire au présent règlement soit sanctionné conformément à leur droit national. Les sanctions prévues sont effectives, proportionnées et dissuasives.

Article 58

Charge de la preuve

1. Les États membres prennent les mesures nécessaires afin que les personnes qui s'estiment victimes d'une discrimination en raison du traitement ou de l'échange de leurs données à caractère personnel ne supportent pas la charge de la preuve. Lorsqu'une personne estime qu'elle aurait fait l'objet d'une discrimination dans le cadre d'une comparaison automatisée effectuée au titre du présent règlement

devant une juridiction ou une autre autorité judiciaire compétente, les autorités de l'État membre ayant traité les données justifient l'absence de discrimination.

2. Le paragraphe 1 ne s'applique pas aux procédures pénales.

3. Les États membres ne prennent pas de mesures spécifiques au sens du paragraphe 1 pour les procédures dans lesquelles il appartient à la juridiction ou à l'instance judiciaire compétente d'instruire les faits de l'espèce.

Article 59

Responsabilité

Si le non-respect, par un État membre, des obligations qui lui incombent au titre du présent règlement cause un dommage au routeur ou à l'EPRIS, cet État membre en est tenu pour responsable, sauf si, et dans la mesure où, l'eu-LISA, Europol ou un autre État membre lié par le présent règlement n'a pas pris de mesures raisonnables pour prévenir le dommage ou en atténuer les effets.

Article 60

Audits par le Contrôleur européen de la protection des données

1. Le Contrôleur européen de la protection des données veille à ce que soit réalisé, tous les quatre ans au minimum, un audit des opérations de traitement des données à caractère personnel effectuées aux fins du présent règlement par l'eu-LISA et Europol, conformément aux normes internationales applicables en matière d'audit. Un rapport d'audit est communiqué au Parlement européen, au Conseil, à la Commission, aux États membres et à l'agence de l'Union concernée. Europol et l'eu-LISA ont la possibilité de formuler des observations avant l'adoption des rapports.

2. L'eu-LISA et Europol communiquent au Contrôleur européen de la protection des données les renseignements qu'il demande et lui octroient l'accès à tous les documents qu'il demande et à leurs registres visés aux articles 40 et 45, et lui permettent d'accéder, à tout moment, à l'ensemble de leurs locaux.

Article 61

Coopération entre les autorités de contrôle et le Contrôleur européen de la protection des données

1. Les autorités de contrôle et le Contrôleur européen de la protection des données, agissant chacun dans les limites de leurs compétences respectives, coopèrent activement dans le cadre de leurs responsabilités respectives et assurent un contrôle coordonné de l'application du présent règlement, notamment si le Contrôleur européen de la protection des données ou une autorité de contrôle découvre des différences importantes entre les pratiques des États membres ou l'existence de transferts potentiellement illicites transitant par les canaux de communication du mécanisme de Prüm II.

2. Dans les cas visés au paragraphe 1 du présent article, un contrôle coordonné est assuré conformément à l'article 62 du règlement (UE) 2018/1725.

3. Le comité européen de la protection des données envoie un rapport d'activités conjoint au Parlement européen, au Conseil, à la Commission, à Europol et à l'eu-LISA au plus tard [*deux ans après l'entrée en service du routeur et de l'EPRIS*], puis tous les deux ans par la suite. Ce rapport comporte un chapitre sur chaque État membre, établi par l'autorité de contrôle de l'État membre concerné.

Article 62

Communication de données à caractère personnel à des pays tiers et à des organisations internationales

Les données traitées conformément au présent règlement ne sont pas transférées à des pays tiers ou à des organisations internationales ni mises à leur disposition de manière automatisée.

CHAPITRE 7

RESPONSABILITÉS

Article 63

Responsabilités incombant aux États membres

1. Chaque État membre est responsable:

(a) de la connexion à l'infrastructure du routeur;

(b) de l'intégration des systèmes et infrastructures nationaux existants avec le routeur;

(c) de l'organisation, de la gestion, du fonctionnement et de la maintenance de son infrastructure nationale existante et de sa connexion au routeur;

(d) de la connexion à l'infrastructure de l'EPRIS;

(e) de l'intégration des systèmes et infrastructures nationaux existants avec l'EPRIS;

(f) de l'organisation, de la gestion, du fonctionnement et de la maintenance de son infrastructure nationale existante et de sa connexion à l'EPRIS;

(g) de la gestion et des modalités de l'accès au routeur du personnel dûment autorisé des autorités nationales compétentes, conformément au présent règlement, ainsi que de l'établissement d'une liste de ce personnel et de ses qualifications et de la mise à jour régulière de cette liste;

(h) de la gestion et des modalités de l'accès à l'EPRIS du personnel dûment autorisé des autorités nationales compétentes, conformément au présent règlement, ainsi que de l'établissement d'une liste de ce personnel et de ses qualifications et de la mise à jour régulière de cette liste;

(i) de la gestion et des modalités de l'accès à Eucaris du personnel dûment autorisé des autorités nationales compétentes, conformément au présent règlement, ainsi que de l'établissement d'une liste de ce personnel et de ses qualifications et de la mise à jour régulière de cette liste;

(j) de la confirmation manuelle d'une correspondance telle que visée à l'article 6, paragraphe 3, à l'article 7, paragraphe 3, à l'article 13, paragraphe 2, à l'article 22, paragraphe 2, et à l'article 26, paragraphe 2;

(k) de la disponibilité des données nécessaires à l'échange de données, conformément aux articles 6, 7, 13, 18, 22 et 26;

(l) de l'échange d'informations, conformément aux articles 6, 7, 13, 18, 22 et 26;

(m) de la suppression de toute donnée reçue d'un État membre requis dans les 48 heures suivant la notification par l'État membre requis que les données à caractère personnel transmises étaient inexactes, n'étaient plus à jour ou avaient été transmises de manière illicite;

(n) du respect des exigences en matière de qualité des données établies par le présent règlement.

2. Chaque État membre est chargé de connecter ses autorités nationales compétentes au routeur, à l'EPRIS et à Eucaris.

Article 64

Responsabilités incombant à Europol

1. Europol est responsable de la gestion et des modalités de l'accès au routeur, à l'EPRIS et à Eucaris de son personnel dûment autorisé, conformément au présent règlement.

2. Europol est également responsable du traitement des requêtes concernant des données d'Europol par le routeur. Europol adapte ses systèmes d'information en conséquence.

3. Europol est responsable de toute adaptation technique de son infrastructure nécessaire à l'établissement de la connexion au routeur et à Eucaris.

4. Europol est responsable du développement de l'EPRIS en coopération avec les États membres. L'EPRIS fournit les fonctionnalités prévues aux articles 42 à 46.

Europol assure la gestion technique de l'EPRIS. La gestion technique de l'EPRIS comprend toutes les tâches et solutions techniques nécessaires au fonctionnement de l'infrastructure centrale de l'EPRIS et la fourniture continue de services aux États membres, 24 heures sur 24 et sept jours sur sept, conformément au présent règlement. Elle comprend les travaux de maintenance et les perfectionnements techniques indispensables pour que l'EPRIS fonctionne à un niveau satisfaisant de qualité technique, notamment quant au temps de réponse pour l'interrogation des bases de données nationales, conformément aux spécifications techniques.

5. Europol assure la formation à l'utilisation technique de l'EPRIS.

6. Europol est responsable des procédures visées aux articles 49 et 50.

Article 65

Responsabilités incombant à l'eu-LISA durant la phase de conception et de développement du routeur

1. L'eu-LISA veille à ce que l'infrastructure centrale du routeur soit exploitée conformément au présent règlement.

2. Le routeur est hébergé par l'eu-LISA sur ses sites techniques et fournit les fonctionnalités prévues dans le présent règlement, conformément aux conditions de sécurité, de disponibilité, de qualité et de performance visées à l'article 66, paragraphe 1.

3. L'eu-LISA est responsable du développement du routeur et de toute adaptation technique nécessaire au fonctionnement du routeur.

L'eu-LISA n'a accès à aucune des données à caractère personnel traitées par le routeur.

L'eu-LISA définit la conception de l'architecture physique du routeur, y compris de ses infrastructures de communication, ainsi que les spécifications techniques et son évolution en ce qui concerne l'infrastructure centrale et l'infrastructure de communication sécurisée. Cette conception est adoptée par le conseil d'administration, sous réserve d'un avis favorable de la Commission. L'eu-LISA met

également en œuvre toutes les adaptations nécessaires des éléments d'interopérabilité découlant de la mise en place du routeur, comme prévu par le présent règlement.

L'eu-LISA développe et met en œuvre le routeur dès que possible après l'adoption par la Commission des mesures prévues à l'article 37, paragraphe 6.

Le développement consiste en l'élaboration et la mise en œuvre des spécifications techniques, en la réalisation d'essais et en la gestion et la coordination générales du projet.

4. Au cours de la phase de conception et de développement, le conseil de gestion du programme d'interopérabilité visé à l'article 54 du règlement (UE) 2019/817 et à l'article 54 du règlement (UE) 2019/818 se réunit régulièrement. Il veille à la bonne gestion de la phase de conception et de développement du routeur.

Le conseil de gestion du programme d'interopérabilité soumet chaque mois au conseil d'administration de l'eu-LISA des rapports écrits sur l'état d'avancement du projet. Le conseil de gestion du programme d'interopérabilité n'a aucun pouvoir décisionnel ni aucun mandat lui permettant de représenter les membres du conseil d'administration de l'eu-LISA.

Le groupe consultatif visé à l'article 77 se réunit régulièrement jusqu'à la mise en service du routeur. Après chaque réunion, il rend compte au comité de gestion du programme d'interopérabilité. Il fournit l'expertise technique nécessaire à l'appui des tâches du conseil de gestion du programme d'interopérabilité et suit l'état de préparation des États membres.

Article 66

Responsabilités incombant à l'eu-LISA à la suite de la mise en service du routeur

1. Après la mise en service du routeur, l'eu-LISA est responsable de la gestion technique de l'infrastructure centrale du routeur, y compris de sa maintenance et de ses évolutions technologiques. Elle veille, en coopération avec les États membres, à ce que la meilleure technologie disponible soit utilisée, sous réserve d'une analyse coûts-avantages. L'eu-LISA est également responsable de la gestion technique de l'infrastructure de communication nécessaire.

La gestion technique du routeur comprend toutes les tâches et solutions techniques nécessaires au fonctionnement du routeur et la fourniture continue de services aux États membres et à Europol, 24 heures sur 24 et sept jours sur sept, conformément au présent règlement. Elle comprend les travaux de maintenance et les perfectionnements techniques indispensables pour que le routeur fonctionne à un niveau satisfaisant de qualité technique, notamment quant à la disponibilité et au temps de réponse pour soumettre des demandes aux bases de données nationales et aux données d'Europol, conformément aux spécifications techniques.

Le routeur est développé et géré de manière à garantir un accès rapide, efficace et contrôlé, une disponibilité totale et ininterrompue du routeur et un temps de réponse adapté aux besoins opérationnels des autorités compétentes des États membres et d'Europol.

2. Sans préjudice de l'article 17 du statut des fonctionnaires de l'Union européenne fixé dans le règlement (CEE, Euratom, CECA) nº 259/68 du Conseil[42], l'eu-LISA applique des règles appropriées en matière de secret professionnel ou impose des obligations de confidentialité équivalentes à tous les membres de son personnel appelés à travailler avec des données conservées dans les éléments d'interopérabilité. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après la cessation de leur activité.

[42] JO L 56 du 4.3.1968, p. 1.

L’eu-LISA n’a accès à aucune des données à caractère personnel traitées par le routeur.

3. L’eu-LISA s’acquitte aussi des tâches liées à la fourniture d’une formation à l’utilisation technique du routeur.

CHAPITRE 8

MODIFICATIONS D’AUTRES INSTRUMENTS EXISTANTS

Article 67

Modifications apportées aux décisions 2008/615/JAI et 2008/616/JAI du Conseil

1. Les articles 2 à 6 et les sections 2 et 3 du chapitre 2 de la décision 2008/615/JAI sont remplacés à l’égard des États membres liés par le présent règlement à compter de la date d’application des dispositions du présent règlement relatives au routeur telles qu’énoncées à l’article 74.

   Par conséquent, les articles 2 à 6 et les sections 2 et 3 du chapitre 2 de la décision 2008/615/JAI sont supprimés à compter de la date d’application des dispositions du présent règlement relatives au routeur telles qu’énoncées à l’article 74.

2. Les chapitres 2 à 5 et les articles 18, 20 et 21 de la décision 2008/616/JAI sont remplacés à l’égard des États membres liés par le présent règlement à compter de la date d’application des dispositions du présent règlement relatives au routeur telles qu’énoncées à l’article 74.

Par conséquent, les chapitres 2 à 5 et les articles 18, 20 et 21 de la décision 2008/616/JAI sont supprimés à compter de la date d’application des dispositions du présent règlement relatives au routeur telles qu’énoncées à l’article 74.

Article 68

Modifications apportées au règlement (UE) 2018/1726

Le règlement (UE) 2018/1726 est modifié comme suit:

(1) L’article 13 *bis* suivant est inséré:

«Article 13 *bis*

Tâches liées au routeur

En ce qui concerne le règlement (UE) .../... du Parlement européen et du Conseil*[*le présent règlement*], l’Agence s’acquitte des tâches liées au routeur que lui confère ledit règlement.

_____

* Règlement (UE) [numéro] du Parlement européen et du Conseil du xy relatif à/au [titre officiellement adopté] (JO L ...)».

À l’article 17, le paragraphe 3 est remplacé par le texte suivant:

«3. L’Agence a son siège à Tallinn en Estonie.

Les tâches liées au développement et à la gestion opérationnelle visées à l'article 1er, paragraphes 4 et 5, aux articles 3 à 8 et aux articles 9, 11 et 13 *bis* sont menées sur le site technique à Strasbourg en France.

Un site de secours à même d'assurer le fonctionnement d'un système d'information à grande échelle en cas de défaillance dudit système est installé à Sankt Johann im Pongau en Autriche.».

Article 69

Modifications apportées au règlement (UE) 2019/817

À l'article 6, paragraphe 2, du règlement (UE) 2019/817, le point d) suivant est ajouté:

«d) une infrastructure de communication sécurisée entre l'ESP et le routeur établie par le règlement (UE) .../... du Parlement européen et du Conseil* [*le présent règlement*].

_____

* Règlement (UE) [numéro] du Parlement européen et du Conseil du xy relatif à/au [titre officiellement adopté] (JO L ...)».

Article 70

Modifications apportées au règlement (UE) 2019/818

Le règlement (UE) 2019/818 est modifié comme suit:

(1) À l'article 6, paragraphe 2, le point d) suivant est ajouté:

«d) une infrastructure de communication sécurisée entre l'ESP et le routeur établie par le règlement (UE) .../... du Parlement européen et du Conseil* [*le présent règlement*].

_____

* Règlement (UE) [numéro] du Parlement européen et du Conseil du xy relatif à/au [titre officiellement adopté] (JO L ...)».

(2) À l'article 39, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Un répertoire central des rapports et statistiques (CRRS) est créé pour soutenir les objectifs du SIS, d'Eurodac et de l'ECRIS-TCN, conformément aux différents instruments juridiques régissant ces systèmes, et pour fournir des statistiques intersystèmes et des rapports analytiques à des fins stratégiques, opérationnelles et de qualité des données. Le CRRS soutient également les objectifs du mécanisme de Prüm II.

2. L'eu-LISA établit, met en œuvre et héberge sur ses sites techniques le CRRS contenant les données et les statistiques visées à l'article 74 du règlement (UE) 2018/1862 et à l'article 32 du règlement (UE) 2019/816, séparées logiquement par système d'information de l'UE. L'eu-LISA collecte également les données et les statistiques provenant du routeur visé à l'article 65, paragraphe 1, du règlement (UE) .../... * [*le présent règlement*]. L'accès au CRRS est accordé,

moyennant un accès contrôlé et sécurisé et des profils d'utilisateur spécifiques, aux seules fins de l'élaboration de rapports et de statistiques, aux autorités visées à l'article 74 du règlement (UE) 2018/1862, à l'article 32 du règlement (UE) 2019/816 et à l'article 65, paragraphe 1, du règlement (UE) .../... * [*le présent règlement*].».

CHAPITRE 9

DISPOSITIONS FINALES

Article 71

Établissement de rapports et de statistiques

1. Le personnel dûment autorisé des autorités compétentes des États membres, de la Commission, d'Europol et de l'eu-LISA a accès en consultation aux données énumérées ci-après concernant le routeur, uniquement aux fins de l'établissement de rapports et de statistiques:

(a) le nombre de requêtes introduites par chaque État membre et par Europol;

(b) le nombre de requêtes par catégorie de données;

(c) le nombre de requêtes lancées dans chacune des bases de données connectées;

(d) le nombre de correspondances au regard de la base de données de chaque État membre par catégorie de données;

(e) le nombre de correspondances au regard des données d'Europol par catégorie de données;

(f) le nombre de correspondances confirmées lorsqu'il y a eu des échanges de données de base; et

(g) le nombre de requêtes lancées dans le répertoire commun de données d'identité par l'intermédiaire du routeur.

Il n'est pas possible d'identifier des personnes à partir de ces données.

2. Le personnel dûment autorisé des autorités compétentes des États membres, d'Europol et de la Commission a accès en consultation aux données énumérées ci-après concernant Eucaris, uniquement aux fins de l'établissement de rapports et de statistiques:

(a) le nombre de requêtes introduites par chaque État membre et par Europol;

(b) le nombre de requêtes lancées dans chacune des bases de données connectées;

(c) le nombre de correspondances au regard de la base de données de chaque État membre.

Il n'est pas possible d'identifier des personnes à partir de ces données.

3. Le personnel dûment autorisé des autorités compétentes des États membres, de la Commission et d'Europol a accès en consultation aux données énumérées ci-après concernant l'EPRIS, uniquement aux fins de l'établissement de rapports et de statistiques:

(a) le nombre de requêtes introduites par chaque État membre et par Europol;

(b) le nombre de requêtes lancées dans chacune des bases de données connectées;

(c) le nombre de correspondances au regard de la base de données de chaque État membre.

Il n'est pas possible d'identifier des personnes à partir de ces données.

4. L'eu-LISA stocke les données visées par ces paragraphes.

Les données permettent aux autorités visées au paragraphe 1 d'obtenir des rapports et des statistiques personnalisables afin de renforcer l'efficacité de la coopération en matière répressive.

Article 72

Coûts

1. Les coûts afférents à la création et au fonctionnement du routeur et de l'EPRIS sont à la charge du budget général de l'Union.

2. Les coûts afférents à l'intégration des infrastructures nationales existantes et à leur connexion au routeur et à l'EPRIS, ainsi que les coûts afférents à la création de bases de données nationales d'images faciales et d'index nationaux de registre de la police aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière sont à la charge du budget général de l'Union.

Les coûts suivants ne sont pas admissibles:

(a) les coûts afférents au bureau de gestion de projets des États membres (réunions, missions, locaux);

(b) les coûts afférents à l'hébergement des systèmes d'information nationaux (espace, mise en œuvre, électricité, refroidissement);

(c) les coûts afférents au fonctionnement des systèmes d'information nationaux (contrats conclus avec les opérateurs et contrats d'appui);

(d) les coûts afférents à la conception, au développement, à la mise en œuvre, au fonctionnement et à la maintenance des réseaux de communication nationaux.

3. Chaque État membre prend en charge les coûts afférents à la gestion, à l'utilisation et à la maintenance de l'application informatique Eucaris visée à l'article 19, paragraphe 1.

4. Chaque État membre prend en charge les coûts afférents à la gestion, à l'utilisation et à la maintenance de ses connexions au routeur et à l'EPRIS.

Article 73

Notifications

1. Les États membres notifient à l'eu-LISA le nom des autorités visées à l'article 36 qui peuvent utiliser le routeur ou y avoir accès.

2. L'eu-LISA informe la Commission des résultats concluants des essais visés à l'article 74, paragraphe 1, point b).

3. Les États membres notifient à la Commission, à Europol et à l'eu-LISA les points de contact nationaux.

Article 74

Mise en service

1. La Commission fixe, par la voie d'un acte d'exécution, la date à compter de laquelle les États membres et les agences de l'Union peuvent commencer à utiliser le routeur, dès que les conditions suivantes sont remplies:

(a) les mesures prévues à l'article 37, paragraphe 6, ont été adoptées;

(b) l'eu-LISA a déclaré que les essais complets du routeur qu'elle a menés en coopération avec les autorités des États membres et Europol ont été concluants.

Dans cet acte d'exécution, la Commission fixe également la date à compter de laquelle les États membres et les agences de l'Union doivent commencer à utiliser le routeur. Cette date est fixée à un an après la date fixée conformément au premier alinéa.

La Commission peut reporter la date à compter de laquelle les États membres et les agences de l'Union doivent commencer à utiliser le routeur d'un an au maximum lorsqu'une évaluation de la mise en œuvre du routeur a montré la nécessité d'un tel report. Cet acte d'exécution est adopté en conformité avec la procédure visée à l'article 76, paragraphe 2.

2. La Commission fixe, par la voie d'un acte d'exécution, la date à compter de laquelle les États membres et les agences de l'Union doivent commencer à utiliser l'EPRIS, dès que les conditions suivantes sont remplies:

(a) les mesures prévues à l'article 44, paragraphe 7, ont été adoptées;

(b) Europol a déclaré que les essais complets de l'EPRIS qu'elle a menés en coopération avec les autorités des États membres ont été concluants.

3. La Commission fixe, par la voie d'un acte d'exécution, la date à compter de laquelle Europol doit mettre à la disposition des États membres les données biométriques obtenues auprès de pays tiers, conformément à l'article 49, dès que les conditions suivantes sont remplies:

(a) le routeur est en service;

(b) Europol a déclaré que les essais complets de la connexion qu'elle a menés en coopération avec les autorités des États membres et l'eu-LISA ont été concluants.

4. La Commission fixe, par la voie d'un acte d'exécution, la date à compter de laquelle Europol doit avoir accès aux données stockées dans les bases de données des États membres conformément à l'article 50, dès que les conditions suivantes sont remplies:

(a) le routeur est en service;

(b) Europol a déclaré que les essais complets de la connexion qu'elle a menés en coopération avec les autorités des États membres et l'eu-LISA ont été concluants.

Article 75

Dispositions transitoires et dérogations

1. Les États membres et les agences de l'Union commencent à appliquer les articles 21 à 24, l'article 47 et l'article 50, paragraphe 6, à compter de la date fixée conformément à l'article 74, paragraphe 1, premier alinéa, à l'exception des États membres qui n'ont pas commencé à utiliser le routeur.

2. Les États membres et les agences de l'Union commencent à appliquer les articles 25 à 28 et l'article 50, paragraphe 4, à compter de la date fixée conformément à l'article 74, paragraphe 2.

3. Les États membres et les agences de l'Union commencent à appliquer l'article 49 à compter de la date fixée conformément à l'article 74, paragraphe 3.

4. Les États membres et les agences de l'Union commencent à appliquer l'article 50, paragraphes 1, 2, 3, 5 et 7, à compter de la date fixée conformément à l'article 74, paragraphe 4.

Article 76

Procédure de comité

1. La Commission est assistée par un comité. Ce comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique. Lorsque le comité n'émet aucun avis, la Commission n'adopte pas le projet d'acte d'exécution et l'article 5, paragraphe 4, troisième alinéa, du règlement (UE) nº 182/2011 s'applique.

Article 77

Groupe consultatif

Les responsabilités du groupe consultatif sur l'interopérabilité de l'eu-LISA sont étendues de façon à couvrir le routeur. Ce groupe consultatif sur l'interopérabilité apporte à l'eu-LISA son expertise en rapport avec le routeur, notamment dans le contexte de l'élaboration de son programme de travail annuel et de son rapport d'activité annuel.

Article 78

Manuel pratique

La Commission, en étroite coopération avec les États membres, Europol et l'eu-LISA, met à disposition un manuel pratique sur la mise en œuvre et la gestion du présent règlement. Le manuel pratique contient des orientations techniques et opérationnelles, des recommandations et des bonnes pratiques. La Commission adopte le manuel pratique sous la forme d'une recommandation.

Article 79

Suivi et évaluation

1. L'eu-LISA et Europol veillent respectivement à ce que des procédures soient mises en place pour suivre le développement du routeur et de l'EPRIS par rapport aux objectifs fixés en matière de planification et de coûts et suivre le fonctionnement du routeur et de l'EPRIS par rapport aux objectifs fixés en matière de résultats techniques, de coût-efficacité, de sécurité et de qualité du service.

2. Au plus tard [*un an après l'entrée en vigueur du présent règlement*], puis tous les ans pendant la phase de développement du routeur, l'eu-LISA présente au Parlement européen et au Conseil un rapport sur l'état d'avancement du développement du routeur. Ce rapport contient des informations détaillées sur les coûts encourus et des informations sur tout risque susceptible d'avoir une incidence sur les coûts globaux qui sont à la charge du budget général de l'Union conformément à l'article 72.

Une fois le développement du routeur achevé, l'eu-LISA présente au Parlement européen et au Conseil un rapport qui explique en détail la manière dont les objectifs, en particulier ceux ayant trait à la planification et aux coûts, ont été réalisés, et justifie les éventuels écarts.

3. Au plus tard [*un an après l'entrée en vigueur du présent règlement*], puis tous les ans pendant la phase de développement de l'EPRIS, Europol présente au Parlement européen et au Conseil un rapport sur l'état de préparation de la mise en œuvre du présent règlement et sur l'état d'avancement du développement de l'EPRIS, y compris des informations détaillées sur les coûts encourus et des informations sur tout risque susceptible d'avoir une incidence sur les coûts globaux qui sont à la charge du budget général de l'Union conformément à l'article 72.

Une fois le développement de l'EPRIS achevé, Europol présente au Parlement européen et au Conseil un rapport qui explique en détail la manière dont les objectifs, en particulier ceux ayant trait à la planification et aux coûts, ont été réalisés, et justifie les éventuels écarts.

4. Aux fins de la maintenance technique, l'eu-LISA et Europol ont accès aux informations nécessaires concernant les opérations de traitement de données effectuées respectivement dans le routeur et l'EPRIS.

5. Deux ans après la mise en service du routeur, puis tous les deux ans par la suite, l'eu-LISA présente au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique du routeur, y compris sur sa sécurité.

6. Deux ans après la mise en service de l'EPRIS, puis tous les deux ans par la suite, Europol présente au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique de l'EPRIS, y compris sur sa sécurité.

7. Trois ans après la mise en service du routeur et de l'EPRIS visée à l'article 74, puis tous les quatre ans par la suite, la Commission réalise une évaluation globale du mécanisme de Prüm II, qui comprend:

(a) une évaluation de l'application du présent règlement;

(b) un examen des résultats obtenus par rapport aux objectifs du présent règlement et de l'incidence sur les droits fondamentaux;

(c) l'incidence, l'efficacité et l'efficience du fonctionnement du mécanisme de Prüm II et de ses pratiques de travail au regard de ses objectifs, de son mandat et de ses tâches;

(d) une évaluation de la sécurité du mécanisme de Prüm II.

La Commission transmet le rapport d'évaluation au Parlement européen, au Conseil, au Contrôleur européen de la protection des données et à l'Agence des droits fondamentaux de l'Union européenne.

8. Les États membres et Europol communiquent à l'eu-LISA et à la Commission les informations nécessaires à l'établissement des rapports visés aux paragraphes 2 et 5. Ces informations ne peuvent porter préjudice aux méthodes de travail ni comprendre des indications sur les sources, les membres du personnel ou les enquêtes des autorités désignées.

9. Les États membres communiquent à Europol et à la Commission les informations nécessaires à l'établissement des rapports visés aux paragraphes 3 et 6. Ces informations ne peuvent porter préjudice aux méthodes de travail ni comprendre des indications sur les sources, les membres du personnel ou les enquêtes des autorités désignées.

10. Les États membres, l'eu-LISA et Europol communiquent à la Commission les informations nécessaires à la réalisation des évaluations visées au paragraphe 7. Les États membres communiquent également à la Commission le nombre de correspondances confirmées dans la base de données de chaque État membre par catégorie de données.

Article 80

Entrée en vigueur et applicabilité

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Bruxelles, le

Par le Parlement européen
Le président

Par le Conseil
Le président

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE L'INITIATIVE LÉGISLATIVE

1.1. Dénomination de l'initiative législative

Proposition de règlement du Parlement européen et du Conseil relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil

1.2. Domaine(s) politique(s) concerné(s)

Domaine(s) politique(s): affaires intérieures

Activité(s): sécurité

1.3. La proposition porte sur:

☐ **une action nouvelle**

☐ **une action nouvelle suite à un projet pilote/une action préparatoire**[43]

☒ **la prolongation d'une action existante**

☐ **une fusion d'une ou de plusieurs actions vers une autre action/une action nouvelle**

1.4. Objectif(s)

1.4.1. Objectif général / objectifs généraux

Pour répondre aux besoins opérationnels urgents et aux appels du Conseil à envisager une révision des décisions Prüm[44] en vue d'en élargir le champ d'application et de mettre à jour les exigences techniques et juridiques nécessaires, l'initiative devrait renforcer l'échange automatisé de données dans le cadre de Prüm afin d'aider les services répressifs des États membres à lutter contre la criminalité.

1.4.2. Objectif(s) spécifique(s)

L'initiative vise à atteindre les objectifs suivants:

1) **Objectif spécifique I:** Fournir une solution technique pour un échange automatisé de données efficient entre les services répressifs de l'UE afin qu'ils soient informés des données pertinentes disponibles dans la base de données nationale d'un autre État membre;

2) **Objectif spécifique II:** Faire en sorte que tous les services répressifs compétents de l'UE aient accès à des données pertinentes supplémentaires (à savoir les images faciales et les registres de la police) provenant des bases de données nationales d'autres États membres;

3) **Objectif spécifique III:** Faire en sorte que les données pertinentes (en termes de sources de données) provenant de la base de données d'Europol soient mises à la disposition des services répressifs nationaux et qu'Europol exploite tout le potentiel de ses données;

[43] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

[44] Décisions 2008/615/JAI et 2008/616/JAI du Conseil.

4) **Objectif spécifique IV:** Fournir aux services répressifs un accès efficient aux données réelles correspondant à une concordance («hit») qui sont disponibles dans la base de données nationale d'un autre État membre ou auprès d'Europol.

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que l'initiative législative devrait avoir sur les bénéficiaires/la population visée.

L'initiative s'attaquera effectivement aux problèmes recensés et renforcera le cadre actuel de Prüm au moyen de capacités supplémentaires ciblées et solides, afin d'intensifier son soutien aux États membres pour renforcer l'échange d'informations, avec pour objectif final de prévenir les infractions pénales et terroristes et d'enquêter sur celles-ci, dans le plein respect des droits fondamentaux.

Les bénéficiaires finaux de toutes les options privilégiées sont les **citoyens**, qui bénéficieront directement et indirectement **d'une meilleure lutte contre la criminalité et d'une baisse des taux de criminalité**. Sur le plan de l'efficience, les principaux bénéficiaires sont les **services répressifs nationaux**. L'initiative apporte des solutions efficientes à des problèmes dont la résolution coûterait sinon plus cher ou serait moins efficiente.

1.4.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations.

Le développement du routeur et du système d'index européen des registres de la police (EPRIS) débutera dès que les conditions préalables auront été remplies, c'est-à-dire lorsque la proposition législative aura été adoptée par les colégislateurs et que les conditions techniques préalables seront remplies. Alors que les travaux sur le routeur commencent sous la forme d'un nouveau projet, les travaux sur l'EPRIS devraient s'appuyer sur l'actuel projet ADEP.EPRIS.

Objectif spécifique: le système doit être prêt à être mis en service à la date d'échéance cible

D'ici à 2023, la proposition sera envoyée aux colégislateurs pour adoption. Il est supposé que le processus d'adoption sera achevé en 2024, par analogie avec le temps nécessaire pour d'autres propositions.

Dans cette hypothèse, le lancement de la période de développement est fixé au début de 2025 (= T0) afin d'avoir un point de référence à partir duquel les durées sont comptées et non des dates absolues. Si l'adoption par les colégislateurs intervient à une date ultérieure, le calendrier sera décalé en conséquence.

Le développement du routeur et de l'EPRIS devrait avoir lieu en 2025 et 2026, la mise en service étant prévue pour 2027.

Les principaux indicateurs mentionnés ci-après permettront de suivre la réalisation et la performance des objectifs spécifiques:

Objectif spécifique I: Fournir une solution technique pour un échange automatisé de données efficient.

- Nombre de cas d'utilisation (= nombre de demandes de requêtes pouvant être traitées par le routeur) par période de temps.

Nombre de cas d'utilisation (= nombre de demandes de requêtes pouvant être traitées par l'EPRIS) par période de temps.

Objectif spécifique II: faire en sorte que des données pertinentes supplémentaires soient disponibles

- Nombre de demandes de requêtes à l'aide d'images faciales
- Nombre de demandes de requêtes à l'aide de registres de la police

- Nombre de correspondances à la suite de requêtes effectuées à l'aide d'images faciales

- Nombre de correspondances à la suite de requêtes effectuées à l'aide de registres de la police

Objectif spécifique III: Faire en sorte que les données pertinentes (en termes de sources de données) provenant de la base de données d'Europol soient mises à la disposition des services répressifs nationaux et qu'Europol exploite tout le potentiel de ses données.

- Nombre de demandes de requêtes de données biométriques d'Europol provenant de pays tiers

- Nombre de correspondances avec des données biométriques d'Europol provenant de pays tiers

- Nombre de demandes de requêtes émises par Europol

- Nombre de correspondances résultant de demandes de requêtes émises par Europol

Objectif spécifique IV: Fournir aux services répressifs un accès efficient aux données réelles correspondant à une concordance qui sont disponibles dans la base de données nationale d'un autre État membre ou auprès d'Europol.

- Nombre de correspondances à la suite de demandes de requêtes par rapport au nombre de fois où l'échange de données de base a été demandé

1.5. Justification(s) de l'initiative législative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative législative

La mise en œuvre de l'initiative législative nécessite des mesures techniques et procédurales au niveau de l'UE et des États membres, lesquelles devraient être appliquées dès l'entrée en vigueur de la législation révisée. Les ressources concernées – en particulier les ressources humaines – devraient être revues à la hausse au fil du temps, en fonction des mesures.

Les principales actions devant être entreprises à la suite de l'entrée en vigueur de la proposition sont les suivantes:

Pour créer le routeur Prüm:

Atteindre l'objectif consistant à fournir aux utilisateurs Prüm II une connexion unique à toutes les bases de données des États membres et aux données d'Europol pour envoyer des demandes de requêtes à l'aide de données biométriques.

Prévoir un nouveau processus de suivi au niveau de l'UE avec un échange semi-automatisé de données réelles correspondant à une concordance.

Créer/élargir l'EPRIS

Atteindre l'objectif consistant à fournir aux utilisateurs Prüm II une connexion unique à toutes les bases de données des États membres participants contenant des registres de la police pour envoyer des demandes de requêtes à l'aide de registres de police.

Permettre aux États membres d'échanger de nouvelles catégories de données

Permettre l'échange d'images faciales et de registres de la police via Prüm II.

Permettre aux États membres de vérifier automatiquement des données provenant de pays tiers auprès d'Europol dans le cadre de Prüm:

Permettre aux États membres de vérifier des données biométriques provenant de pays tiers via Prüm II.

Permettre à Europol de vérifier des données provenant de pays tiers dans les bases de données nationales des États membres:

Permettre à Europol d'utiliser des données provenant de pays tiers pour effectuer des recherches dans les bases de données des États membres via Prüm II.

Les objectifs devant tous être atteints, la solution globale réside dans une combinaison des éléments indiqués ci-dessus.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

Les formes graves de criminalité et le terrorisme présentent un caractère transnational. Une action menée au niveau national ne peut donc y répondre efficacement à elle seule. C'est pourquoi les États membres choisissent de travailler ensemble, dans le cadre de l'Union européenne, afin de faire face aux menaces que représentent les formes graves de criminalité et le terrorisme.

Par ailleurs, l'évolution des menaces pour la sécurité, stimulée par les diverses manières dont les criminels exploitent les avantages offerts par la transformation numérique, la mondialisation et la mobilité, impose également de soutenir efficacement, au niveau de l'UE, les travaux des services répressifs nationaux. Une action de l'UE constitue un moyen effectif et efficient de renforcer le soutien apporté aux États membres pour lutter contre les formes graves de criminalité et le terrorisme afin de s'adapter à l'évolution de ces menaces.

La proposition permettra de réaliser d'importantes économies d'échelle en transférant, du niveau national vers Europol, les tâches et les services qui peuvent être exécutés plus efficacement au niveau de l'UE. La proposition apporte donc des solutions efficientes à des problèmes dont la résolution coûterait plus cher s'il fallait utiliser 27 solutions nationales différentes, ou à des problèmes impossibles à traiter au niveau national en raison de leur caractère transnational.

1.5.3. Leçons tirées d'expériences similaires

L'évaluation des décisions Prüm a montré que:

- Le cadre de Prüm est pertinent compte tenu des besoins et défis actuels et futurs liés à la sécurité et plus précisément aux enquêtes pénales. La coopération et l'échange d'informations entre les services répressifs des États membres, ainsi que la possibilité de consulter et de comparer les données relatives à l'ADN, aux empreintes digitales et à l'immatriculation des véhicules dans les bases de données d'autres États membres aux fins de la prévention des infractions pénales et des enquêtes en la matière, sont jugés d'une importance capitale pour la sauvegarde de la sécurité intérieure de l'UE et de la sécurité de ses citoyens.

- Le concept des décisions Prüm répond aux besoins des enquêteurs criminels, des victimes de la criminalité, des spécialistes de la criminalistique, des détenteurs de bases de données et des praticiens du droit en ce qui concerne les catégories de données disponibles dans les limites de ce cadre.

- En évitant la nécessité d'interroger bilatéralement chaque État membre, l'échange automatisé de données dans le cadre de Prüm permet des gains d'efficacité dans l'échange d'informations en matière répressive puisqu'il accélère les échanges et réduit dans une certaine mesure la charge administrative. L'on a constaté que ces avantages l'emportent sur les investissements nécessaires à la mise en œuvre du cadre de Prüm. En outre, le système automatisé Prüm permet de réaliser d'importantes économies en termes de temps de travail. Il subsiste toutefois une charge administrative liée à la vérification des concordances et des rapports, ainsi qu'à la réception/transmission des informations relevant de la seconde étape.

- Des évolutions et des changements considérables ont également pris forme en ce qui concerne le cadre juridique de l'UE, les besoins opérationnels et les possibilités en matière technique et de criminalistique depuis l'adoption des décisions Prüm en 2008. Plusieurs initiatives et systèmes de l'UE et internationaux visant à faciliter l'échange d'informations entre les services répressifs ont été mis au point. Il existe essentiellement des complémentarités entre les décisions Prüm et d'autres actes législatifs de l'UE/internationaux pertinents, y compris le cadre d'interopérabilité. Des complémentarités existent également avec certains systèmes d'information centraux de l'UE qui ont des finalités différentes. Des synergies potentielles peuvent être trouvées en ce qui concerne Europol et le cadre d'interopérabilité.

- Cependant, la mise en œuvre des décisions Prüm est lente. En effet, près de dix ans après la date limite de mise en œuvre du 26 août 2011, les États membres n'ont pas tous achevé la procédure d'évaluation et un certain nombre de liens bilatéraux n'ont pas été établis en raison de la complexité technique et des importantes ressources financières et humaines qui sont nécessaires. Par conséquent, les demandes de requêtes ne peuvent pas faire l'objet d'une vérification dans les données de certains États membres si la connexion bilatérale correspondante n'a pas été établie. Cela limite la capacité d'identification des criminels et de détection des liens transfrontières entre les infractions, ce qui entrave l'échange d'informations et le fonctionnement du système Prüm.

- Le fait que les suites données aux concordances en vertu du cadre de Prüm s'effectue en application du droit national et, donc, en dehors du champ d'application des décisions Prüm, est également considéré comme un problème qui entrave le fonctionnement du système Prüm. En effet, en raison des différences entre les règles et procédures nationales, l'échange de données relatives aux suites données aux concordances est fragmenté dans la mesure où il faut parfois des semaines, voire des mois, pour recevoir les informations pertinentes qui sont à l'origine d'une concordance.

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

Les investissements requis au niveau de l'UE sont compatibles avec le cadre financier pluriannuel 2021-2027, le financement étant assuré dans la rubrique «Sécurité et défense» et la rubrique «Migration et frontières».

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

Les crédits nécessaires pour financer le développement du cadre de Prüm II n'ont pas été prévus dans le cadre des dotations du CFP pour Europol et l'eu-LISA, étant donné que la présente proposition est nouvelle et que les montants correspondants n'étaient pas connus au moment de la présentation de la proposition. Il est proposé d'augmenter les dotations d'Europol et d'eu-LISA pour les années 2024, 2025, 2026 et 2027 par des réductions correspondantes du Fonds pour la sécurité intérieure (FSI) et de l'instrument relatif à la gestion des frontières et à la politique des visas (IGFV), respectivement.

1.6. Durée et incidence financière de l'initiative législative

☐ **durée limitée**

☐ Proposition/initiative en vigueur à partir de [JJ/MM]AAAA jusqu'en [JJ/MM]AAAA

☐ Incidence financière de AAAA jusqu'en AAAA

☒ **durée illimitée**

Mise en œuvre avec une période de montée en puissance de 2024 jusqu'en 2026,

puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[45]

☒ **Gestion directe** par la Commission

– X dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives

☒ **Gestion partagée** avec les États membres

☒ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

☐ à des organisations internationales et à leurs agences (à préciser);

☐ à la BEI et au Fonds européen d'investissement;

☒ aux organismes visés aux articles 70 et 71;

☐ à des organismes de droit public;

☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

Remarques

Périodes	Phase de développement	Phase de fonctionnement	Mode de gestion	Acteur
Développement et maintenance (du routeur et de l'EPRIS)	X	X	Indirecte	eu-LISA Europol
Adaptation des bases de données Europol	X	X	Indirecte	Europol

[45] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Périodes	Phase de développement	Phase de fonctionnement	Mode de gestion	Acteur
Développement ou amélioration des bases de données nationales existantes, intégration des systèmes nationaux	X	X	Partagée (ou directe)	COM + États membres

La période de développement débute en 2024 et dure jusqu'à la réalisation de chaque élément de l'initiative, de 2024 à 2027.

1. Gestion directe par la DG HOME: pendant la période de développement, si nécessaire, des mesures peuvent également être mises en œuvre directement par la Commission. Il pourrait s'agir, en particulier, d'un soutien financier de l'Union à certaines activités sous forme de subventions (y compris aux autorités nationales des États membres), de marchés publics et/ou du remboursement des coûts supportés par des experts externes.

2. Gestion partagée: Au cours de la phase de développement, les États membres seront tenus d'adapter leurs systèmes nationaux afin de se connecter au routeur et à l'EPRIS et de prendre les mesures nécessaires pour assurer l'échange d'images faciales et de registres de la police.

3. Gestion indirecte: l'eu-LISA et Europol se chargeront du développement des volets informatiques du projet, à savoir, respectivement, le routeur et l'EPRIS. Cela comprend toute modification nécessaire de leur architecture existante afin d'offrir les capacités décrites dans la proposition.

Pendant la période de fonctionnement, l'eu-LISA et Europol se chargeront de l'ensemble des activités techniques liées à la maintenance du routeur et de l'EPRIS, respectivement.

Europol assurera le développement et la maintenance de ses systèmes afin de garantir la disponibilité de leurs données dans le contexte du cadre de Prüm.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

L'eu-LISA et Europol veillent, respectivement, à ce que des procédures soient mises en place pour suivre le développement du routeur et de l'EPRIS par rapport aux objectifs fixés en matière de planification et de coûts et suivre le fonctionnement du routeur et de l'EPRIS par rapport aux objectifs fixés en matière de résultats techniques, de coût-efficacité, de sécurité et de qualité du service.

Au plus tard un an après l'adoption du règlement proposé, puis tous les ans durant la phase de développement du routeur, l'eu-LISA présente un rapport au Parlement européen et au Conseil sur l'état d'avancement du développement du routeur. Ce rapport contient des informations détaillées sur les coûts encourus et des informations sur tout risque susceptible d'avoir une incidence sur les coûts globaux qui sont à la charge du budget général de l'Union.

Une fois le développement du routeur achevé, l'eu-LISA soumet au Parlement européen et au Conseil un rapport qui explique en détail la manière dont les objectifs, en particulier ceux ayant trait à la planification et aux coûts, ont été atteints, et justifie les éventuels écarts.

Au plus tard un an après l'adoption du règlement proposé, puis tous les ans durant la phase de développement de l'EPRIS, Europol présente au Parlement européen et au Conseil un rapport sur l'état d'avancement des préparations pour la mise en œuvre du présent règlement et sur l'état d'avancement du développement de l'EPRIS, y compris des informations détaillées sur les coûts encourus et des informations sur tout risque susceptible d'avoir une incidence sur les coûts globaux qui sont à la charge du budget général de l'Union.

Une fois le développement de l'EPRIS achevé, Europol soumet au Parlement européen et au Conseil un rapport qui explique en détail la manière dont les objectifs, en particulier ceux ayant trait à la planification et aux coûts, ont été atteints, et justifie les éventuels écarts.

Aux fins de la maintenance technique, l'eu-LISA et Europol ont accès aux informations nécessaires concernant les opérations de traitement de données effectuées, respectivement, dans le routeur et l'EPRIS.

Deux ans après la mise en service du routeur, puis tous les deux ans par la suite, l'eu-LISA présente au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique du routeur, y compris sur sa sécurité.

Deux ans après la mise en service de l'EPRIS, puis tous les deux ans par la suite, Europol présente au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique de l'EPRIS, y compris sur sa sécurité.

Trois ans après la mise en service de tous les éléments du règlement proposé, puis tous les quatre ans, la Commission présente une évaluation globale du cadre de Prüm II, comprenant:

(a) une évaluation de l'application du règlement;

(b) un examen des résultats obtenus par rapport aux objectifs fixés dans le règlement et de son impact sur les droits fondamentaux;

(c) l'incidence, l'efficacité et l'efficience du fonctionnement de Prüm II et de ses pratiques de travail au regard de ses objectifs, de son mandat et de ses missions;

(d) une évaluation de la sécurité de Prüm II.

La Commission transmet le rapport d'évaluation au Parlement européen, au Conseil, au Contrôleur européen de la protection des données et à l'Agence des droits fondamentaux de l'Union européenne.

Les États membres et Europol communiquent à l'eu-LISA et à la Commission les informations nécessaires à l'établissement des rapports susmentionnés. Ces informations ne peuvent porter préjudice aux méthodes de travail ni comprendre des indications sur les sources, les membres du personnel ou les enquêtes des autorités désignées.

Les États membres communiquent à Europol et à la Commission les informations nécessaires à l'élaboration des rapports susmentionnés. Ces informations ne peuvent porter préjudice aux méthodes de travail ni comprendre des indications sur les sources, les membres du personnel ou les enquêtes des autorités désignées.

L'eu-LISA et Europol communiquent à la Commission les informations nécessaires à l'élaboration de ses évaluations.

2.2. Système(s) de gestion et de contrôle

2.2.1. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

Les risques suivants ont été recensés:

- pression sur les ressources opérationnelles en raison de l'augmentation des flux de données et de l'évolution constante de la situation en matière d'activités criminelles;

- multiplication des tâches et des demandes tant pour l'eu-LISA que pour Europol;

- insuffisance des ressources humaines et financières par rapport aux besoins opérationnels;

- manque de ressources informatiques, entraînant des retards dans les développements et mises à jour nécessaires du système central;

- risques liés au traitement par Europol de données à caractère personnel et nécessité d'évaluer et d'adapter régulièrement les garanties techniques et procédurales afin d'assurer la protection des données à caractère personnel et des droits fondamentaux;

- interdépendance entre les préparatifs que l'eu-LISA doit effectuer en ce qui concerne le routeur et les préparatifs que les États membres et Europol doivent effectuer en ce qui concerne la mise en place d'une interface technique pour la transmission des données via le routeur.

Ces risques peuvent être atténués par l'application de techniques de gestion de projet, notamment en prévoyant des mesures d'urgence dans les projets de développement et une dotation en personnel suffisante pour pouvoir absorber les pics de travail. En effet, l'effort est généralement estimé en supposant que la charge de travail est uniformément répartie dans le temps, alors que la réalité des projets consiste en une charge de travail inégale qui est absorbée par des allocations de ressources plus élevées.

Le recours à un prestataire externe pour ces travaux de développement comporte plusieurs risques, en particulier:

1. le risque que le prestataire n'alloue pas des ressources suffisantes au projet ou qu'il conçoive et développe un système qui ne soit pas du dernier cri;

2. le risque que les techniques et modalités administratives applicables aux systèmes d'information à grande échelle ne soient pas intégralement respectées, le prestataire y voyant un moyen de réduire les coûts;

3. le risque que le prestataire se heurte à des difficultés financières pour des raisons étrangères au projet.

Ces risques sont atténués par l'attribution de contrats sur la base de critères de qualité rigoureux, la vérification des références des prestataires et le maintien d'une relation étroite avec eux. Enfin, en dernier recours, des clauses de pénalité et de résiliation sévères peuvent être incluses et appliquées au besoin.

Europol met en œuvre un cadre de contrôle interne spécifique fondé sur le cadre de contrôle interne de la Commission européenne et sur le cadre de contrôle interne intégré établi à l'origine par le comité des organisations de sponsoring (Committee of Sponsoring Organisations). Le document unique de programmation doit fournir des informations sur les systèmes de contrôle interne, tandis que le rapport d'activité annuel consolidé (RAAC) doit contenir des informations sur l'efficience et l'efficacité des systèmes de contrôle interne, y compris en ce qui concerne l'évaluation des risques. D'après le RAAC de 2019, sur la base de l'analyse des éléments du contrôle interne et des principes qui ont fait l'objet d'un suivi durant l'année 2019, en utilisant à la fois des éléments quantitatifs et qualitatifs, le système de contrôle interne d'Europol est considéré comme étant présent et fonctionnant de manière intégrée dans l'ensemble de l'Agence.

Pour le budget exécuté par l'eu-LISA, un cadre de contrôle interne spécifique fondé sur le cadre de contrôle interne de la Commission européenne est nécessaire. Le document unique de programmation doit fournir des informations sur les systèmes de contrôle interne, tandis que le rapport d'activité annuel consolidé (RAAC) doit contenir des informations sur l'efficience et l'efficacité des systèmes de contrôle interne, y compris en ce qui concerne l'évaluation des risques. Le RAAC 2019 indique que la direction de l'Agence a une assurance raisonnable quant au fait que des contrôles internes appropriés sont en place et fonctionnent conformément aux attentes. Tout au long de l'année, les principaux risques ont été adéquatement recensés et gérés. Cette assurance est en outre confirmée par les résultats des audits internes et externes réalisés.

Tant pour Europol que pour l'eu-LISA, un niveau supplémentaire de supervision interne est également assuré par la structure d'audit interne d'Europol, sur la base d'un plan d'audit annuel, en tenant compte notamment de l'évaluation des risques au sein d'Europol. Cette structure d'audit interne aide Europol à atteindre ses objectifs en fournissant une méthode systématique et structurée pour évaluer l'efficacité des processus de gestion des risques, de contrôle et de gouvernance, ainsi qu'en publiant des recommandations en vue de l'amélioration de ces processus.

En outre, le contrôleur européen de la protection des données (CEPD) et le délégué à la protection des données dans les deux agences (une fonction indépendante rattachée directement au secrétariat du conseil d'administration) supervisent le traitement de données à caractère personnel par les agences.

Enfin, en tant que direction générale partenaire d'Europol et de l'eu-LISA, la DG HOME procède chaque année à un exercice de gestion des risques afin de détecter et d'évaluer les éventuels risques majeurs liés aux activités des agences. Les risques jugés critiques sont signalés chaque année dans le plan de gestion de la DG HOME et sont accompagnés d'un plan d'action spécifiant la mesure d'atténuation.

2.2.2. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

Le rapport «coûts du contrôle/valeur des fonds concernés gérés» est présenté par la Commission. Le RAA 2020 de la DG HOME fait état de 0,21 % pour ce rapport en ce qui concerne les entités chargées de la gestion indirecte et les agences décentralisées, y compris Europol et l'eu-LISA.

La Cour des comptes européenne a confirmé la légalité et la régularité des comptes annuels d'Europol et de l'eu-LISA pour 2019, qui présentent un taux d'erreur inférieur à 2 %. Rien n'indique que le taux d'erreur se détériorera dans les années à venir.

Par ailleurs, tant pour Europol que pour l'eu-LISA, l'article 80 de leurs règlements financiers respectifs prévoit la possibilité pour l'agence de partager une structure d'audit interne avec d'autres organismes de l'Union œuvrant dans le même domaine d'activité si la structure d'audit interne d'un organisme de l'Union ne présente pas un bon rapport coût/efficacité.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.

Les mesures prévues pour lutter contre la fraude sont exposées à l'article 35 du règlement (UE) nº 1077/2011.

Les mesures relatives à la lutte contre la fraude, la corruption et toute autre activité illégale sont décrites, notamment, à l'article 66 du règlement Europol et au titre X du règlement financier d'Europol.

Europol prend notamment part aux activités de prévention de la fraude de l'Office européen de lutte antifraude et informe sans délai la Commission des cas présumés de fraude et autres irrégularités financières, conformément à sa stratégie antifraude interne.

Une mise à jour de la stratégie antifraude d'Europol a été adoptée par le conseil d'administration en 2020.

Les mesures en lien avec la lutte contre la fraude, la corruption et toutes autres activités illégales sont mises en évidence, entre autres, à l'article 50 du règlement relatif à l'eu-LISA et sous le titre X du règlement financier de l'eu-LISA.

L'eu-LISA participe notamment aux activités de prévention de la fraude de l'Office européen de lutte antifraude et informe sans retard la Commission des cas présumés de fraude et autres irrégularités financières, conformément à sa stratégie interne de lutte antifraude.

Par ailleurs, en tant que direction générale partenaire, la DG HOME a élaboré et mis en œuvre sa propre stratégie antifraude sur la base de la méthode fournie par l'OLAF. Les agences décentralisées, y compris Europol et l'-eu-LISA, relèvent de cette stratégie. Dans son RAA de 2020, la DG HOME a conclu que les processus de prévention et de détection des cas de fraude fonctionnaient de manière satisfaisante et contribuaient dès lors à assurer la réalisation des objectifs de contrôle interne.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE L'INITIATIVE LÉGISLATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro	CD/CND[46]	de pays AELE[47]	de pays candidats[48]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du

[46] CD CD = crédits dissociés / CND = crédits non dissociés.

[47] AELE: Association européenne de libre-échange.

[48] Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

						règlement financier

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Contribution			
	Numéro	CD/CND	de pays AELE	de pays candidats	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
5	12.02.01 – Fonds pour la sécurité intérieure	CD	NON	NON	NON	NON
5	12.01.01 – Dépenses d'appui en faveur du Fonds pour la sécurité intérieure	CND	NON	NON	NON	NON
5	12.10.01 – Agence de l'Union européenne pour la coopération des services répressifs (Europol)	CND	NON	NON	NON	NON
4	11.10.02 – Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA)	CND	NON	NON	NON	NON

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	5	Sécurité et défense

Europol			Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Titre 1: Dépenses de personnel	Engagements	(1)		0,551	1,102	0,847	0,847	**3,347**
	Paiements	(2)		0,551	1,102	0,847	0,847	**3,347**
Titre 2: Dépenses d'infrastructure et de fonctionnement	Engagements	(1a)		1,49	1,052	0,516	0,516	**3,574**
	Paiements	(2a)		1,49	1,052	0,516	0,516	**3,574**
Titre 3: Dépenses opérationnelles	Engagements	(3a)						
	Paiements	(3b)						
TOTAL des crédits pour Europol	Engagements	=1+1a +3a		**2,041**	**2,154**	**1,363**	**1,363**	**6,921**
	Paiements	=2+2a +3b		**2,041**	**2,154**	**1,363**	**1,363**	**6,921**

Remarque: les crédits supplémentaires demandés dans le contexte de la présente proposition pour Europol seront couverts par le Fonds pour la sécurité intérieure (FSI) au titre de la rubrique 5.

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	4	–Migration et frontières

eu-LISA			Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Titre 1: Dépenses de personnel	Engagements	(1)		0,456	0,988	1,52	1,45	**4,414**
	Paiements	(2)		0,456	0,988	1,52	1,45	**4,414**
Titre 2: Dépenses d'infrastructure et de fonctionnement	Engagements	(1a)		4,15	3,55	1,4	0	**9,1**
	Paiements	(2a)		4,15	3,55	1,4	0	**9,1**
Titre 3: Dépenses opérationnelles	Engagements	(3a)		0	0	1	1,2	**2,2**
	Paiements	(3b)		0	0	1	1,2	**2,2**
TOTAL des crédits pour l'eu-LISA	Engagements	=1+1a +3a		**4,606**	**4,538**	**3,92**	**2,65**	**15,714**
	Paiements	=2+2a +3b		**4,606**	**4,538**	**3,92**	**2,65**	**15,714**

Remarque: les crédits supplémentaires demandés dans le cadre de la présente proposition pour l'eu-LISA seront couverts par l'instrument relatif à la gestion des frontières et à la politique des visas (IGFV) au titre de la rubrique 4.

Rubrique du cadre financier pluriannuel	5	Résilience, Sécurité et Défense

DG Migration et affaires intérieures			Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Fonds pour la sécurité intérieure	Engagements	(1)		13,64	40	40		**93,64**
	Paiements	(2)		4,68	6,55	9,39		**34,65**
TOTAL des crédits pour la DG HOME	Engagements			13,64	40	40		**93,64**
	Paiements			4,68	6,55	9,39		**34,65**

Remarque: les crédits demandés dans le contexte de la proposition seront couverts par des crédits déjà prévus dans la fiche financière législative du règlement sur le FSI. Aucune ressource financière ou humaine supplémentaire n'est requise dans le cadre de cette proposition législative.

Les coûts par État membre comprennent:

- la modernisation de leur infrastructure pour soutenir l'échange de services web et la mise en place de la connexion avec le routeur central, ce qui implique des efforts d'analyse et de définition du nouveau paysage architectural;
- la mise à niveau de leur infrastructure afin de faciliter l'échange de services web et la mise en place de la connexion avec le routeur central;
- la configuration d'un système d'échange de services web et la mise en place de la connexion avec le routeur central;
- la conception d'une nouvelle architecture nationale et des spécifications pour garantir l'accès aux données nationales par l'intermédiaire des solutions développées (routeur et EPRIS);
- la mise en place d'un nouvel indice ou la mise à disposition d'un indice déjà existant pour l'échange de registres de la police;

- la mise en place d'une nouvelle base de données d'images faciales ou la mise à disposition d'une base de données d'images faciales déjà existante aux fins d'échanges;
- l'intégration de la solution nationale;
- les coûts génériques liés à la gestion du projet.

Le tableau suivant indique les coûts par catégorie:

Indiquer les objectifs et les réalisations **DG Home** ⇩			Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type		Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
Routeur	Connexion au routeur des bases de données existantes				26	2,314	26	6,787	26	6,787			26	15,89
Images faciales	Création d'une nouvelle base de données				13 *	2,84	13	8,329	13	8,329			13	19,5
	Connexion de la base de données au routeur				26	2,72	26	7,996	26	7,996			26	18,72

Registres de la police	Création d'une base de données des registres de la police et connexion à l'EPRIS			26	5,763	26	16,959	26	16,959			26	39,7
Total					**13,64**		**40**		**40**				**93,64**

*Nombre estimé d'États membres sans base de données d'images faciales

Rubrique du cadre financier pluriannuel	**7**	«Dépenses administratives»

En Mio EUR (à la 3e décimale)

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
DG: HOME							
• Ressources humaines			0,608	0,684	0,608	0,608	**2,508**
• Autres dépenses administratives			0,225	0,225	0,186	0,186	0,822
TOTAL DG HOME	Crédits						

TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total engagements = Total paiements)	0,833	0,833	0,794	0,794	**3,330**	

En Mio EUR (à la 3e décimale)

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
TOTAL des crédits	Engagements		20,287	46,692	45,283	4,013	**116,275**

pour les RUBRIQUES 1 à 5 du cadre financier pluriannuel	Paiements		11,329	13,247	14,647	18,059	**57,282**

3.2.2. Incidence estimée sur les crédits d'Europol

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

☒ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations			Année		Année		Année		Année		Année		TOTAL	
			2023		**2024**		**2025**		**2026**		**2027**			
⇩	Type	Coût moyen[49]	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût
Coûts pour Europol (non liés aux ressources humaines)														
- Réalisation	Infrastructure et maintenance					0,764		0,326		0,226		0,226		1,542
- Réalisation	Prestataires					0,726		0,726		0,290		0,290		2,032
COÛT TOTAL						1,490		1,052		0,516		0,516		3,574

[49] Compte tenu de la nature opérationnelle particulière de ces réalisations, il n'est pas possible de déterminer un coût unitaire précis pour chacune d'entre elles ni un volume exact attendu de réalisations, notamment car certaines d'entre elles concernent des activités répressives qui doivent s'adapter à des activités criminelles imprévisibles.

3.2.3. Incidence estimée sur les crédits de l'eu-LISA

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

☒ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations			Année		Année		Année		Année		Année		TOTAL	
			2023		**2024**		**2025**		**2026**		**2027**			
⇩	Type	Coût moyen[50]	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût
Coûts pour l'eu-LISA (non liés aux ressources humaines)														
- Réalisation	Infrastructure[51]					1,85		2,15		0,7		0		4,7

[50] Compte tenu de la nature opérationnelle particulière de ces réalisations, il n'est pas possible de déterminer un coût unitaire précis pour chacune d'entre elles ni un volume exact attendu de réalisations, notamment car certaines d'entre elles concernent des activités répressives qui doivent s'adapter à des activités criminelles imprévisibles.

[51] Comprend le matériel informatique, les logiciels, la fourniture de réseaux, la sécurité.

- Réalisation	Prestataires[52]					1,4		0,7		0,7		0		2,8
- Réalisation	Mécanisme de mise en correspondance micro					0,9		0,7		0		0		
- Réalisation	Maintenance					0		0		1		1,2		2,2
COÛT TOTAL						4,15		3,55		2,4		1,2		11,3

[52] Comprend les coûts des services professionnels, de conception et des essais.

3.2.4. Incidence estimée sur les ressources humaines d'Europol

3.2.4.1. Synthèse

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Agents temporaires – Nombre de référence						
Agents temporaires – Agents supplémentaires par rapport au nombre de référence (nombre cumulé)	0	0,551	1,101	0,847	0,847	**3,347**
Agents temporaires – TOTAL						
Agents contractuels – Nombre de référence						
Experts nationaux détachés – Nombre de référence (demande figurant dans le projet de budget 2021)						
TOTAL – Coûts supplémentaires uniquement	0	0,551	1,101	0,847	0,847	**3,347**
TOTAL – Incluant la valeur de référence et les coûts supplémentaires						

Besoins en personnel (ETP):

	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**
Agents temporaires – Nombre de référence	**0**	**9,5**	**9,5**	**21,5**	**19,5**
Agents temporaires – Agents supplémentaires par rapport au nombre de référence (nombre cumulé)	0	6,5	6,5	5	5

Agents temporaires – TOTAL		**16**	**16**	**26,5**	**24,5**
Agents contractuels					
Experts nationaux détachés					
TOTAL	**0**	**16,5**	**16,5**	**26,5**	**24,5**

Les ressources humaines nécessaires à la réalisation des objectifs de la proposition ont été estimées en coopération avec Europol. Ces estimations tiennent compte de l'augmentation attendue de la charge de travail à mesure que les parties intéressées auront de plus en plus recours aux services d'Europol au fil du temps, ainsi que du temps nécessaire à Europol pour absorber les ressources afin d'éviter une situation dans laquelle l'Agence ne serait pas en mesure de mettre pleinement en œuvre la contribution de l'UE et d'engager les crédits en temps voulu.

Les ressources humaines nécessaires à la mise en œuvre des objectifs de la proposition seront partiellement couvertes par le personnel existant au sein d'Europol (niveau de référence) et en partie par des ressources supplémentaires (personnel supplémentaire par rapport au scénario de référence).

Aucune augmentation du nombre d'agents contractuels n'est prévue dans la FFL.

Pour la mise en œuvre de Prüm II, les ressources nécessaires à Europol peuvent être réparties en 3 catégories:

1) les coûts des TIC pour la connexion au routeur biométrique de l'eu-LISA, les travaux de développement nécessaires dans les systèmes d'information d'Europol afin de rendre accessibles les données provenant de tiers aux fins de recherches effectuées par les États membres et d'intégrer les recherches dans Prüm avec les données de tiers dans l'interface de recherche unique USE-UI d'Europol,

2) les coûts liés au personnel de la direction des opérations d'Europol chargé d'effectuer les recherches avec des données provenant de tiers et aux experts en biométrie chargés de vérifier les concordances,

3) l'hébergement d'un routeur central pour les registres de la police. Il s'agira notamment de coûts ponctuels pour le matériel (y compris différents environnements de production et d'essai pour les États membres), du personnel chargé des TIC chargé d'assurer le développement et la gestion des modifications du logiciel ADEP.EPRIS, des essais avec les États membres, d'un service d'assistance 24/7 pour aider les États membres en cas de problème. Afin de garantir un soutien total aux États membres, il est nécessaire de disposer de profils différents au sein du personnel chargé des TIC, par exemple des agents pour la coordination générale, des ingénieurs pour la spécification des exigences, des développeurs, des testeurs, des administrateurs de système. Il est prévu que le personnel chargé des TIC soit légèrement plus nombreux au cours de la première année après la mise en service.

En raison des contraintes de sécurité et du plafond convenu pour les agents contractuels, la majorité des tâches liées à Prüm doivent être exécutées par le personnel d'Europol. Certaines activités moins sensibles devraient être sous-traitées à des contractants (essais, certaines tâches de développement).

Agents temporaires en ETP (nombre de référence + agents supplémentaires)	**2023**	**2024**	**2025**	**2026**	**2027**
Gestion de projet		1,0	1,0	0,5	0,5
Experts (total)		14,5	14,5	18,0	16,0
• ***Biométrie***		*1,0*	*1,0*	*4,0*	*4,0*
• ***Personnel opérationnel***		*0,5*	*0,5*	*4,0*	*4,0*
• ***TIC***		*13,0*	*13,0*	*10,0*	*8,0*
Service d'assistance/suivi		0,0	0,0	7,0	7,0
Coordination générale		1,0	1,0	1,0	1,0
Total		**16,5**	**16,5**	**26,5**	**24,5**

3.2.5. Incidence estimée sur les ressources humaines de l'eu-LISA

3.2.5.1. Synthèse

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Agents temporaires – Nombre de référence						
Agents temporaires – Agents supplémentaires par rapport au nombre de référence (nombre cumulé)		0,456	0,988	1,52	1,368	**4,332**
Agents temporaires – TOTAL						
Agents contractuels – Nombre de référence						
Agents contractuels – Agents supplémentaires					0,082	**0,082**
Experts nationaux détachés – Nombre de référence (demande figurant dans le projet de budget 2021)[53]						
TOTAL – Coûts supplémentaires uniquement		0,456	0,988	1,52	1,45	**4,414**
TOTAL – Incluant la valeur de référence et les coûts supplémentaires						

Besoins en personnel (ETP):

	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**

[53] Niveaux des effectifs indiqués dans le projet de budget 2021, calculés sur la base des coûts unitaires moyens du personnel à utiliser pour la FFL. La moitié des crédits annuels correspondants sont calculés pour l'année au cours de laquelle le personnel est recruté.

Agents temporaires – Nombre de référence					
Agents temporaires – Agents supplémentaires par rapport au nombre de référence (nombre cumulé)		6	7	10	9
Agents temporaires – TOTAL					
Agents contractuels – nombre de référence					
Agents contractuels – Agents supplémentaires					2
Experts nationaux détachés					
TOTAL		**6**	**7**	**10**	**11**

Les ressources humaines nécessaires à la réalisation des objectifs du nouveau mandat ont été estimées en coopération avec l'eu-LISA. Ces estimations tiennent compte de l'augmentation attendue de la charge de travail à mesure que les parties intéressées auront de plus en plus recours aux services de l'eu-LISA au fil du temps, ainsi que du temps nécessaire à l'eu-LISA pour absorber les ressources afin d'éviter une situation dans laquelle l'Agence ne serait pas en mesure de mettre pleinement en œuvre la contribution de l'UE et d'engager les crédits en temps voulu.

Ces estimations sont fondées sur les niveaux d'effectifs suivants:

	Phase								
	Analyse et Conception			Construction et Développement			Fonctionnement		
Type de contrat	AT	AC	Total	AT	AC	Total	AT	AC	Total
Profil	Nbre	Nbre		Nbre	Nbre		Nbre	Nbre	
Architecte en informatique	1		1	1		1	1		1
Gestion des essais	1		1	1		1	0,5		0,5
Gestion des mises en production et des modifications			0	1		1	1		1
Administrateur de réseau	1		1	1		1	1		1
Gestion de la sécurité	2		2	2		2	2		2
Agent de soutien de 1er niveau (24/7)			0			0		1	1

Administrateur de soutien de 2e niveau (24/7)			0			0		1	1
Gestion de programme et de projet	1		1	1		1	0,5		0,5
Propriétaire de produit			0	1		1	1		1
Expert en biométrie	1		1	1		1	1		1
Administrateur de système/Infra	1		1	1		1	1		1
Total (AC + AT)	**8**		**8**	**10**		**10**	**9**	**2**	**11**

Profils	Année -1 (Préparation et Conception)	Année 1	Année 2	Année 3	Année 4	Année 5
Architecte en informatique (AT)	1	1	1	1	1	1
Gestion des essais (AT)		1	1	0,5	0,5	0,5
Gestion des mises en production et des			1	1	1	1

modifications (AT)						
Administrateur de réseau (AT)	1	1	1	1	1	1
Gestion de la sécurité (AT)	1	1	2	2	2	2
Agent de soutien de 1er niveau (24/7) – (AC)				1	1	1
Administrateur de soutien de 2e niveau (24/7) – (AC)				1	1	1
Gestion de programme et de projet (AT)	1	1	1	0,5	0,5	0,5
Propriétaire de produit (AT)			1	1	1	1
Expert en biométrie (AT)	1	1	1	1	1	1
Administrateur de système/ Infrastructure (AT)	1	1	1	1	1	1
TOTAL	**6**	**7**	**10**	**11**	**11**	**11**

3.2.5.2. Besoins estimés en ressources humaines pour la DG partenaire

☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

☒ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en valeur entière (ou au plus avec une décimale)

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**
• **Emplois du tableau des effectifs (fonctionnaires et agents temporaires)**						
XX 01 01 01 (au siège et dans les bureaux de représentation de la Commission)			5	5	4	4
XX 01 01 02 (en délégation)						
XX 01 05 01 (recherche indirecte)						
10 01 05 01 (recherche directe)						
• **Personnel externe (en équivalents temps plein: ETP)**[54]						
XX 01 02 01 (AC, END, INT de l'enveloppe globale)						
XX 01 02 02 (AC, AL, END, INT et JPD dans les délégations)						
XX 01 04 ***yy***[55]	- au siège[56]					
	- en délégation					
XX 01 05 02 (AC, END, INT sur recherche indirecte)						
10 01 05 02 (AC, END, INT sur recherche directe)						
Autres lignes budgétaires (à spécifier)						
TOTAL			**5**	**5**	**4**	**4**

XX est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts partiellement (3 ETP) par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle

[54] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

[55] Sous-plafond de personnel externe financé sur crédits opérationnels (anciennes lignes «BA»).

[56] Essentiellement pour les Fonds structurels, le Fonds européen agricole pour le développement rural (Feader) et le Fonds européen pour la pêche (FEP).

et compte tenu des contraintes budgétaires existantes. La DG aura également besoin de personnel supplémentaire (2 ETP).

Description des tâches à effectuer:

Cinq fonctionnaires pour le suivi. Le personnel assume les obligations de la Commission pour l'exécution du programme: vérifier le respect des instruments législatifs, résoudre les problèmes de conformité, élaborer des rapports pour le Parlement européen et le Conseil, évaluer les progrès réalisés par les États membres, tenir le droit dérivé à jour, y compris toute évolution concernant les normes. Étant donné que le programme est une activité venant s'ajouter aux charges de travail existantes, des effectifs supplémentaires sont nécessaires (2 ETP). L'une de ces augmentations de personnel est limitée en termes de durée et ne couvre que la période de développement, tandis que la seconde représente l'absorption des tâches du secrétariat du Conseil, étant donné que les décisions du Conseil sont transformées en un règlement, la Commission doit reprendre les tâches du secrétariat du Conseil dont la charge de travail correspond à 1 ETP.

3.2.6. Compatibilité avec le cadre financier pluriannuel actuel

☐ La proposition/l'initiative est compatible avec le cadre financier pluriannuel actuel.

☐ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel[57].

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants. […]

3.2.7. Participation de tiers au financement

La proposition/l'initiative ne prévoit pas de cofinancement par des tierces parties.

La proposition/l'initiative prévoit un cofinancement estimé ci-après:

En Mio EUR (à la 3e décimale)

	Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			Total
Préciser l'organisme de cofinancement								
TOTAL crédits cofinancés								

[57] Voir les articles 11 et 17 du règlement (UE, Euratom) nº 1311/2013 du Conseil fixant le cadre financier pluriannuel pour la période 2014-2020.

3.3. Incidence estimée sur les recettes

☒ La proposition/l'initiative est sans incidence financière sur les recettes.

☐ La proposition/l'initiative a une incidence financière décrite ci-après:

- ☐ sur les ressources propres
- ☐ sur les autres recettes
- ☐ veuillez indiquer si les recettes sont affectées à des lignes de dépenses

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[58]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)		
Article …….								

Pour les recettes diverses qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

[…]

Préciser la méthode de calcul de l'incidence sur les recettes.

[…]

[58] En ce qui concerne les ressources propres traditionnelles (droits de douane et cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.

ANNEXE 5

de la
DÉCISION DE LA COMMISSION

relative aux règles internes sur l'exécution du budget général de l'Union européenne (section Commission européenne) à l'attention des services de la Commission

ANNEXE
de la FICHE FINANCIÈRE LÉGISLATIVE

ANNEXE
de la FICHE FINANCIÈRE LÉGISLATIVE

Dénomination de la proposition:

Proposition de règlement relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les règlements (UE) 2018/1726, 2019/817 et 2019/818 et abrogeant les décisions 2008/615/JAI et 2008/616/JAI du Conseil

1. VOLUME ET COÛT DES RESSOURCES HUMAINES ESTIMÉES NÉCESSAIRES

2. COÛT DES AUTRES DÉPENSES DE NATURE ADMINISTRATIVE

3. TOTAL DES FRAIS ADMINISTRATIFS

4. MÉTHODES DE CALCUL UTILISÉES POUR L'ESTIMATION DES COÛTS

4.1. Ressources humaines

4.2. Autres dépenses administratives

La présente annexe accompagne la fiche financière législative lors du lancement de la consultation interservices.

Les tableaux de données servent à alimenter les tableaux contenus dans la fiche financière législative. Ils constituent un document strictement interne à la Commission.

(1) Coût des ressources humaines estimées nécessaires

☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

X☐ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

RUBRIQUE 7 du cadre financier pluriannuel		**2024**		**2025**		**2026**		**2027**								**TOTAL**	
		ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits
• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)																	
20 01 02 01 – Siège et bureaux de représentation	AD	5	0,608	5	0,684	4	0,608	4	0,608							4	2,508
	AST																
20 01 02 03 – Délégations de l'Union	AD																
	AST																
• Personnel externe[59]																	
20 02 01 et 20 02 02 – Personnel externe – Siège et bureaux de représentation	AC																
	END																
	INT																
20 02 03 – Personnel externe - Délégations de l'Union	AC																
	AL																
	END																

[59] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

	INT																
	JPD																
Autres lignes budgétaires liées aux RH (*à préciser*)																	
Sous-total RH – RUBRIQUE 7		5	0,608	5	0,684	4	0,608	4	0,608							4	2,508

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

(2) Coût des autres dépenses de nature administrative

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative
☑ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

RUBRIQUE 7 du cadre financier pluriannuel	**2024**	**2025**	**2026**	**2027**				**Total**
Au siège ou sur le territoire de l'UE:								
20 02 06 01 – Frais de mission et de représentation	0,035	0,035	0,035	0,035				**0,140**
20 02 06 02 – Frais de conférences et de réunions	0,125	0,125	0,125	0,125				**0,500**
20 02 06 03 – Comités (comité Prüm II)[60]	0,065	0,065	0,026	0,026				**0,182**
20 02 06 04 – Études et consultations								
20 04 – Dépenses informatiques (systèmes institutionnels)[61]								
Autres lignes budgétaires hors RH (*à préciser le cas échéant*)								
Dans les délégations de l'Union								
20 02 07 01 - Frais de mission, de conférence et de								

[60] Comité Prüm II, environ 10 réunions par an en 2024 et 2025, puis 4 réunions par an dont la moitié seulement est prise en compte dans les coûts (l'autre moitié prenant la forme de vidéoconférences).

[61] L'avis de l'équipe chargée des investissements informatiques de la DG DIGIT est requis [voir les lignes directrices sur le financement de la technologie de l'information, C(2020) 6126 final du 10.9.2020, page 7].

représentation								
20 02 07 02 – Perfectionnement professionnel								
20 03 05 – Infrastructure et logistique								
Autres lignes budgétaires hors RH (*à préciser le cas échéant*)								
Sous-total Autres – RUBRIQUE 7 du cadre financier pluriannuel	0,225	0,225	0,186	0,186				**0,822**

En Mio EUR (à la 3e décimale)

Hors RUBRIQUE 7 du cadre financier pluriannuel	**2024**	**2025**	**2026**	**2027**				**Total**
Dépenses d'assistance technique et administrative (hors personnel externe), sur crédits opérationnels (anciennes lignes «BA»):								
- au siège								
- dans les délégations de l'Union								
Autres dépenses de gestion pour la recherche								

Dépenses pour les systèmes informatiques soutenant une politique consacrées aux programmes opérationnels[62]								
Dépenses pour les systèmes informatiques institutionnels consacrées aux programmes opérationnels[63]								
Autres lignes budgétaires hors RH (*à préciser le cas échéant*)								
Sous-total Autres – Hors RUBRIQUE 7 du cadre financier pluriannuel								
Total des autres dépenses administratives (toutes les rubriques du CFP)	0,225	0,225	0,186	0,186				**0,822**

[62] L'avis de l'équipe chargée des investissements informatiques de la DG DIGIT est requis [voir les lignes directrices sur le financement de la technologie de l'information, C(2020) 6126 final du 10.9.2020, page 7].

[63] Ce poste comprend les systèmes administratifs locaux et les contributions au cofinancement des systèmes informatiques institutionnels [voir les lignes directrices sur le financement de la technologie de l'information, C(2020) 6126 final du 10.9.2020].

(3) Total des coûts administratifs (toutes les rubriques du CFP)

En Mio EUR (à la 3e décimale)

Synthèse	2024	2025	2026	2027				Total
Rubrique 7 – Ressources humaines	0,608	0,684	0,608	0,608				**2,508**
Rubrique 7 – Autres dépenses administratives	0,225	0,225	0,186	0,186				**0,822**
Sous-total rubrique 7								
Hors Rubrique 7 – Ressources humaines								
Hors Rubrique 7 – Autres dépenses administratives								
Sous-total Autres rubriques								
TOTAL RUBRIQUE 7 et Hors RUBRIQUE 7	0,833	0,833	0,794	0,794				**3,330**

Les besoins en crédits de nature administrative seront couverts par les crédits déjà affectés à la gestion de l'action et/ou réaffectés, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

4. METHODES DE CALCUL UTILISEES POUR L'ESTIMATION DES COUTS

4.1. Ressources humaines

Cette partie explicite la méthode de calcul retenue pour l'estimation des ressources humaines jugées nécessaires [hypothèses concernant la charge de travail, y inclus les métiers spécifiques (profils de postes Sysper 2), les catégories de personnel et les coûts moyens correspondants].

RUBRIQUE 7 du cadre financier pluriannuel

NB: les coûts moyens par catégorie de personnel au siège sont disponibles sur BudgWeb, à l'adresse suivante: https://myintracomm.ec.europa.eu/budgweb/FR/pre/legalbasis/Pages/pre-040-020_preparation.aspx

Fonctionnaires et agents temporaires:

Conformément à la circulaire de la DG BUDGET aux membres du réseau des unités financières – RUF/2020/23 du 30.11.2020 [voir annexe 1, Ares(2020)7207955 du 30.11.2020], 1AD représente un coût de 152 000 EUR par an. La moitié des crédits annuels correspondants sont calculés pour l'année au cours de laquelle le personnel est recruté et retiré progressivement.

Les besoins en ressources humaines seront couverts partiellement (3 ETP) par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes. La DG aura également besoin de personnel supplémentaire (2 ETP).

Description des tâches à effectuer:

Cinq fonctionnaires pour le suivi. Le personnel assume les obligations de la Commission pour l'exécution du programme: vérifier le respect des instruments législatifs, résoudre les problèmes de conformité, élaborer des rapports pour le Parlement européen et le Conseil, évaluer les progrès réalisés par les États membres, tenir le droit dérivé à jour, y compris toute évolution concernant les normes. Étant donné que le programme est une activité venant s'ajouter aux charges de travail existantes, des effectifs supplémentaires sont nécessaires (2 ETP). L'une de ces augmentations de personnel est limitée en termes de durée et ne couvre que la période de développement, tandis que la seconde représente l'absorption des tâches du secrétariat du Conseil, étant donné que les décisions du Conseil sont transformées en un règlement, la Commission doit reprendre les tâches du secrétariat du Conseil dont la charge de travail correspond à 1 ETP.

- Personnel externe

Hors RUBRIQUE 7 du cadre financier pluriannuel

- Seulement postes financés à charge du budget de la recherche

- Personnel externe

4.2. Autres dépenses administratives

Détailler par ligne budgétaire la méthode de calcul utilisée,

en particulier les hypothèses sous-jacentes (par exemple nombre de réunions par an, coûts moyens, etc.)

RUBRIQUE 7 du cadre financier pluriannuel

On estime qu'en moyenne 35 missions auront lieu chaque année, y compris des missions pour les réunions statutaires (groupe consultatif, groupes de travail de l'eu-LISA et d'Europol et réunions liées à l'EPRIS et l'Eucaris), pour participer aux réunions et conférences liées à Prüm. Le coût unitaire par mission est calculé sur la base du déplacement d'1 fonctionnaire pour une durée moyenne de 2 jours par mission et est fixé à 500 EUR par mission et par jour.

Le coût unitaire par réunion/conférence d'experts est fixé à 25 000 EUR pour 50 participants. On estime que 5 réunions seront organisées chaque année.

Le coût unitaire par réunion du comité est fixé à 13 000 EUR pour 26 participants, en supposant un remboursement pour 1 participant par ÉM pour une mission d'une journée afin de participer à une réunion du comité. On estime que 10 réunions seront organisées par an en 2024 et 2025 (5 en présentiel et 5 en vidéoconférence), puis 4 réunions par an à partir de 2026 (2 en présentiel et 2 en vidéoconférence).

Hors RUBRIQUE 7 du cadre financier pluriannuel