



UNION EUROPÉENNE

LE PARLEMENT EUROPÉEN

LE CONSEIL

**Strasbourg, le 13 mars 2024
(OR. en)**

**2021/0410 (COD)
LEX 2301**

**PE-CONS 75/1/23
REV 1**

**IXIM 237
ENFOPOL 525
JAI 1599
CODEC 2358**

**RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL
RELATIF À LA CONSULTATION ET L'ÉCHANGE AUTOMATISÉS DE DONNÉES
DANS LE CADRE DE LA COOPÉRATION POLICIÈRE,
ET MODIFIANT LES DÉCISIONS 2008/615/JAI ET 2008/616/JAI DU CONSEIL
ET LES RÈGLEMENTS (UE) 2018/1726, (UE) 2019/817
ET (UE) 2019/818 DU PARLEMENT EUROPÉEN ET DU CONSEIL
(RÈGLEMENT PRÛM II)**

RÈGLEMENT (UE) 2024/...
DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 mars 2024

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

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 européen¹,

statuant conformément à la procédure législative ordinaire²,

¹ JO C 323 du 26.8.2022, p. 69.

² Position du Parlement européen du 8 février 2024 (non encore parue au Journal officiel) et décision du Conseil du 26 février 2024.

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 doit être réalisé au moyen, entre autres, de mesures appropriées visant à prévenir et à lutter contre la criminalité et les autres menaces pour la sécurité publique, y compris la criminalité organisée et le terrorisme, conformément à la communication de la Commission du 24 juillet 2020 intitulée "La stratégie de l'UE pour l'union de la sécurité". Cet objectif exige que les services répressifs échangent des données, de manière efficiente et en temps utile, afin de prévenir et de détecter efficacement les infractions pénales et d'enquêter en la matière.
- (2) L'objectif du présent règlement est d'améliorer, de rationaliser et de faciliter l'échange d'informations en matière pénale et de données relatives à l'immatriculation des véhicules, aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière, entre les autorités compétentes des États membres et entre les États membres et 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 Conseil³, dans le plein respect des droits fondamentaux et des règles en matière de protection des données.

³ 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).

- (3) 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/JAI⁴ et 2008/616/JAI⁵ du Conseil, qui établissent les 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 transfrontière et, partant, pour protéger la sécurité interne de l'Union et de ses citoyens.

⁴ 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).

⁵ 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).

- (4) En s'appuyant sur les procédures existantes pour la consultation automatisée de données, le présent règlement fixe les conditions et les procédures de consultation et d'échange automatisés des profils ADN, des données dactyloscopiques, de certaines données relatives à l'immatriculation des véhicules, des images faciales et des fichiers de police. Cela devrait être sans préjudice du traitement de ces données dans le système d'information Schengen (SIS), de l'échange d'informations supplémentaires liées à ces données par l'intermédiaire des bureaux SIRENE en vertu du règlement (UE) 2018/1862 du Parlement européen et du Conseil⁶ ou des droits des personnes dont les données sont traitées dans ce système.

⁶ 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) n° 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).

- (5) Le présent règlement établit un cadre pour l'échange d'informations entre les services chargés de la prévention et de la détection des infractions pénales et des enquêtes en la matière (ci-après dénommé "cadre Prüm II"). Conformément à l'article 87, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, le présent règlement couvre toutes les autorités compétentes des États membres, y compris, sans s'y limiter, les services de police, les services des douanes et autres services répressifs spécialisés dans les domaines de la prévention ou de la détection des infractions pénales et des enquêtes en la matière. Par conséquent, dans le contexte du présent règlement, toute autorité qui est responsable de la gestion d'une base de données nationale couverte par le présent règlement ou qui accorde une autorisation judiciaire pour communiquer des données devrait être considérée comme relevant du champ d'application du présent règlement tant que les informations sont échangées aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière.
- (6) Tout traitement ou échange de données à caractère personnel aux fins du présent règlement ne devrait donner lieu à aucune discrimination à l'encontre des personnes, quel qu'en soit le motif. Il devrait respecter pleinement la dignité humaine, l'intégrité des personnes et d'autres droits fondamentaux, y compris 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) Il convient que tout traitement ou échange de données à caractère personnel soit soumis aux dispositions relatives à la protection des données du chapitre 6 du présent règlement et, le cas échéant, à celles de la directive (UE) 2016/680 du Parlement européen et du Conseil⁷ ou du règlement (UE) 2018/1725⁸, (UE) 2016/794 ou (UE) 2016/679⁹ du Parlement européen et du Conseil. La directive (UE) 2016/680 s'applique à l'utilisation du cadre Prüm II en ce qui concerne les recherches de personnes disparues et l'identification de restes humains non identifiés aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière. Le règlement (UE) 2016/679 s'applique à l'utilisation du cadre Prüm II en ce qui concerne les recherches de personnes disparues et l'identification de restes humains non identifiés à d'autres fins.

⁷ 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).

⁸ 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) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

⁹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

- (8) En prévoyant la consultation automatisée de profils ADN, de données dactyloscopiques, de certaines données relatives à l'immatriculation des véhicules, d'images faciales et de fichiers de police, le présent règlement a également pour objectif de permettre la recherche de personnes disparues et l'identification de restes humains non identifiés. Ces consultations automatisées devraient suivre les règles et les procédures établies dans le présent règlement. Ces consultations automatisées sont sans préjudice de l'introduction dans le SIS de signalements concernant des personnes disparues et de l'échange d'informations supplémentaires concernant ces signalements au titre du règlement (UE) 2018/1862.
- (9) Lorsque les États membres souhaitent recourir au cadre Prüm II pour rechercher des personnes disparues et identifier des restes humains, ils devraient adopter des mesures législatives nationales pour désigner les autorités nationales compétentes à cet effet et pour fixer les procédures, conditions et critères spécifiques à cet effet. En ce qui concerne les recherches de personnes disparues en dehors du domaine des enquêtes pénales, les mesures législatives nationales devraient clairement indiquer les motifs humanitaires pour lesquels une recherche de personnes disparues peut être effectuée. Ces recherches devraient respecter le principe de proportionnalité. Les motifs humanitaires devraient inclure les catastrophes naturelles ou d'origine humaine ainsi que d'autres motifs tout aussi justifiés, tels que les soupçons de suicide.

- (10) Le présent règlement fixe les conditions et les procédures de consultation automatisée de profils ADN, de données dactyloscopiques, de certaines données relatives à l'immatriculation des véhicules, d'images faciales et de fichiers de police ainsi que les règles relatives à l'échange de données de base à la suite d'une concordance confirmée sur des données biométriques. Il ne s'applique pas à l'échange d'informations supplémentaires allant au-delà de ce qui est prévu par le présent règlement, qui est réglementé par la directive (UE) 2023/977 du Parlement européen et du Conseil¹⁰.
- (11) La directive 2023/977 fournit un cadre juridique cohérent au niveau de l'Union afin de garantir que les autorités compétentes d'un État membre disposent d'un accès équivalent aux informations détenues par d'autres États membres lorsqu'elles ont besoin de ces informations pour lutter contre la criminalité et le terrorisme. Afin de renforcer l'échange d'informations, cette directive formalise et clarifie les règles et les procédures de partage d'informations entre les autorités compétentes des États membres, notamment à des fins d'enquêtes, y compris le rôle du point de contact unique de chaque État membre dans ces échanges.
- (12) Les objectifs des échanges de profils ADN au titre du présent règlement sont sans préjudice de la compétence exclusive des États membres pour décider de la finalité de leurs bases de données ADN nationales, y compris la prévention ou la détection d'infractions pénales.

¹⁰ Directive (UE) 2023/977 du Parlement européen et du Conseil du 10 mai 2023 relative à l'échange d'informations entre les services répressifs des États membres et abrogeant la décision-cadre 2006/960/JAI du Conseil (JO L 134 du 22.5.2023, p. 1).

- (13) Les États membres devraient, lors de la première connexion au routeur établi par le présent règlement, effectuer des consultations automatisées de profils ADN en comparant tous les profils ADN stockés dans leurs bases de données avec tous les profils ADN stockés dans les bases de données de tous les autres États membres et les données d'Europol. L'objectif de cette première consultation automatisée est d'éviter toute lacune dans l'identification des concordances entre les profils ADN stockés dans la base de données d'un État membre et les profils ADN stockés dans les bases de données de tous les autres États membres et les données d'Europol. La première consultation automatisée devrait être effectuée de manière bilatérale, mais ne devrait pas nécessairement être effectuée dans les bases de données de tous les autres États membres et les données d'Europol en même temps. Les modalités pour effectuer ces consultations, y compris le calendrier et la quantité par lot, devraient être convenues de manière bilatérale et conformément aux règles et procédures fixées dans le présent règlement.
- (14) À la suite de la première consultation automatisée de profils ADN, les États membres devraient effectuer des consultations automatisées en comparant tous les nouveaux profils ADN ajoutés à leurs bases de données avec tous les profils ADN stockés dans les bases de données d'autres États membres et avec les données d'Europol. Ces consultations automatisées des nouveaux profils ADN devrait avoir lieu régulièrement. Lorsque de telles consultations n'ont pas pu avoir lieu, l'État membre concerné devrait pouvoir les effectuer à un stade ultérieur afin de s'assurer que des concordances n'ont pas été manquées. Les modalités pour effectuer ces consultations ultérieures, y compris le calendrier et la quantité par lot, devraient être convenues de manière bilatérale conformément aux règles et procédures fixées dans le présent règlement.

- (15) En ce qui concerne la consultation automatisée de données relatives à l'immatriculation des véhicules, les États membres et Europol 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, qui connecte tous les États membres participants dans un réseau. Aucun élément central n'est nécessaire pour établir la communication, chaque État membre communiquant directement avec les autres États membres connectés, tandis qu'Europol communique directement avec les bases de données connectées.
- (16) 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 personnes condamnées pour avoir commis une infraction pénale ou soupçonnées d'avoir commis une infraction pénale ou, lorsque le droit national de l'État membre requis l'autorise, de victimes, recueillies conformément au droit national, pourrait fournir des informations supplémentaires permettant d'identifier les criminels avec succès et de lutter contre la criminalité. Compte tenu du caractère sensible des données concernées, il ne devrait être possible d'effectuer des consultations automatisées qu'aux fins de la prévention ou de la détection d'une infraction pénale, passible d'une peine maximale d'emprisonnement d'au moins un an au titre du droit de l'État membre requérant, ou des enquêtes en la matière.
- (17) La consultation automatisée de données biométriques par les autorités compétentes des États membres chargées de la prévention et de la détection des infractions pénales et des enquêtes en la matière au titre 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 et des enquêtes en la matière.

- (18) La participation à la consultation et à l'échange automatisés de fichiers de police devrait rester volontaire. Lorsque les États membres décident de participer, il ne devrait leur être possible, dans un esprit de réciprocité, d'interroger les bases de données des autres États membres que s'ils mettent leurs propres bases de données à la disposition de ceux-ci pour qu'ils puissent les interroger. Les États membres participants devraient établir des index nationaux des fichiers de police. Il devrait revenir aux États membres de décider des bases de données nationales établies aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière, à utiliser pour créer leurs index nationaux des fichiers de police. Ces index comprennent des données provenant de bases de données nationales que la police vérifie habituellement lorsqu'elle reçoit des demandes d'informations d'autres services répressifs. Le présent règlement établit le système d'index européen des fichiers de police (EPRIS) conformément au principe du respect de la vie privée dès la conception. Les garanties en matière de protection des données comprennent la pseudonymisation, car les index et les interrogations ne contiennent pas des données à caractère personnel claires, mais des chaînes alphanumériques. Il est important que l'EPRIS empêche les États membres ou Europol de renverser la pseudonymisation et de révéler les données d'identification qui ont donné lieu à la concordance. Compte tenu du caractère sensible des données concernées, les échanges d'index nationaux des fichiers de police au titre du présent règlement ne devraient concerner que les données des personnes condamnées pour avoir commis une infraction pénale ou soupçonnées d'avoir commis une infraction pénale. En outre, il ne devrait être possible d'effectuer des consultations automatisées des index nationaux des fichiers de police qu'aux fins de la prévention et de la détection d'une infraction pénale passible d'une peine maximale d'emprisonnement d'au moins un an au titre du droit de l'État membre requérant, et des enquêtes en la matière.

- (19) L'échange de fichiers de police au titre du présent règlement est sans préjudice de l'échange de casiers judiciaires au moyen du système européen d'information sur les casiers judiciaires (ECRIS) existant, établi par la décision-cadre 2009/315/JAI du Conseil¹¹.
- (20) Ces dernières années, Europol a, conformément au règlement (UE) 2016/794, reçu d'autorités de pays tiers un grand nombre de données biométriques de suspects et de personnes condamnées pour terrorisme et pour des infractions pénales, y compris, des informations du champ de bataille provenant de zones de guerre. Dans de nombreux cas, ces données n'ont pas pu être exploitées pleinement parce qu'elles ne sont pas toujours à la disposition des autorités compétentes des États membres. L'intégration dans le cadre Prüm II des données fournies par des pays tiers et stockées par Europol et, partant, la mise à la disposition des autorités compétentes des États membres de ces données conformément au rôle d'Europol en tant que centre d'information criminelle de l'Union est nécessaire pour améliorer la prévention et la détection des infractions pénales graves et les enquêtes en la matière. Cela contribue également à créer des synergies entre les différents outils de répression et garantit que les données sont utilisées de la manière la plus efficace possible.

¹¹ Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres (JO L 93 du 7.4.2009, p. 23).

- (21) Europol devrait pouvoir consulter les bases de données des États membres au titre du cadre Prüm II à partir des données reçues d'autorités de pays tiers, dans le plein respect des règles et conditions prévues par le règlement (UE) 2016/794, afin d'établir des liens transfrontières entre les affaires pénales pour lesquelles Europol est compétent. La possibilité d'utiliser les données de Prüm, en plus d'autres bases de données dont dispose Europol, permettrait de procéder à une analyse plus complète et plus éclairée, ce qui permettra à Europol d'apporter un meilleur soutien aux autorités compétentes des États membres aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière.
- (22) Europol devrait veiller à ce que ses demandes de consultation n'excèdent pas les capacités de consultation établies par les États membres en ce qui concerne les données dactyloscopiques et les images faciales. En cas de concordance entre les données utilisées pour la consultation et les données stockées dans les bases de données des États membres, il devrait revenir aux États membres de décider s'ils transmettent ou non à Europol les informations nécessaires à l'accomplissement de ses missions.
- (23) Le règlement (UE) 2016/794 s'applique dans son intégralité à la participation d'Europol au cadre Prüm II. Toute utilisation par Europol de données reçues de pays tiers est régie par l'article 19 du règlement (UE) 2016/794. Toute utilisation par Europol de données obtenues lors de consultations automatisées au titre du cadre Prüm II devrait être soumise au consentement de l'État membre qui a fourni les données et est régie par l'article 25 du règlement (UE) 2016/794 si les données sont transférées à des pays tiers.

- (24) 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 a dû établir une connexion avec chaque État membre participant aux échanges, ce qui signifiait au moins 26 connexions par État membre, par catégorie de données. Le routeur et l'EPRIS simplifieront l'architecture technique du cadre Prüm et serviront 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. L'EPRIS devrait exiger une connexion unique par État membre participant en ce qui concerne les fichiers de police.

- (25) Le routeur devrait être connecté au portail de recherche européen créé par les règlements (UE) 2019/817¹² et (UE) 2019/818¹³ du Parlement européen et du Conseil afin de permettre aux autorités compétentes des États membres et à Europol d'interroger en même temps les bases de données nationales au titre du présent règlement et le répertoire commun de données d'identité établi par lesdits règlements, à des fins répressives, conformément auxdits règlements. Il convient donc de modifier ces règlements en conséquence. En outre, il y a lieu de modifier le règlement (UE) 2019/818 afin de permettre le stockage des rapports et des statistiques du routeur dans le répertoire central des rapports et statistiques.

¹² 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) n° 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).

¹³ 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).

- (26) Une référence de données biométriques devrait pouvoir être une référence provisoire ou un numéro de contrôle de l'opération.
- (27) Les systèmes automatisés d'identification par empreintes digitales et les systèmes de reconnaissance d'image faciale utilisent des modèles biométriques composés de données provenant d'une extraction de caractéristiques à partir d'échantillons biométriques réels. Les modèles biométriques devraient être obtenus à partir des données biométriques, mais il ne devrait pas être possible d'obtenir les mêmes données biométriques à partir des modèles biométriques.
- (28) Le routeur devrait classer, lorsque l'État membre requérant le décide et s'il y a lieu en fonction du type de données biométriques, les réponses de l'État membre ou des États membres requis ou d'Europol en comparant les données biométriques utilisées pour les interrogations et les données biométriques transmises dans les réponses de l'État membre ou des États membres requis ou d'Europol.

- (29) En cas de concordance entre les données utilisées pour la consultation et les données détenues dans la base de données nationale de l'État membre ou des États membres requis, après la confirmation manuelle de cette concordance par un membre qualifié du personnel de l'État membre requérant et après la transmission d'une description des faits et l'indication de l'infraction sous-jacente au moyen du tableau commun des catégories d'infractions figurant dans un acte d'exécution devant être adopté en vertu de la décision-cadre 2009/315/JAI, l'État membre requis devrait renvoyer un ensemble limité de données de base, dans la mesure où de telles données de base sont disponibles. L'ensemble limité de données de base devrait être renvoyé par l'intermédiaire du routeur et, sauf lorsqu'une autorisation judiciaire est requise au titre du droit national, dans les 48 heures à compter du moment où les conditions pertinentes sont remplies. Ce délai garantira un échange rapide de communications entre les autorités compétentes des États membres. Les États membres devraient conserver le contrôle de la communication de l'ensemble limité de données de base. L'intervention humaine devrait être maintenue aux points clés du processus, y compris pour la décision de lancer une interrogation, pour la décision de confirmer une concordance, pour la décision de solliciter la réception de l'ensemble de données de base à la suite d'une concordance confirmée, et pour la décision de communiquer des données à caractère personnel à l'État membre requérant, afin de garantir qu'aucune donnée de base ne sera échangée de manière automatisée.

- (30) Dans le cas particulier de l'ADN, l'État membre requis devrait également pouvoir confirmer une concordance entre deux profils ADN, lorsque cela est pertinent à des fins d'enquête en matière d'infractions pénales. Après la confirmation de cette concordance par l'État membre requis et après la transmission d'une description des faits et l'indication de l'infraction sous-jacente au moyen du tableau commun des catégories d'infractions figurant dans un acte d'exécution devant être adopté en vertu de la décision-cadre 2009/315/JAI, l'État membre requérant devrait renvoyer un ensemble limité de données de base par l'intermédiaire du routeur dans les 48 heures à compter du moment où les conditions pertinentes sont remplies, sauf lorsqu'une autorisation judiciaire est requise au titre du droit national.
- (31) Les données légalement transmises et reçues au titre du présent règlement sont soumises aux délais de conservation et d'examen établis en vertu de la directive (UE) 2016/680.
- (32) La norme de format universel pour les messages (UMF) devrait être utilisée pour le développement du routeur et de l'EPRIS autant que possible. Tout échange automatisé de données au titre du présent règlement devrait utiliser la norme UMF autant que possible. Les autorités compétentes des États membres et Europol sont aussi encouragés à utiliser la norme UMF pour tout autre échange de données entre eux dans le contexte du cadre Prüm II. La norme UMF devrait servir de 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.

- (33) Seules les informations non classifiées devraient être échangées par l'intermédiaire du cadre Prüm II.
- (34) Chaque État membre devrait notifier aux autres États membres, à la Commission, 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), créée par le règlement (UE) 2018/1726 du Parlement européen et du Conseil¹⁴, et à Europol le contenu de ses bases de données nationales mises à disposition par l'intermédiaire du cadre Prüm II et les conditions régissant les consultations automatisées.

¹⁴ 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) n° 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) n° 1077/2011 (JO L 295 du 21.11.2018, p. 99).

- (35) Certains aspects du cadre 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 modalités et spécifications techniques pour les procédures de consultation automatisée, les normes d'échange de données, y compris les normes de qualité minimales, et les éléments de données à échanger. Afin d'assurer des conditions uniformes d'exécution du présent règlement en ce qui concerne ces aspects, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil¹⁵.
- (36) La qualité des données revêt la plus grande importance en tant que garde-fou et condition préalable essentielle pour garantir l'efficacité du présent règlement. Dans le cadre de la consultation automatisée de données biométriques, et afin de garantir que les données transmises sont de qualité suffisante et de réduire le risque de fausses concordances, une norme de qualité minimale devrait être mise en place et régulièrement révisée.

¹⁵ Règlement (UE) n° 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).

- (37) Compte tenu de l'ampleur et du caractère sensible des données à caractère personnel échangées aux fins du présent règlement, et de l'existence de règles nationales différentes pour le stockage d'informations sur les personnes dans les bases de données nationales, il importe de veiller à ce que les bases de données utilisées pour la consultation automatisée au titre du présent règlement soient créées conformément au droit national et à la directive (UE) 2016/680. Par conséquent, avant de connecter leurs bases de données nationales au routeur ou à l'EPRIS, les États membres devraient effectuer une analyse d'impact relative à la protection des données conformément à la directive (UE) 2016/680 et, le cas échéant, consulter l'autorité de contrôle comme le prévoit ladite directive.
- (38) Les États membres et Europol devraient s'assurer de l'exactitude et de la pertinence des données à caractère personnel traitées en vertu du présent règlement. Lorsqu'un État membre ou Europol se rend compte que des données qui ont été transmises sont inexactes ou ne sont plus d'actualité ou n'auraient pas dû être transmises, il devrait adresser une notification à l'État membre qui a reçu les données ou Europol, selon le cas, sans retard injustifié. Tous les États membres concernés ou Europol, selon le cas, devraient rectifier ou supprimer les données en conséquence sans retard injustifié. Lorsque l'État membre qui a reçu les données ou Europol a des raisons de penser que les données transmises sont inexactes ou devraient être supprimées, il devrait informer l'État membre qui a fourni les données sans retard injustifié.

- (39) Un suivi rigoureux de la mise en œuvre du présent règlement est de la plus haute importance. Il convient notamment de prévoir des mesures pour garantir efficacement le respect des règles relatives au traitement des données à caractère personnel, et les responsables de ce traitement, ainsi que les autorités de contrôle et le Contrôleur européen de la protection des données, le cas échéant, devraient assurer un suivi et des audits réguliers. Des dispositions permettant de vérifier régulièrement l'admissibilité des interrogations et la licéité du traitement des données devraient également être mises en place.
- (40) Les autorités de contrôle et le Contrôleur européen de la protection des données devraient assurer un contrôle coordonné de l'application du présent règlement dans le cadre de leurs responsabilités, en particulier lorsqu'ils constatent des divergences majeures entre les pratiques des États membres ou des transferts potentiellement illicites
- (41) Lors de la mise en œuvre du présent règlement, il est essentiel que les États membres et Europol prennent note de la jurisprudence de la Cour de justice de l'Union européenne en ce qui concerne l'échange de données biométriques.
- (42) Trois ans après la mise en service du routeur et de l'EPRIS, et tous les quatre ans par la suite, la Commission devrait élaborer un rapport d'évaluation comprenant une évaluation de l'application du présent règlement par les États membres et Europol, et notamment du respect par les États membres des garanties applicables en matière de protection des données. Les rapports d'évaluation devraient également comporter un examen des résultats obtenus au regard des objectifs du présent règlement et de son incidence sur les droits fondamentaux. Les rapports d'évaluation devraient aussi évaluer l'incidence, les performances, l'efficacité, l'efficience, la sécurité et les méthodes de travail du cadre Prüm II.

- (43) Étant donné que le présent règlement prévoit l'établissement d'un nouveau cadre Prüm, il convient de supprimer les dispositions des décisions 2008/615/JAI et 2008/616/JAI qui ne sont plus pertinentes. Il convient de modifier lesdites décisions en conséquence.
- (44) Étant donné que le routeur doit être développé et géré par l'eu-LISA, le règlement (UE) 2018/1726 devrait être modifié en ajoutant celui-ci aux tâches de l'eu-LISA.
- (45) Étant donné que les objectifs du présent règlement, à savoir renforcer la coopération policière transfrontière et permettre aux autorités compétentes des États membres de rechercher des personnes disparues et d'identifier des restes humains non identifiés, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent, en raison des dimensions et des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.
- (46) Conformément aux articles 1^{er} et 2 du protocole n° 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 celui-ci ni soumis à son application.

- (47) Conformément à l'article 3 du protocole n° 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.
- (48) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu un avis le 2 mars 2022¹⁶,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

¹⁶ JO C 225 du 9.6.2022, p. 6.

Chapitre 1

Dispositions générales

Article premier

Objet

Le présent règlement établit un cadre pour la consultation et l'échange d'informations entre les autorités compétentes des États membres (ci-après dénommé "cadre Prüm II") en fixant:

- a) les conditions et les procédures de consultation automatisée de profils ADN, de données dactyloscopiques, de certaines données relatives à l'immatriculation des véhicules, d'images faciales et d'archives de police, et
- b) les règles relatives à l'échange de données de base à la suite d'une concordance confirmée sur des données biométriques.

Article 2

Objectif

Le cadre Prüm II a pour objectif d'approfondir la coopération transfrontière dans les matières relevant de la partie III, titre V, chapitres 4 et 5, du traité sur le fonctionnement de l'Union européenne, notamment en facilitant l'échange d'informations entre les autorités compétentes des États membres, dans le plein respect des droits fondamentaux des personnes physiques, dont 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.

Le cadre Prüm II a également pour objectif de permettre aux autorités compétentes des États membres de rechercher des personnes disparues dans le contexte d'enquêtes pénales ou pour des motifs humanitaires, ainsi que d'identifier des restes humains, conformément à l'article 29, pour autant que ces autorités soient habilitées à effectuer de telles recherches et à procéder à de telles identifications au titre du droit national.

Article 3

Champ d'application

Le présent règlement s'applique aux bases de données, créées conformément au droit national et utilisées pour le transfert automatisé de profils ADN, de données dactyloscopiques, de certaines données relatives à l'immatriculation des véhicules, d'images faciales et d'archives de police, dans le respect, selon le cas, de la directive (UE) 2016/680 ou du règlement (UE) 2018/1725, (UE) 2016/794 ou (UE) 2016/679.

Article 4

Définitions

Aux fins du présent règlement, on entend par:

- 1) "loci" (au singulier: "locus"): segments d'ADN contenant les caractéristiques d'identification d'un échantillon d'ADN humain analysé;
- 2) "profil ADN": un code alphanumérique qui représente un ensemble de loci ou la structure moléculaire particulière issue de divers loci;

- 3) "données indexées ADN": un profil ADN et la référence visée à l'article 7;
- 4) "profil ADN identifié": le profil ADN d'une personne identifiée;
- 5) "profil ADN non identifié": le profil ADN recueilli lors d'une enquête pénale et appartenant à une personne non encore identifiée, y compris un profil ADN obtenu à partir de traces;
- 6) "données dactyloscopiques": les images d'empreintes digitales, les images d'empreintes digitales latentes, les images d'empreintes de paumes de mains, les images d'empreintes de paumes de mains latentes et des modèles de telles images (points caractéristiques codés) qui sont stockés et traités dans une base de données automatisée;
- 7) "données indexées dactyloscopiques": des données dactyloscopiques et la référence visée à l'article 12;
- 8) "données dactyloscopiques non identifiées": les données dactyloscopiques recueillies lors d'une enquête sur une infraction pénale et appartenant à une personne non encore identifiée, y compris des données dactyloscopiques obtenues à partir de traces;
- 9) "données dactyloscopiques identifiées": les données dactyloscopiques d'une personne identifiée;
- 10) "affaire individuelle": un dossier unique lié à la prévention ou à la détection d'une infraction pénale ou à une enquête en la matière, à la recherche d'une personne disparue ou à l'identification de restes humains non identifiés;

- 11) "image faciale": une image numérique du visage;
- 12) "données indexées d'image faciale": une image faciale et la référence visée à l'article 21;
- 13) "image faciale non identifiée": une image faciale recueillie lors d'une enquête sur une infraction pénale et appartenant à une personne non encore identifiée, y compris une image faciale obtenue à partir de traces;
- 14) "image faciale identifiée": l'image faciale d'une personne identifiée;
- 15) "données biométriques": les profils ADN, les données dactyloscopiques ou les images faciales;
- 16) "données alphanumériques": les données représentées par des lettres, des chiffres, des caractères spéciaux, des espaces et des signes de ponctuation;
- 17) "concordance": l'existence d'une correspondance résultant d'une comparaison automatisée entre des données à caractère personnel détenues dans une base de données;
- 18) "candidat": les données avec lesquelles une concordance a été établie;
- 19) "État membre requérant": un État membre effectuant une consultation par l'intermédiaire du cadre Prüm II;
- 20) "État membre requis": un État membre dont les bases de données sont consultées par un État membre requérant par l'intermédiaire du cadre Prüm II;

- 21) "fichiers de police": les données biographiques de suspects ou de personnes condamnées disponibles dans les bases de données nationales créées à des fins de prévention et de détection des infractions pénales et des enquêtes en la matière;
- 22) "pseudonymisation": la pseudonymisation telle qu'elle est définie à l'article 3, point 5, de la directive (UE) 2016/680;
- 23) "suspect": une personne telle qu'elle est visée à l'article 6, point a), de la directive (UE) 2016/680;
- 24) "données à caractère personnel": les données à caractère personnel telles qu'elles sont définies à l'article 3, point 1, de la directive (UE) 2016/680.
- 25) "données d'Europol": toutes les données opérationnelles à caractère personnel traitées par Europol conformément au règlement (UE) 2016/794;
- 26) "autorités compétentes": toute autorité publique compétente pour la prévention ou la détection d'infractions pénales ou les enquêtes en la matière ou tout autre organisme ou entité à qui sont confiés, par le droit de l'État membre, l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la prévention ou de la détection d'infractions pénales ou des enquêtes en la matière.
- 27) "autorité de contrôle": une autorité publique indépendante instituée par un État membre en vertu de l'article 41 de la directive (UE) 2016/680;

- 28) "SIENA": l'application de réseau d'échange sécurisé d'informations, gérée et développée par Europol conformément au règlement (UE) 2016/794;
- 29) "incident": un incident tel qu'il est défini à l'article 6, point 6), de la directive (UE) 2022/2555 du Parlement européen et du Conseil¹⁷.
- 30) "incident important": un incident, sauf si cet incident 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;
- 31) "cybermenace importante": une cybermenace ayant la possibilité et la capacité de provoquer un incident important, et dont le but est de provoquer un incident important;
- 32) "vulnérabilité importante": une vulnérabilité qui entraînera probablement un incident important si elle est exploitée.

¹⁷ Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

Chapitre 2

Échange de données

SECTION 1

PROFILS ADN

Article 5

Données indexées ADN

1. Les États membres s'assurent de la disponibilité des données indexées ADN provenant de leurs bases de données ADN nationales aux fins des consultations automatisées effectuées par d'autres États membres et par Europol en vertu du présent règlement.

Les données indexées ADN ne contiennent aucune donnée supplémentaire permettant l'identification directe d'une personne.

Les profils ADN non identifiés sont reconnaissables en tant que tels.

2. Les données indexées ADN sont traitées conformément au présent règlement et dans le respect du droit national applicable au traitement de ces données.

3. La Commission adopte un acte d'exécution afin de préciser les caractéristiques d'identification d'un profil ADN devant être échangé. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 6

Consultation automatisée de profils ADN

1. Aux fins d'enquêtes en matière d'infractions pénales, les États membres effectuent, lors de la première connexion au routeur par l'intermédiaire de leurs points de contact nationaux, une consultation automatisée en comparant tous les profils ADN stockés dans leurs bases de données ADN, avec tous les profils ADN stockés dans les bases de données ADN de tous les autres États membres et les données d'Europol. Chaque État membre convient de manière bilatérale avec chaque autre État membre et Europol des modalités de ces consultations automatisées conformément aux règles et aux procédures prévues par le présent règlement.
2. Aux fins d'enquêtes en matière d'infractions pénales, les États membres effectuent, par l'intermédiaire de leurs points de contact nationaux, des consultations automatisées en comparant tous les nouveaux profils ADN ajoutés à leurs bases de données ADN avec tous les profils ADN stockés dans les bases de données ADN de tous les autres États membres et les données d'Europol.

3. Lorsque les consultations visées au paragraphe 2 n'ont pas pu être effectuées, l'État membre concerné peut convenir de manière bilatérale avec chaque autre État membre et avec Europol de les effectuer à un stade ultérieur en comparant les profils ADN avec tous les profils ADN stockés dans les bases de données ADN de tous les autres États membres et les données d'Europol. L'État membre concerné convient de manière bilatérale avec chaque autre État membre et avec Europol des modalités de ces consultations automatisées conformément aux règles et aux procédures prévues par le présent règlement.
4. Les consultations visées aux paragraphes 1, 2 et 3 ne sont effectuées que dans le cadre d'affaires individuelles et dans le respect du droit national de l'État membre requérant.
5. Lorsqu'une consultation automatisée révèle une concordance entre un profil ADN transmis et les profils ADN stockés dans la ou les bases de données consultées 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 concordance a été mise en évidence.
6. Le point de contact national de l'État membre requérant peut décider de confirmer une concordance entre deux profils ADN. Lorsqu'il décide de confirmer une concordance entre deux profils ADN, il en informe l'État membre requis et veille à ce qu'au moins un membre qualifié du personnel procède à un examen manuel pour confirmer cette concordance avec les données indexées ADN reçues de l'État membre requis.

7. Lorsque cela est pertinent aux fins d'enquêtes en matière d'infractions pénales, le point de contact national de l'État membre requis peut décider de confirmer une concordance entre deux profils ADN. Lorsqu'il décide de confirmer une concordance entre deux profils ADN, il en informe l'État membre requérant et veille à ce qu'au moins un membre qualifié du personnel procède à un examen manuel pour confirmer cette concordance avec les données indexées ADN reçues de l'État membre requérant.

Article 7

Références des profils ADN

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

- a) une référence permettant aux États membres, en cas de concordance, d'extraire des données supplémentaires et d'autres informations de leurs bases de données ADN nationales afin de les transmettre à un, à plusieurs ou à tous les autres États membres, conformément à l'article 47, ou à Europol, conformément à l'article 49, paragraphe 6;
- b) une référence permettant à Europol, en cas de concordance, d'extraire des données supplémentaires et d'autres informations aux fins de l'article 48, paragraphe 1, du présent règlement afin de les transmettre à un, à plusieurs ou à tous les États membres conformément au règlement (UE) 2016/794;
- c) un code indiquant l'État membre qui détient le profil ADN;

- d) un code indiquant si le profil ADN est un profil ADN identifié ou un profil ADN non identifié.

Article 8

Principes régissant l'échange de profils ADN

1. Les États membres prennent des mesures appropriées pour assurer la confidentialité et l'intégrité des données indexées ADN transmises aux autres États membres ou à Europol, y compris leur cryptage. Europol prend des mesures appropriées pour assurer la confidentialité et l'intégrité des données indexées ADN transmises aux États membres, y compris leur cryptage.
2. Chaque État membre et Europol veillent à ce que les profils ADN qu'ils transmettent soient d'une qualité suffisante pour permettre une comparaison automatisée. La Commission établit, par voie d'actes d'exécution, une norme de qualité minimale pour permettre la comparaison des profils ADN.
3. La Commission adopte des actes d'exécution précisant les normes européennes ou internationales à utiliser par les États membres et par Europol pour l'échange de données indexées ADN.
4. Les actes d'exécution visés aux paragraphes 2 et 3 du présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 9

Règles applicables aux demandes et aux réponses relatives aux profils ADN

1. Une demande de consultation automatisée de profils ADN inclut uniquement les informations suivantes:
 - a) le code de l'État membre requérant;
 - b) les date et heure de la demande et le numéro de demande;
 - c) les données indexées ADN;
 - d) une indication précisant si les profils ADN transmis sont des profils ADN non identifiés ou des profils ADN identifiés.

2. Une réponse apportée à une demande visée au paragraphe 1 inclut uniquement les informations suivantes:
 - a) une indication précisant s'il y a eu une ou plusieurs concordances ou aucune concordance;
 - b) les date et heure de la demande et le numéro de demande;
 - c) les date et heure de la réponse et le numéro de 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) une indication précisant si les profils ADN transmis sont des profils ADN non identifiés ou des profils ADN identifiés;
 - g) les profils ADN pour lesquels une concordance est établie.
3. Une concordance n'est automatiquement notifiée que lorsque la consultation automatisée a mis en évidence une concordance fondée sur un nombre minimal de loci. La Commission adopte des actes d'exécution précisant le nombre minimal de loci à cette fin en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.
4. Lorsqu'une consultation effectuée avec des profils ADN non identifiés met en évidence une concordance, chaque État membre requis disposant de données concordantes peut insérer, dans sa base de données nationale, une marque indiquant que ce profil ADN a déjà fait l'objet d'une concordance à la suite d'une consultation effectuée par un autre État membre. Le marquage comprend la référence du profil ADN utilisé par l'État membre requérant.
5. Les États membres veillent à ce que les demandes visées au paragraphe 1 du présent article soient cohérentes avec les notifications transmises en vertu de l'article 74. Ces notifications figurent dans le manuel pratique visé à l'article 79.

SECTION 2

DONNEES DACTYLOSCOPIQUES

Article 10

Données indexées dactyloscopiques

1. Les États membres s'assurent de la disponibilité des données indexées dactyloscopiques provenant de leurs bases de données nationales créées aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière.
2. Les données indexées dactyloscopiques ne contiennent aucune donnée supplémentaire permettant l'identification directe d'une personne.
3. Les données dactyloscopiques non identifiées sont reconnaissables en tant que telles.

Article 11

Consultation automatisée de données dactyloscopiques

1. Aux fins de la prévention et de la détection des infractions pénales et 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 stockées dans leurs bases de données nationales créées à cet effet, pour effectuer des consultations automatisées par comparaison de données indexées dactyloscopiques.

Les consultations visées au premier alinéa ne sont effectuées que dans le cadre d'affaires individuelles et dans le respect du droit national de l'État membre requérant.

2. Le point de contact national de l'État membre requérant peut décider de confirmer une concordance entre deux ensembles de données dactyloscopiques. Lorsqu'il décide de confirmer une concordance entre deux ensembles de données dactyloscopiques, il en informe l'État membre requis et veille à ce qu'au moins un membre qualifié du personnel procède à un examen manuel pour confirmer cette concordance avec les données indexées dactyloscopiques reçues de l'État membre requis.

Article 12

Références des données dactyloscopiques

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

- a) une référence permettant aux États membres, en cas de concordance, d'extraire des données supplémentaires et d'autres informations de leurs bases de données visées à l'article 10 afin de les transmettre à un, à plusieurs ou à tous les autres États membres, conformément à l'article 47, ou à Europol, conformément à l'article 49, paragraphe 6;
- b) une référence permettant à Europol, en cas de concordance, d'extraire des données supplémentaires et d'autres informations aux fins de l'article 48, paragraphe 1, du présent règlement afin de les transmettre à un, à plusieurs ou à tous les États membres conformément au règlement (UE) 2016/794;

- c) un code indiquant l'État membre qui détient les données dactyloscopiques.

Article 13

Principes régissant l'échange de données dactyloscopiques

1. Les États membres prennent des mesures appropriées pour assurer la confidentialité et l'intégrité des données dactyloscopiques transmises aux autres États membres ou à Europol, y compris leur cryptage. Europol prend des mesures appropriées pour assurer la confidentialité et l'intégrité des données dactyloscopiques transmises aux États membres, y compris leur cryptage.
2. Tous les États membres et Europol veillent à ce que les données dactyloscopiques qu'ils transmettent soient d'une qualité suffisante pour permettre une comparaison automatisée. La Commission établit, par voie d'actes d'exécution, une norme de qualité minimale pour permettre la comparaison des données dactyloscopiques.
3. Les données dactyloscopiques sont numérisées et transmises aux autres États membres ou à Europol conformément aux normes européennes ou internationales. La Commission adopte des actes d'exécution précisant les normes européennes ou internationales pertinentes à utiliser par les États membres et par Europol pour l'échange de données dactyloscopiques.
4. Les actes d'exécution visés aux paragraphes 2 et 3 du présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 14

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 ou par Europol afin de garantir la disponibilité du système et d'éviter qu'il ne soit surchargé. Dans le même but, Europol 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 les autres États membres, la Commission, l'eu-LISA et Europol de leurs capacités maximales de consultation par jour pour les données dactyloscopiques identifiées et non identifiées. Europol informe les États membres, la Commission et l'eu-LISA de ses capacités maximales de consultation par jour pour les données dactyloscopiques identifiées et non identifiées. Les États membres ou Europol peuvent, de manière temporaire ou permanente, augmenter ces capacités de consultation à tout moment, notamment en cas d'urgence. Lorsqu'un État membre augmente ces capacités maximales de consultation, il notifie aux autres États membres, à la Commission, à l'eu-LISA et à Europol les nouvelles capacités maximales de consultation. Lorsqu'Europol augmente ces capacités maximales de consultation, il notifie aux États membres, à la Commission et à l'eu-LISA les nouvelles capacités maximales de consultation.

2. La Commission adopte des actes d'exécution précisant les nombres maximaux de candidats admis pour comparaison par transmission et la répartition entre les États membres des capacités de consultation non utilisées, en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 15

*Règles applicables aux demandes et aux réponses
relatives aux données dactyloscopiques*

1. Une demande de consultation automatisée de données dactyloscopiques inclut uniquement les informations suivantes:
 - a) le code de l'État membre requérant;
 - b) les date et heure de la demande et le numéro de demande;
 - c) les données indexées dactyloscopiques.
2. Une réponse apportée à une demande visée au paragraphe 1 inclut uniquement les informations suivantes:
 - a) une indication précisant s'il y a eu une ou plusieurs concordances ou aucune concordance;
 - b) les date et heure de la demande et le numéro de demande;
 - c) les date et heure de la réponse et le numéro de 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 concordance est établie.
3. Les États membres veillent à ce que les demandes visées au paragraphe 1 du présent article soient cohérentes avec les notifications transmises en vertu de l'article 74. Ces notifications figurent dans le manuel pratique visé à l'article 79.

SECTION 3

DONNEES RELATIVES A L'IMMATRICULATION DES VEHICULES

Article 16

Consultation automatisée de données relatives à l'immatriculation des véhicules

1. Aux fins de la prévention et de la détection des infractions pénales et 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 relatives à l'immatriculation des véhicules suivantes, afin d'effectuer, dans le cadre d'affaires individuelles, des consultations automatisées:
- a) les données relatives au propriétaire ou au détenteur du véhicule;
 - b) les données relatives au véhicule.

2. Les consultations visées au paragraphe 1 ne sont effectuées qu'avec les éléments suivants:
 - a) un numéro de châssis complet;
 - b) un numéro d'immatriculation complet; ou
 - c) lorsque le droit national de l'État membre requis l'autorise, les données relatives au propriétaire ou au détenteur du véhicule.

3. Les consultations visées au paragraphe 1 effectuées avec des données relatives au propriétaire ou au détenteur du véhicule ne sont effectuées que dans le cas de suspects ou de personnes condamnées. Toutes les données d'identification suivantes sont utilisées aux fins de ces consultations:
 - a) lorsque le propriétaire ou le détenteur du véhicule est une personne physique:
 - i) le ou les prénoms de la personne physique;
 - ii) le ou les noms de famille de la personne physique; et
 - iii) la date de naissance de la personne physique;
 - b) lorsque le propriétaire ou le détenteur du véhicule est une personne morale, le nom de cette personne morale.

4. Les consultations visées au paragraphe 1 ne sont effectuées que dans le respect du droit national de l'État membre requérant.

Article 17

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 précisant les éléments de données des données relatives à l'immatriculation des véhicules qui peuvent être échangés et la procédure technique permettant à Eucaris d'interroger les bases de données des États membres. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 18

Tenue de registres

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

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

- a) une indication précisant si c'est un État membre ou Europol qui a lancé la demande d'interrogation; lorsque c'est un État membre qui a lancé la demande d'interrogation, l'État membre en question;
- b) les date et heure de la demande;
- c) les date et heure de la réponse;
- d) les bases de données nationales auxquelles une demande d'interrogation a été envoyée;
- e) les bases de données nationales qui ont fourni une réponse positive.

2. Les registres visés au paragraphe 1 ne sont utilisés que pour collecter des statistiques, pour contrôler la protection des données, y compris vérifier l'admissibilité d'une interrogation 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 trois ans 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 à ces procédures.

3. Aux fins du contrôle de la protection des données, y compris de la vérification de l'admissibilité d'une interrogation 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 55.

SECTION 4

IMAGES FACIALES

Article 19

Données indexées d'images faciales

1. Les États membres s'assurent de la disponibilité des données indexées d'images faciales des suspects, des personnes condamnées et, lorsque le droit national l'autorise, des victimes, provenant de leurs bases de données nationales créées aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière.
2. Les données indexées d'images faciales ne contiennent aucune donnée supplémentaire permettant l'identification directe d'une personne.
3. Les images faciales non identifiées sont reconnaissables en tant que telles.

Article 20

Consultation automatisée d'images faciales

1. Aux fins de la prévention et de la détection des infractions pénales passibles d'une peine maximale d'emprisonnement d'au moins un an au titre du droit de l'État membre requérant, et 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 d'images faciales stockées dans leurs bases de données nationales, afin d'effectuer des consultations automatisées.

Les consultations visées au premier alinéa ne sont effectuées que dans le cadre d'affaires individuelles et dans le respect du droit national de l'État membre requérant.

Le profilage tel qu'il est visé à l'article 11, paragraphe 3, de la directive (UE) 2016/680 est interdit.

2. Le point de contact national de l'État membre requérant peut décider de confirmer une concordance entre deux images faciales. Lorsqu'il décide de confirmer une concordance entre deux images faciales, il en informe l'État membre requis et veille à ce qu'au moins un membre qualifié du personnel procède à un examen manuel pour confirmer cette concordance avec les données indexées d'images faciales reçues de l'État membre requis.

Article 21

Références des images faciales

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

- a) une référence permettant aux États membres, en cas de concordance, d'extraire des données supplémentaires et d'autres informations de leurs bases de données visées à l'article 19 afin de les transmettre à un, à plusieurs ou à tous les autres États membres, conformément à l'article 47, ou à Europol, conformément à l'article 49, paragraphe 6;
- b) une référence permettant à Europol, en cas de concordance, d'extraire des données supplémentaires et d'autres informations aux fins de l'article 48, paragraphe 1, du présent règlement afin de les transmettre à un, à plusieurs ou à tous les États membres, conformément au règlement (UE) 2016/794;
- c) un code indiquant l'État membre qui détient les images faciales.

Article 22

Principes régissant l'échange d'images faciales

1. Les États membres prennent des mesures appropriées pour assurer la confidentialité et l'intégrité des images faciales transmises aux autres États membres ou à Europol, y compris leur cryptage. Europol prend des mesures appropriées pour assurer la confidentialité et l'intégrité des images faciales transmises aux États membres, y compris leur cryptage.

2. Chaque État membre et Europol veillent à ce que les images faciales qu'ils transmettent soient d'une qualité suffisante pour permettre une comparaison automatisée. La Commission établit, par voie d'actes d'exécution, une norme de qualité minimale pour permettre la comparaison des images faciales. Lorsque le rapport visé à l'article 80, paragraphe 7, fait apparaître un risque élevé de fausses concordances, la Commission réexamine ces actes d'exécution.
3. La Commission adopte des actes d'exécution précisant les normes européennes ou internationales pertinentes à utiliser par les États membres et par Europol pour l'échange d'images faciales.
4. Les actes d'exécution visés aux paragraphes 2 et 3 du présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 23

Capacités de consultation pour les images faciales

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 ou par Europol afin de garantir la disponibilité du système et d'éviter qu'il ne soit surchargé. Dans le même but, Europol 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 les autres États membres, la Commission, l'eu-LISA et Europol de leurs capacités maximales de consultation par jour pour les images faciales identifiées et non identifiées. Europol informe les États membres, la Commission et l'eu-LISA de ses capacités maximales de consultation par jour pour les images faciales identifiées et non identifiées. Les États membres ou Europol peuvent, de manière temporaire ou permanente, augmenter ces capacités de consultation à tout moment, notamment en cas d'urgence. Lorsqu'un État membre augmente ces capacités maximales de consultation, il notifie aux autres États membres, à la Commission, à l'eu-LISA et à Europol les nouvelles capacités maximales de consultation. Lorsqu'Europol augmente ces capacités maximales de consultation, il notifie aux États membres, à la Commission et à l'eu-LISA les nouvelles capacités maximales de consultation.

2. La Commission adopte des actes d'exécution précisant les nombres maximaux de candidats admis pour comparaison par transmission et la répartition entre les États membres des capacités de consultation non utilisées, en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 24

Règles applicables aux demandes et aux réponses relatives aux images faciales

1. Une demande de consultation automatisée d'images faciales inclut uniquement les informations suivantes:
 - a) le code de l'État membre requérant;

- b) les date et heure de la demande et le numéro de demande;
 - c) les données indexées d'images faciales.
2. Une réponse apportée à une demande visée au paragraphe 1 inclut uniquement les informations suivantes:
- a) une indication précisant s'il y a eu une ou plusieurs concordances ou aucune concordance;
 - b) les date et heure de la demande et le numéro de demande;
 - c) les date et heure de la réponse et le numéro de 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 concordance est établie.
3. Les États membres veillent à ce que les demandes visées au paragraphe 1 du présent article soient cohérentes avec les notifications transmises en vertu de l'article 74. Ces notifications figurent dans le manuel pratique visé à l'article 79.

SECTION 5

FICHIERS DE POLICE

Article 25

Fichiers de police

1. Les États membres peuvent participer à l'échange automatisé de fichiers de police. Aux fins de ces échanges, les États membres participants s'assurent de la disponibilité des index nationaux des fichiers de police qui contiennent des ensembles de données biographiques de suspects et de personnes condamnées provenant de leurs bases de données nationales créées aux fins de la prévention et de la détection des infractions pénales et des enquêtes en la matière. Ces ensembles de données ne contiennent que les données suivantes dans la mesure où elles sont disponibles:
 - a) le ou les prénoms;
 - b) le ou les noms de famille;
 - c) le ou les pseudonymes et le ou les noms utilisés antérieurement;
 - d) la date de naissance;
 - e) la ou les nationalités;
 - f) le pays de naissance;
 - g) le sexe.

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

Article 26

Consultation automatisée des index nationaux des fichiers de police

Aux fins de la prévention et de la détection des infractions pénales passibles d'une peine maximale d'emprisonnement d'au moins un an au titre du droit de l'État membre requérant, et des enquêtes en la matière, les États membres qui participent à l'échange automatisé de fichiers de police autorisent les points de contact nationaux d'autres États membres participants et Europol à accéder aux données provenant de leurs index nationaux des fichiers de police, afin d'effectuer des consultations automatisées.

Les consultations visées au premier alinéa ne sont effectuées que dans le cadre d'affaires individuelles et dans le respect du droit national de l'État membre requérant.

Article 27

Références des fichiers de police

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

- a) une référence permettant aux États membres, en cas de concordance, d'extraire des données biographiques et d'autres informations de leurs index nationaux des fichiers de police visés à l'article 25 afin de les transmettre à un, à plusieurs ou à tous les autres États membres, conformément à l'article 44;
- b) un code indiquant l'État membre qui détient les fichiers de police.

Article 28

Règles applicables aux demandes et aux réponses relatives aux fichiers de police

1. Une demande de consultation automatisée des index nationaux des fichiers de police inclut uniquement les informations suivantes:
 - a) le code de l'État membre requérant;
 - b) les date et heure de la demande et le numéro de demande;
 - c) les données visées à l'article 25, dans la mesure où elles sont disponibles.

2. Une réponse apportée à une demande visée au paragraphe 1 inclut uniquement les informations suivantes:
 - a) une indication précisant le nombre de concordances;
 - b) les date et heure de la demande et le numéro de demande;
 - c) les date et heure de la réponse et le numéro de réponse;
 - d) les codes de l'État membre requérant et de l'État membre requis;
 - e) les références des fichiers de police obtenus des États membres requis.

3. Les États membres veillent à ce que les demandes visées au paragraphe 1 du présent article soient cohérentes avec les notifications transmises en vertu de l'article 74. Ces notifications figurent dans le manuel pratique visé à l'article 79.

SECTION 6
DISPOSITIONS COMMUNES

Article 29

Personnes disparues et restes humains non identifiés

1. Lorsqu'une autorité nationale y a été habilitée par des mesures législatives nationales visées au paragraphe 2, elle peut effectuer des consultations automatisées en utilisant le cadre Prüm II uniquement aux fins suivantes:
 - a) la recherche de personnes disparues dans le cadre d'enquêtes pénales ou pour des motifs humanitaires;
 - b) l'identification de restes humains.

2. Les États membres qui souhaitent faire usage de la possibilité prévue au paragraphe 1 désignent, au moyen de mesures législatives nationales, les autorités nationales compétentes aux fins qui y sont prévues et fixent les procédures, les conditions et les critères, y compris les motifs humanitaires pour lesquels il est autorisé d'effectuer des consultations automatisées aux fins de la recherche de personnes disparues visée au paragraphe 1, point a).

Article 30

Points de contact nationaux

Chaque État membre désigne un ou plusieurs points de contact nationaux aux fins des articles 6, 11, 16, 20 et 26.

Article 31

Mesures d'exécution

La Commission adopte des actes d'exécution précisant les modalités techniques applicables aux États membres en ce qui concerne les procédures énoncées aux articles 6, 11, 16, 20 et 26. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 77, 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 automatisée de profils ADN, de données dactyloscopiques, de données relatives à l'immatriculation de véhicules, d'images faciales et de fichiers de police soit possible 24 heures sur 24, sept jours sur sept.

2. Les points de contact nationaux s'informent immédiatement mutuellement et informent immédiatement la Commission, l'eu-LISA et Europol de toute indisponibilité de l'échange automatisé de données, y compris, le cas échéant, de toute défaillance technique entraînant cette indisponibilité.

Les points de contact nationaux conviennent, conformément au droit de l'Union et au droit national applicables, d'autres modalités temporaires d'échange d'informations à utiliser lorsque l'échange automatisé de données est indisponible.

3. Lorsque l'échange automatisé de données est indisponible, les points de contact nationaux veillent à ce qu'il soit rétabli par tous les moyens nécessaires et sans tarder.

Article 33

Justification du traitement des données

1. Chaque État membre conserve une trace des justifications des interrogations effectuées par ses autorités compétentes.

Europol conserve une trace des justifications des interrogations qu'elle effectue.

2. Les justifications visées au paragraphe 1 comprennent:
 - a) l'objet de l'interrogation, y compris une référence à l'affaire ou à l'enquête spécifique et, le cas échéant, à l'infraction pénale;

- b) une indication précisant si l'interrogation concerne un suspect ou une personne condamnée pour une infraction pénale, une victime d'une infraction pénale, une personne disparue ou des restes humains non identifiés;
 - c) une indication précisant si l'interrogation vise à identifier une personne ou à obtenir plus de données sur une personne connue.
3. Les justifications visées au paragraphe 1 du présent article peuvent être reliées aux registres visés aux articles 18, 40 et 45. Ces justifications ne peuvent être utilisées que pour évaluer si les consultations sont proportionnées et nécessaires aux fins de la prévention et de la détection d'une infraction pénale et des enquêtes en la matière, pour contrôler la protection des données, y compris vérifier l'admissibilité d'une interrogation 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 trois ans 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. Pour évaluer la proportionnalité et la nécessité des consultations aux fins de la prévention ou de la détection d'une infraction pénale, ou des enquêtes en la matière, ou aux fins du contrôle de la protection des données, y compris de la vérification de l'admissibilité d'une interrogation 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 55.

Article 34

Utilisation du format universel pour les messages

1. La norme de format universel pour les messages (UMF) établie par l'article 38 du règlement (UE) 2019/818 est utilisée pour le développement du routeur visé à l'article 35 du présent règlement et du système d'index européen des fichiers de police (EPRIS) autant que possible.
2. Tout échange automatisé de données conformément au présent règlement utilise la norme UMF autant que possible.

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 entre les États membres et Europol aux fins de l'interrogation, de l'extraction et de la notation de données biométriques ainsi que de l'extraction de données alphanumériques 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 nationales visées aux articles 5, 10 et 19 et des données d'Europol;
 - b) un canal de communication sécurisé entre l'infrastructure centrale, les autorités compétentes autorisées à utiliser le routeur en vertu de l'article 36 et Europol;

- c) une infrastructure de communication sécurisée entre l'infrastructure centrale et le portail de recherche européen, établie par l'article 6 du règlement (UE) 2019/817 et l'article 6 du règlement (UE) 2019/818, aux fins de l'article 39.

Article 36

Utilisation du routeur

L'utilisation du routeur est réservée aux autorités compétentes des États membres qui sont autorisées à accéder aux profils ADN, aux données dactyloscopiques et aux images faciales et à les échanger, conformément au présent règlement, ainsi qu'à Europol, conformément au présent règlement et au règlement (UE) 2016/794.

Article 37

Processus

1. Les autorités compétentes autorisées à utiliser le routeur en vertu de l'article 36 ou Europol demandent une interrogation en soumettant des données biométriques au routeur. Le routeur envoie la demande d'interrogation aux bases de données de tous les États membres ou de certains États membres et aux données d'Europol en même temps que les données soumises par l'utilisateur conformément à ses droits d'accès.

2. Dès réception d'une demande d'interrogation en provenance du routeur, chaque État membre requis interroge ses bases de données de manière automatisée et sans tarder. Dès réception d'une demande d'interrogation en provenance du routeur, Europol interroge les données d'Europol de manière automatisée et sans tarder.
3. Toute concordance mise en évidence à partir des interrogations visées au paragraphe 2 est renvoyée de manière automatisée au routeur. Lorsqu'il n'y a pas de concordance, l'État membre requérant reçoit une notification de manière automatisée.
4. Le routeur classe, lorsque l'État membre requérant le décide et s'il y a lieu, les réponses en comparant les données biométriques utilisées pour les interrogations et les données biométriques transmises dans les réponses du ou des États membres requis ou d'Europol.
5. Le routeur renvoie la liste des données biométriques pour lesquelles une concordance a été établie et leur classement à l'utilisateur du routeur.
6. La Commission adopte des actes d'exécution précisant la procédure technique permettant au routeur d'interroger les bases de données des États membres et les données d'Europol, le format dans lequel le routeur répond à ces interrogations ainsi que les règles techniques de comparaison et de classement des concordances entre les données biométriques. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 38
Contrôle de la qualité

L'État membre requis contrôle, selon une procédure automatisée, la qualité des données transmises.

Lorsque 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 à des fins répressives

1. Lorsque les autorités désignées, telles qu'elles sont définies à l'article 4, point 20), du règlement (UE) 2019/817 et à l'article 4, point 20), du règlement (UE) 2019/818, sont autorisées à utiliser le routeur en vertu de l'article 36 du présent règlement, elles peuvent interroger les bases de données des États membres et les données d'Europol en même temps que 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, sous réserve que les conditions applicables au titre du droit de l'Union aient été remplies et que l'interrogation soit lancée 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 interrogations du 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 de ces interrogations est transmis par l'intermédiaire du portail de recherche européen.

Des interrogations simultanées des bases de données des États membres et des données d'Europol et du répertoire commun de données d'identité ne sont lancées que lorsqu'il existe des motifs raisonnables de croire que des données sur un suspect, un auteur ou une victime d'une infraction terroriste ou d'autres infractions pénales graves, telles qu'elles sont définies 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) une indication précisant si c'est un État membre ou Europol qui a lancé la demande d'interrogation; lorsque c'est un État membre qui a lancé la demande d'interrogation, l'État membre en question;
 - b) les date et heure de la demande;

- c) les date et heure de la réponse;
 - d) les bases de données nationales ou les données d'Europol auxquelles une demande d'interrogation 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 interrogation a été effectuée en même temps dans le répertoire commun de données d'identité.
2. Chaque État membre tient des registres des interrogations effectuées par le personnel de ses autorités compétentes dûment autorisé à utiliser le routeur et des registres des interrogations demandées par les autres États membres.
- Europol tient des registres des interrogations effectuées par son personnel dûment autorisé.
3. Les registres visés aux paragraphes 1 et 2 ne sont utilisés que pour collecter des statistiques, pour contrôler la protection des données, y compris vérifier l'admissibilité d'une interrogation 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 trois ans 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 à ces procédures.
4. Aux fins du contrôle de la protection des données, y compris de la vérification de l'admissibilité d'une interrogation 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 55.

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, l'eu-LISA adresse une notification, de manière automatisée, aux utilisateurs du routeur visés à l'article 36. L'eu-LISA prend des mesures appropriées pour remédier sans tarder 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 en raison d'une défaillance de l'infrastructure nationale d'un État membre, cet État membre adresse une notification, de manière automatisée, aux autres États membres, à la Commission, à l'eu-LISA et à Europol. L'État membre concerné prend les mesures appropriées pour remédier sans tarder à l'impossibilité technique d'utiliser le routeur.

3. Lorsqu'il est techniquement impossible d'utiliser le routeur pour interroger les données d'Europol en raison d'une défaillance de l'infrastructure d'Europol, Europol adresse une notification, de manière automatisée, aux États membres, à la Commission et à l'eu-LISA. Europol prend les mesures appropriées pour remédier sans tarder à l'impossibilité technique d'utiliser le routeur.

SECTION 2

EPRIS

Article 42

EPRIS

1. Le système d'index européen des fichiers de police (EPRIS) est établi. Aux fins de la consultation automatisée des index nationaux des fichiers de police visée à l'article 26, les États membres et Europol utilisent l'EPRIS.
2. L'EPRIS se compose des éléments suivants:
 - a) une infrastructure décentralisée dans les États membres, comprenant un outil de recherche permettant l'interrogation simultanée des index nationaux des fichiers de police, qui repose sur les bases de données nationales;
 - b) une infrastructure centrale, soutenant l'outil de recherche, permettant l'interrogation simultanée des index nationaux des fichiers de police;
 - c) un canal de communication sécurisé entre l'infrastructure centrale, les États membres et Europol.

Article 43
Utilisation de l'EPRIS

1. Aux fins de la consultation des index nationaux des fichiers de police par l'intermédiaire de l'EPRIS, au moins deux des ensembles de données suivants sont utilisés:
 - a) le ou les prénoms;
 - b) le ou les noms de famille;
 - c) la date de naissance.

2. Lorsqu'ils sont disponibles, les ensembles de données suivants peuvent également être utilisés:
 - a) le ou les pseudonymes et le ou les noms utilisés antérieurement;
 - b) la ou les nationalités;
 - c) le pays de naissance;
 - d) le sexe.

3. Les données visées au paragraphe 1, points a) et b), et au paragraphe 2, point a), sont pseudonymisées.

Article 44
Processus

1. Lorsqu'un État membre ou Europol demande une interrogation, il soumet les données visées à l'article 43.

L'EPRIS envoie la demande d'interrogation aux index nationaux des fichiers de police des États membres avec les données soumises par l'État membre requérant ou par Europol et conformément au présent règlement.

2. Dès réception d'une demande d'interrogation en provenance de l'EPRIS, chaque État membre requis interroge son index national des fichiers de police de manière automatisée et sans tarder.
3. Toute concordance mise en évidence à partir des interrogations visées au paragraphe 1 dans les index des fichiers de police de chaque État membre requis est renvoyée de manière automatisée à l'EPRIS.
4. La liste des concordances est renvoyée de manière automatisée à l'État membre requérant ou à Europol par l'EPRIS. La liste des concordances indique la qualité de la concordance ainsi que le ou les États membres dont les index des fichiers de police contiennent les données qui ont mis en évidence la ou les concordances.

5. Dès réception de la liste des concordances, l'État membre requérant décide des concordances pour lesquelles un suivi est nécessaire et envoie une demande de suivi motivée contenant les données visées aux articles 25 et 27 ainsi que toute information complémentaire pertinente à l'État membre ou aux États membres requis au moyen de SIENA. L'État membre ou les États membres requis traitent ces demandes sans tarder afin de décider de partager ou non les données stockées dans sa ou leur base de données.
6. La Commission adopte des actes d'exécution précisant la procédure technique permettant à l'EPRIS d'interroger les index des fichiers de police des États membres ainsi que le format des réponses et leur nombre maximal. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 45

Tenue de registres

1. Chaque État membre participant et Europol tiennent des registres de toutes les opérations de traitement de données effectuées dans l'EPRIS. Ces registres contiennent les informations suivantes:
 - a) une indication précisant si c'est un État membre ou Europol qui a lancé la demande d'interrogation; lorsque c'est un État membre qui a lancé la demande d'interrogation, l'État membre en question;
 - b) les date et heure de la demande;
 - c) les date et 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 participant tient des registres des demandes d'interrogation effectuées par le personnel de ses autorités compétentes dûment autorisé à utiliser l'EPRIS. Europol tient des registres des demandes d'interrogation effectuées par son personnel dûment autorisé.
 3. Les registres visés aux paragraphes 1 et 2 ne sont utilisés que pour collecter des statistiques, pour contrôler la protection des données, y compris vérifier l'admissibilité d'une interrogation 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 trois ans 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 à ces procédures.
 4. Aux fins du contrôle de la protection des données, y compris de la vérification de l'admissibilité d'une interrogation 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 55.

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 un ou plusieurs index nationaux des fichiers de police en raison d'une défaillance de l'infrastructure d'Europol, Europol adresse une notification, de manière automatisée, aux États membres. Europol prend des mesures pour remédier sans tarder à l'impossibilité technique d'utiliser l'EPRIS.

2. Lorsqu'il est techniquement impossible d'utiliser l'EPRIS pour interroger un ou plusieurs index nationaux des fichiers de police en raison d'une défaillance de l'infrastructure nationale d'un État membre, cet État membre adresse une notification, de manière automatisée, aux autres États membres, à la Commission et à Europol. Les États membres prennent des mesures pour remédier sans tarder à l'impossibilité technique d'utiliser l'EPRIS.

Chapitre 4

Échange de données à la suite d'une concordance

Article 47

Échange de données de base

1. Un ensemble de données de base est renvoyé par l'intermédiaire du routeur dans un délai de 48 heures à compter du moment où toutes les conditions suivantes sont remplies:
 - a) les procédures visées à l'article 6, 11 ou 20 révèlent une concordance entre les données utilisées pour la consultation et les données stockées dans la base de données de l'État membre ou des États membres requis;
 - b) la concordance visée au point a) du présent paragraphe a été confirmée de manière manuelle par un membre qualifié du personnel de l'État membre requérant visé à l'article 6, paragraphe 6, à l'article 11, paragraphe 2, et à l'article 20, paragraphe 2, ou, dans le cas de profils ADN visés à l'article 6, paragraphe 7, de l'État membre requis;

- c) une description des faits et une indication de l'infraction sous-jacente ont été transmises, au moyen du tableau commun des catégories d'infractions figurant dans un acte d'exécution à adopter en vertu de l'article 11 *ter*, paragraphe 1, point a), de la décision-cadre 2009/315/JAI, par l'État membre requérant, ou, dans le cas de profils ADN visés à l'article 6, paragraphe 7, par l'État membre requis, afin d'évaluer la proportionnalité de la demande, y compris la gravité de l'infraction pour laquelle une consultation a été effectuée, conformément au droit national de l'État membre qui fournit l'ensemble de données de base.
2. Lorsque, selon son droit national, un État membre ne peut fournir un ensemble précis de données de base qu'après avoir obtenu une autorisation judiciaire, cet État membre peut déroger au délai énoncé au paragraphe 1 dans la mesure où cela est nécessaire pour obtenir cette autorisation.
3. L'ensemble de données de base visé au paragraphe 1 du présent article est renvoyé par l'État membre requis ou, dans le cas de profils ADN visés à l'article 6, paragraphe 7, par l'État membre requérant.
4. Lorsque la concordance confirmée concerne les données identifiées d'une personne, l'ensemble de données de base visé au paragraphe 1 contient les données suivantes dans la mesure où elles sont disponibles:
- a) le ou les prénoms;
 - b) le ou les noms de famille;
 - c) le ou les pseudonymes et le ou les noms utilisés antérieurement;

- d) la date de naissance;
 - e) la ou les nationalités;
 - f) le lieu et le pays de naissance;
 - g) le sexe;
 - h) la date et le lieu où les données biométriques ont été acquises;
 - i) l'infraction pénale pour laquelle les données biométriques ont été acquises;
 - j) le numéro de l'affaire pénale;
 - k) l'autorité compétente responsable de l'affaire pénale.
5. Lorsque la concordance confirmée concerne des données ou des traces non identifiées, l'ensemble de données de base visé au paragraphe 1 contient les données suivantes dans la mesure où elles sont disponibles:
- a) la date et le lieu où les données biométriques ont été acquises;
 - b) l'infraction pénale pour laquelle les données biométriques ont été acquises;
 - c) le numéro de l'affaire pénale;
 - d) l'autorité compétente responsable de l'affaire pénale.
6. Le renvoi des données de base par l'État membre requis ou, dans le cas de profils ADN visés à l'article 6, paragraphe 7, par l'État membre requérant, est subordonné à la décision d'un être humain.

Chapitre 5

Europol

Article 48

Accès des États membres aux données biométriques fournies par des 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. Lorsqu'une consultation visée au paragraphe 1 met en évidence une concordance entre les données utilisées aux fins de la consultation et les données fournies par un pays tiers et stockées par Europol, le suivi a lieu conformément au règlement (UE) 2016/794.

Article 49

Accès d'Europol aux données stockées dans les bases de données des États membres, à l'aide des données fournies par des pays tiers

1. Lorsque cela est nécessaire pour atteindre les objectifs énoncés à l'article 3 du règlement (UE) 2016/794, Europol a accès, conformément audit règlement et au présent règlement, aux données qui sont stockées par les États membres dans leurs bases de données nationales et dans leurs index nationaux des fichiers de police.

2. Les interrogations d'Europol ayant des données biométriques pour critère de recherche sont effectuées à l'aide du routeur.
3. Les interrogations d'Europol ayant des données relatives à l'immatriculation des véhicules pour critère de recherche sont effectuées à l'aide d'Eucaris.
4. Les interrogations d'Europol ayant des données biographiques de suspects et de personnes condamnées visées à l'article 25 pour critère de recherche sont effectuées à l'aide de l'EPRIS.
5. Europol n'effectue des consultations avec les données fournies par des pays tiers conformément aux paragraphes 1 à 4 du présent article que lorsque cela est nécessaire à l'exécution de ses missions pour les finalités visées à l'article 18, paragraphe 2, points a) et c), du règlement (UE) 2016/794.
6. Lorsque les procédures visées à l'article 6, 11 ou 20 révèlent une concordance entre les données utilisées aux fins de la consultation et les données détenues dans la base de données nationale du ou des États membres requis, Europol n'informe que l'État membre ou les États membres impliqués.

L'État membre requis décide de renvoyer ou non un ensemble de données de base par l'intermédiaire du routeur dans les 48 heures à compter du moment où toutes les conditions suivantes sont remplies:

- a) la concordance visée au premier alinéa a été confirmée de manière manuelle par un membre qualifié du personnel d'Europol;

- b) une description des faits et une indication de l'infraction sous-jacente ont été transmises, au moyen du tableau commun des catégories d'infractions figurant dans un acte d'exécution à adopter en vertu de l'article 11 *ter*, paragraphe 1, point a), de la décision-cadre 2009/315/JHA, par Europol, afin d'évaluer la proportionnalité de la demande, y compris la gravité de l'infraction pour laquelle une consultation a été effectuée, conformément au droit national de l'État membre qui fournit l'ensemble de données de base;
- c) le nom du pays tiers qui a fourni les données a été transmis.

Lorsque, selon son droit national, un État membre ne peut fournir un ensemble précis de données de base qu'après avoir obtenu une autorisation judiciaire, cet État membre peut déroger au délai énoncé au deuxième alinéa dans la mesure où cela est nécessaire pour obtenir cette autorisation.

Lorsque la concordance confirmée concerne les données identifiées d'une personne, l'ensemble de données de base visé au deuxième alinéa contient les données suivantes dans la mesure où elles sont disponibles:

- a) le ou les prénoms;
- b) le ou les noms de famille;
- c) le ou les pseudonymes et le ou les noms utilisés antérieurement;
- d) la date de naissance;

- e) la ou les nationalités;
- f) le lieu et le pays de naissance;
- g) le sexe;
- h) la date et le lieu où les données biométriques ont été acquises;
- i) l'infraction pénale pour laquelle les données biométriques ont été acquises;
- j) le numéro de l'affaire pénale;
- k) l'autorité compétente responsable de l'affaire pénale.

Lorsque la concordance confirmée concerne des données ou des traces non identifiées, l'ensemble de données de base visé au deuxième alinéa contient les données suivantes dans la mesure où elles sont disponibles:

- a) la date et le lieu où les données biométriques ont été acquises;
- b) l'infraction pénale pour laquelle les données biométriques ont été acquises;
- c) le numéro de l'affaire pénale;
- d) l'autorité compétente responsable de l'affaire pénale.

Le renvoi de données de base par l'État membre requis est subordonné à la décision d'un être humain.

7. L'utilisation par Europol des informations obtenues à la suite d'une interrogation effectuée conformément au présent article et de l'échange d'un ensemble de données de base conformément au paragraphe 6 est soumise au consentement de l'État membre dans la base de données duquel la concordance a été mise en évidence. Lorsque 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 50

Finalité du traitement des données

1. Le traitement des données à caractère personnel reçues par un État membre ou par Europol est autorisé uniquement aux fins pour lesquelles les données ont été transmises par l'État membre qui a fourni les données conformément au présent règlement. Le traitement à d'autres fins n'est autorisé qu'avec l'autorisation préalable de l'État membre qui a fourni les données.

2. Le traitement des données transmises par un État membre ou par Europol en vertu de l'article 6, 11, 16, 20 ou 26 est autorisé uniquement lorsque cela est nécessaire aux fins suivantes:
 - a) établir si les profils ADN, les données dactyloscopiques, les données relatives à l'immatriculation des véhicules, les images faciales ou les fichiers de police qui sont comparés concordent;
 - b) échanger un ensemble de données de base conformément à l'article 47;
 - c) préparer et introduire une demande de coopération policière ou d'entraide judiciaire, en cas de concordance de ces données;
 - d) tenir des registres conformément aux articles 18, 40 et 45.

3. Les données reçues par les États membres ou Europol sont effacées immédiatement après les réponses automatisées aux consultations, à moins que la poursuite du traitement ne soit nécessaire aux fins visées au paragraphe 2 ou autorisée conformément au paragraphe 1.
4. Avant de connecter leurs bases de données nationales au routeur ou à l'EPRIS, les États membres effectuent une analyse d'impact relative à la protection des données conformément à l'article 27 de la directive (UE) 2016/680 et, le cas échéant, consultent l'autorité de contrôle comme le prévoit l'article 28 de ladite directive. L'autorité de contrôle peut faire usage des pouvoirs dont elle dispose au titre de l'article 47 de ladite directive, conformément à l'article 28, paragraphe 5, de ladite directive.

Article 51

Exactitude, pertinence et conservation des données

1. Les États membres et Europol s'assurent de l'exactitude et de la pertinence des données à caractère personnel qui sont traitées en vertu du présent règlement. Lorsqu'un État membre ou Europol se rend compte que des données qui sont inexactes ou qui ne sont plus d'actualité ou des données qui n'auraient pas dû être transmises ont été transmises, il le notifie à l'État membre qui a reçu les données ou à Europol sans retard injustifié. Tous les États membres concernés ou Europol rectifient ou suppriment les données en conséquence sans retard injustifié. Lorsque l'État membre qui a reçu les données ou Europol a des raisons de penser que les données transmises sont inexactes ou devraient être supprimées, il en informe l'État membre qui a fourni les données sans retard injustifié.

2. Les États membres et Europol mettent en place des mesures appropriées pour mettre à jour les données pertinentes aux fins du présent règlement.
3. Lorsqu'une personne concernée conteste l'exactitude des données en la possession d'un État membre ou d'Europol, lorsque l'exactitude ne peut être établie de manière fiable par l'État membre concerné ou Europol et lorsque la personne concernée le demande, les données concernées sont marquées. Les États membres ou Europol peuvent lever un tel marquage uniquement avec l'autorisation de la personne concernée ou sur le fondement d'une décision de la juridiction compétente, de l'autorité de contrôle ou du Contrôleur européen de la protection des données, selon le cas.
4. Les données qui n'auraient pas dû être transmises ou reçues sont supprimées. Les données qui ont été légalement transmises et reçues sont supprimées:
 - a) lorsqu'elles ne sont pas ou plus nécessaires au regard de la finalité pour laquelle elles ont été transmises;
 - b) à l'expiration du délai maximal de conservation des données prévu par le droit national de l'État membre qui a fourni les données lorsque celui-ci a informé l'État membre qui a reçu les données ou Europol de ce délai maximal au moment de la transmission des données; ou
 - c) à l'expiration du délai maximal de conservation des données prévu par le règlement (UE) 2016/794.

Lorsqu'il y a des raisons de penser que la suppression des données porterait atteinte aux intérêts de la personne concernée, ces données font l'objet d'une limitation de traitement au lieu d'être supprimées. Les données qui font l'objet d'une limitation de traitement sont traitées uniquement aux fins qui ont empêché leur suppression.

Article 52

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 au sens de l'article 3, point 12), du règlement (UE) 2018/1725 pour le traitement des données à caractère personnel par l'intermédiaire de l'EPRIS.

Article 53

Sécurité du traitement

1. Les autorités compétentes des États membres, l'eu-LISA et Europol veillent à la sécurité du traitement des données à caractère personnel au titre du présent règlement. Les autorités compétentes des États membres, l'eu-LISA et Europol 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. L'eu-LISA adopte les mesures nécessaires concernant le routeur et Europol adopte les mesures nécessaires concernant l'EPRIS 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, grâce à l'attribution d'identifiants individuels et à des modes d'accès confidentiels uniquement, que les personnes autorisées à avoir accès au routeur ou à l'EPRIS, selon le cas, n'ont accès qu'aux données couvertes par leur autorisation d'accès;
 - 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 ou l'EPRIS, selon le cas, à quel moment, par qui et dans quel but elles ont été traitées;
- j) d'empêcher toute lecture, copie, modification ou tout effacement non autorisés de données à caractère personnel pendant leur transmission à partir du routeur ou de l'EPRIS, selon le cas, 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 ou de l'EPRIS, selon le cas, 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.

Les mesures nécessaires visées au premier alinéa comprennent un plan de sécurité, un plan de continuité des activités et un plan de rétablissement après sinistre.

Article 54

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 des dommages ou des pertes aux données qui sont stockées dans le routeur ou dans l'EPRIS 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. En cas d'incident de sécurité concernant le routeur, l'eu-LISA et les États membres concernés ou, selon le cas, Europol coopèrent entre eux afin d'assurer une réaction rapide, efficace et adéquate.
3. En cas d'incident de sécurité concernant l'EPRIS, les États membres concernés et Europol coopèrent entre eux afin d'assurer une réaction rapide, efficace et adéquate.
4. Les États membres notifient à leurs autorités compétentes tout incident de sécurité sans retard injustifié.

Sans préjudice de l'article 92 du règlement (UE) 2018/1725, en cas d'incident de sécurité lié à l'infrastructure centrale du routeur, l'eu-LISA notifie au service de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE) les menaces informatiques importantes, les vulnérabilités importantes et les incidents importants sans retard injustifié 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 au CERT-UE sans retard injustifié.

Sans préjudice de l'article 34 du règlement (UE) 2016/794 et de l'article 92 du règlement (UE) 2018/1725, en cas d'incident de sécurité lié à l'infrastructure centrale de l'EPRIS, Europol notifie au CERT-UE les menaces informatiques importantes, les vulnérabilités importantes et les incidents importants sans retard injustifié 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 au CERT-UE sans retard injustifié.

5. 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 tarder 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.

6. 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 tarder 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 55

Autocontrôle

1. Les États membres veillent à ce que chaque autorité habilitée à utiliser le cadre Prüm II prenne les mesures nécessaires afin de contrôler qu'elle respecte le présent règlement et coopère, au besoin, avec l'autorité de contrôle. Europol prend les mesures nécessaires pour contrôler qu'elle respecte le présent règlement et coopère, le cas échéant, avec le Contrôleur européen de la protection des données.
2. Les responsables du traitement mettent en œuvre les mesures nécessaires afin de contrôler efficacement la conformité des opérations de traitement des données au présent règlement, y compris en vérifiant fréquemment les registres visés aux articles 18, 40 et 45. Ils coopèrent, au besoin et comme il convient, avec les autorités de contrôle ou avec le Contrôleur européen de la protection des données.

Article 56

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 57

Responsabilité

Si le non-respect, par un État membre ou par Europol lorsqu'il effectue des interrogations conformément à l'article 49, des obligations qui leur incombent au titre du présent règlement cause un dommage au routeur ou à l'EPRIS, cet État membre ou Europol 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 58

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. L'eu-LISA et Europol ont la possibilité de formuler des observations avant l'adoption des rapports.

2. L'eu-LISA et Europol transmettent 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. Le présent paragraphe est sans préjudice des pouvoirs dévolus au Contrôleur européen de la protection des données au titre de l'article 58 du règlement (UE) 2018/1725 et, en ce qui concerne Europol, au titre de l'article 43, paragraphe 3, du règlement (UE) 2016/794.

Article 59

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 pour assurer 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 cadre 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. Deux ans après l'entrée en service du router et de l'EPRIS et tous les deux ans par la suite, le comité européen de la protection des données envoie un rapport d'activités, au titre du présent article, au Parlement européen, au Conseil, à la Commission, à l'eu-LISA et à Europol. Ce rapport comporte un chapitre sur chaque État membre, établi par l'autorité de contrôle de l'État membre concerné.

Article 60

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

Un État membre ne transfère à un pays tiers ou à une organisation internationale les données à caractère personnel obtenues au titre du présent règlement que conformément au chapitre V de la directive (UE) 2016/680 et lorsque l'État membre requis a accordé son autorisation avant le transfert.

Europol ne transfère à un pays tiers ou à une organisation internationale les données à caractère personnel obtenues au titre du présent règlement que lorsque les conditions énoncées à l'article 25 du règlement (UE) 2016/794 sont remplies et lorsque l'État membre requis a accordé son autorisation avant le transfert.

Article 61

Rapport avec d'autres actes juridiques relatifs à la protection des données

Tout traitement de données à caractère personnel aux fins du présent règlement est effectué conformément au présent chapitre et à la directive (UE) 2016/680 ou au règlement (UE) 2018/1725, (UE) 2016/794 ou (UE) 2016/679, selon le cas.

Chapitre 7

Responsabilités

Article 62

Responsabilités en matière de devoir de diligence

Les États membres et Europol font preuve de la diligence requise lorsqu'ils évaluent si l'échange automatisé de données relève de l'objectif du cadre Prüm II énoncé à l'article 2 et s'il respecte les conditions qui y sont énoncées, en particulier en ce qui concerne le respect des droits fondamentaux.

Article 63

Formation

Le personnel dûment autorisé des autorités compétentes des États membres, des autorités de contrôle et d'Europol bénéficie, le cas échéant, de ressources et d'une formation adéquates, notamment en matière de protection des données et d'examen précis des concordances, pour s'acquitter des tâches prévues par le présent règlement.

Article 64

Responsabilités des États membres

1. Chaque État membre est responsable:
 - a) de la connexion à l'infrastructure du routeur;

- b) de l'intégration de ses 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 de ses 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 de l'accès et des modalités d'accès au routeur du personnel dûment autorisé de ses autorités 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 de l'accès et des modalités d'accès à l'EPRIS du personnel dûment autorisé de ses autorités 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 de l'accès et des modalités d'accès à Eucaris du personnel dûment autorisé de ses autorités 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, exécutée par du personnel qualifié, d'une concordance telle qu'elle est visée à l'article 6, paragraphe 6, à l'article 6, paragraphe 7, à l'article 11, paragraphe 2, et à l'article 20, paragraphe 2;

- k) de la disponibilité des données nécessaires à l'échange de données, conformément aux articles 5, 10, 16, 19 et 25;
 - l) de l'échange d'informations, conformément aux articles 6, 11, 16, 20 et 26;
 - m) de la correction, de la mise à jour ou de la suppression de toute donnée reçue d'un État membre requis dans les 48 heures à compter de la notification par l'État membre requis que les données transmises étaient inexactes, ne sont plus à jour ou ont été transmises de manière illicite;
 - n) du respect des exigences en matière de qualité des données énoncées dans le présent règlement.
2. Chaque État membre est chargé de connecter ses autorités compétentes au routeur, à l'EPRIS et à Eucaris.

Article 65

Responsabilités d'Europol

1. Europol est responsable de la gestion de l'accès et des modalités d'accès au routeur, à l'EPRIS et à Eucaris de son personnel dûment autorisé, conformément au présent règlement.
2. Europol est responsable du traitement des interrogations 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 l'infrastructure d'Europol nécessaire à l'établissement de la connexion au routeur et à Eucaris.

4. Sans préjudice des consultations effectuées par Europol en vertu de l'article 49, Europol n'a accès à aucune des données à caractère personnel traitées par l'intermédiaire de l'EPRIS.
5. 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 est responsable de la gestion technique de l'EPRIS. La gestion technique de l'EPRIS comprend toutes les tâches et solutions techniques nécessaires au fonctionnement continu de l'infrastructure centrale de l'EPRIS et à 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 soumettre des demandes aux bases de données nationales, conformément aux spécifications techniques.

6. Europol assure la formation à l'utilisation technique de l'EPRIS.
7. Europol est responsable des procédures prévues aux articles 48 et 49.

Article 66

Responsabilités de 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 67, paragraphe 1.
3. L'eu-LISA est responsable du développement du routeur et de toute adaptation technique nécessaire au fonctionnement du routeur.
4. L'eu-LISA n'a accès à aucune des données à caractère personnel traitées par l'intermédiaire du routeur.
5. L'eu-LISA définit la conception de l'architecture physique du routeur, y compris de son infrastructure de communication sécurisée, ainsi que les spécifications techniques et son évolution en ce qui concerne l'infrastructure centrale et l'infrastructure de communication sécurisée. Le conseil d'administration de l'eu-LISA approuve la conception, 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.
6. 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. Ce 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.
7. Au cours de la phase de conception et de développement, le conseil de gestion du programme 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 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 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 sur l'interopérabilité visé à l'article 78 se réunit régulièrement jusqu'à la mise en service du routeur. Après chaque réunion, il rend compte au comité de gestion du programme. Il fournit l'expertise technique nécessaire à l'appui des tâches du conseil de gestion du programme et suit l'état de préparation des États membres.

Article 67

Responsabilités de 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 continu du routeur et à 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 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) n° 259/68 du Conseil¹⁸, 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 le routeur. 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.

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

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

¹⁸ JO L 56 du 4.3.1968, p. 1.

Chapitre 8

Modifications d'autres instruments existants

Article 68

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

1. Dans la décision 2008/615/JAI, l'article 1^{er}, point a), les articles 2 à 6 et les sections 2 et 3 du chapitre 2 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 énoncées à l'article 75, paragraphe 1. Par conséquent, l'article 1^{er}, point a), 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 énoncées à l'article 75, paragraphe 1.
2. Dans la décision 2008/616/JAI, les chapitres 2 à 5 et les articles 18, 20 et 21 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 énoncées à l'article 75, paragraphe 1. 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 énoncées à l'article 75, paragraphe 1.

Article 69

Modifications apportées au règlement (UE) 2018/1726

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

- 1) L'article suivant est inséré:

"Article 8 quinquies

Tâches liées au routeur Prüm II

En ce qui concerne le routeur Prüm II, l'Agence s'acquitte des tâches qui lui sont confiées par le règlement (UE) 2024/... du Parlement européen et du Conseil*+.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... relatif à la consultation et l'échange automatisés de données dans le cadre de la coopération policière, et modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, (UE) 2019/817 et (UE) 2019/818 du Parlement européen et du Conseil (règlement Prüm II) (JO L, ..., ELI: ...)."

- 2) À l'article 17, paragraphe 3, le deuxième alinéa est remplacé par le texte suivant:

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

+ JO: veuillez insérer, dans le corps du texte, le numéro du règlement qui figure dans le document PE-CONS 75/23 (2021/0410 (COD)) et insérer dans la note de bas de page le numéro, la date, le titre et la référence au JO dudit règlement.

3) À l'article 19, le paragraphe 1 est modifié comme suit:

a) le point suivant est inséré:

"*ee ter*) adopte les rapports sur l'état d'avancement du développement du routeur Prüm II en vertu de l'article 80, paragraphe 2, du règlement (UE) .../...⁺";

b) le point ff) est remplacé par le texte suivant:

"ff) adopte les rapports sur le fonctionnement technique de ce qui suit:

- i) le SIS conformément à l'article 60, paragraphe 7, du règlement (UE) 2018/1861 du Parlement européen et du Conseil* et à l'article 74, paragraphe 8, du règlement (UE) 2018/1862 du Parlement européen et du Conseil**;
- ii) le VIS conformément à l'article 50, paragraphe 3, du règlement (CE) n° 767/2008 et à l'article 17, paragraphe 3, de la décision 2008/633/JAI;
- iii) l'EES conformément à l'article 72, paragraphe 4, du règlement (UE) 2017/2226;
- iv) ETIAS conformément à l'article 92, paragraphe 4, du règlement (UE) 2018/1240;
- v) l'ECRIS-TCN et l'application de référence de l'ECRIS conformément à l'article 36, paragraphe 8, du règlement (UE) 2019/816;

⁺ JO: veuillez insérer, dans le corps du texte, le numéro du règlement qui figure dans le document PE-CONS 75/23 (2021/0410 (COD)).

- vi) les éléments d'interopérabilité conformément à l'article 78, paragraphe 3, du règlement (UE) 2019/817 et de l'article 74, paragraphe 3, du règlement (UE) 2019/818;
- vii) le système e-CODEX conformément à l'article 16, paragraphe 1, du règlement (UE) 2022/850;
- viii) la plateforme de collaboration des ECE conformément à l'article 26, paragraphe 6, du règlement (UE) 2023/969;
- ix) le routeur Prüm II conformément à l'article 80, paragraphe 5, du règlement (UE) .../...⁺;

* Règlement (UE) 2018/1861 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 des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 (JO L 312 du 7.12.2018, p. 14).

** 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) n° 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).";

⁺ JO: veuillez insérer, dans le corps du texte, le numéro du règlement qui figure dans le document PE-CONS 75/23 (2021/0410 (COD)).

c) le point hh) est remplacé par le texte suivant:

"hh) adopte des observations formelles sur les rapports du Contrôleur européen de la protection des données relatifs à ses audits effectués conformément à l'article 56, paragraphe 2, du règlement (UE) 2018/1861, à l'article 42, paragraphe 2, du règlement (CE) n° 767/2008, à l'article 31, paragraphe 2, du règlement (UE) n° 603/2013, à l'article 56, paragraphe 2, du règlement (UE) 2017/2226, à l'article 67 du règlement (UE) 2018/1240, à l'article 29, paragraphe 2, du règlement (UE) 2019/816, à l'article 52 des règlements (UE) 2019/817 et (UE) 2019/818, et à l'article 58, paragraphe 1 du règlement (UE) .../...⁺ et veille à ce qu'il soit dûment donné suite à ces audits;"

⁺ JO: veuillez insérer, dans le corps du texte, le numéro du règlement qui figure dans le document PE-CONS 75/23 (2021/0410 (COD)).

Article 70

Modification apportée au règlement (UE) 2019/817

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

- "d) une infrastructure de communication sécurisée entre l'ESP et le routeur établie par le règlement (UE) 2024/... du Parlement européen et du Conseil**.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... relatif à la consultation et l'échange automatisés de données dans le cadre de la coopération policière, et modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, (UE) 2019/817 et (UE) 2019/818 du Parlement européen et du Conseil (règlement Prüm II) (JO L, ..., ELI: ...)."

+ JO: veuillez insérer, dans le corps du texte, le numéro du règlement qui figure dans le document PE-CONS 75/23 (2021/0410 (COD)) et insérer dans la note de bas de page le numéro, la date, le titre et la référence au JO dudit règlement.

Article 71

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 suivant est ajouté:

"d) une infrastructure de communication sécurisée entre l'ESP et le routeur établie par le règlement (UE) 2024/... du Parlement européen et du Conseil*+.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... relatif à la consultation et l'échange automatisés de données dans le cadre de la coopération policière, et modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, (UE) 2019/817 et (UE) 2019/818 du Parlement européen et du Conseil ("règlement Prüm II") (JO L, ..., ELI: ...)."

+ JO: veuillez insérer, dans le corps du texte, le numéro du règlement qui figure dans le document PE-CONS 75/23 (2021/0410 (COD)) et insérer dans la note de bas de page le numéro, la date, le titre et la référence au JO dudit règlement.

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 règlement (UE) .../...⁺.
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 le système d'information de l'UE. L'eu-LISA collecte également les données et les statistiques provenant du routeur visé à l'article 72, paragraphe 1, du règlement (UE) .../...⁺. 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 72, paragraphe 1, du règlement (UE) .../...⁺."

⁺ JO: veuillez insérer, dans le corps du texte, le numéro du règlement qui figure dans le document PE-CONS 75/23 (2021/0410 (COD)).

Chapitre 9

Dispositions finales

Article 72

Établissement de rapports et de statistiques

1. Lorsque cela est nécessaire, le personnel dûment autorisé des autorités compétentes des États membres, de la Commission, de l'eu-LISA et d'Europol a accès aux données énumérées ci-après concernant le routeur, uniquement aux fins de l'établissement de rapports et de statistiques:
 - a) le nombre d'interrogations par État membre et le nombre d'interrogations effectuées par Europol par catégorie de données;
 - b) le nombre d'interrogations dans chacune des bases de données connectées;
 - c) le nombre de concordances par rapport à la base de données de chaque État membre par catégorie de données;
 - d) le nombre de concordances par rapport aux données d'Europol par catégorie de données;
 - e) le nombre de concordances confirmées lorsqu'il y a eu des échanges de données de base;
 - f) le nombre de concordances confirmées lorsqu'il n'y a pas eu d'échanges de données de base;
 - g) le nombre d'interrogations dans le répertoire commun de données d'identité par l'intermédiaire du routeur; et

- h) le nombre de concordances par type comme suit:
 - i) données identifiées (personne) – données non identifiées (trace);
 - ii) données non identifiées (trace) – données identifiées (personne);
 - iii) données non identifiées (trace) – données non identifiées (trace);
 - iv) données identifiées (personne) – données identifiées (personne).

Il ne doit pas être possible d'identifier des personnes à partir des données énoncées au premier alinéa.

- 2. Le personnel dûment autorisé des autorités compétentes des États membres, de la Commission et d'Europol a accès aux données énumérées ci-après concernant Eucaris, uniquement aux fins de l'établissement de rapports et de statistiques:
 - a) le nombre d'interrogations par État membre et le nombre d'interrogations effectuées par Europol;
 - b) le nombre d'interrogations dans chacune des bases de données connectées; et
 - c) le nombre de concordances par rapport à la base de données de chaque État membre.

Il ne doit pas être possible d'identifier des personnes à partir des données énoncées au premier alinéa.

3. Le personnel dûment autorisé des autorités compétentes des États membres, de la Commission et d'Europol a accès aux données énumérées ci-après concernant l'EPRIS, uniquement aux fins de l'établissement de rapports et de statistiques:
 - a) le nombre d'interrogations par État membre et le nombre d'interrogations effectuées par Europol;
 - b) le nombre d'interrogations lancées sur chacun des index connectés; et
 - c) le nombre de concordances par rapport à la base de données de chaque État membre.

Il ne doit pas être possible d'identifier des personnes à partir des données énoncées au premier alinéa.

4. L'eu-LISA stocke les données énoncées au paragraphe 1 du présent article dans le répertoire central des rapports et statistiques établi par l'article 39 du règlement (UE) 2019/818. Europol stocke les données énoncées au paragraphe 3. Ces données permettent aux autorités compétentes des États membres, à la Commission, à l'eu-LISA et à Europol d'obtenir des rapports et des statistiques personnalisables afin de renforcer l'efficacité de la coopération en matière répressive.

Article 73

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 des fichiers de 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 afférents à ce qui suit ne sont pas admissibles:

- a) au bureau de gestion de projets des États membres (réunions, missions, locaux);
 - b) à l'hébergement des systèmes d'information nationaux (espace, mise en œuvre, électricité, refroidissement);
 - c) au fonctionnement des systèmes d'information nationaux (contrats conclus avec les opérateurs et contrats d'appui);
 - d) 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 d'Eucaris.
 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 74
Notifications

1. Les États membres notifient à l'eu-LISA le nom des autorités compétentes visées à l'article 36. Ces autorités peuvent utiliser le routeur ou y avoir accès.
2. L'eu-LISA notifie à la Commission les résultats concluants de l'essai visé à l'article 75, paragraphe 1, point b).
3. Europol notifie à la Commission les résultats concluants de l'essai visé à l'article 75, paragraphe 3, point b).
4. Chaque État membre notifie aux autres États membres, à la Commission, à l'eu-LISA et à Europol le contenu de ses bases de données ADN nationales et les conditions applicables aux consultations automatisées auxquelles s'appliquent les articles 5 et 6.
5. Chaque État membre informe les autres États membres, la Commission, l'eu-LISA et Europol du contenu de ses bases de données dactyloscopiques nationales et des conditions applicables aux consultations automatisées auxquelles s'appliquent les articles 10 et 11.
6. Chaque État membre informe les autres États membres, la Commission, l'eu-LISA et Europol du contenu de ses bases de données d'images faciales nationales et des conditions applicables aux consultations automatisées auxquelles s'appliquent les articles 19 et 20.

7. Chaque État membre qui participe à des échanges automatisés de fichiers de police en vertu des articles 25 et 26 notifie aux autres États membres, à la Commission et à Europol le contenu de ses index nationaux des fichiers de police et des bases de données nationales utilisées pour l'établissement de ces index et les conditions applicables aux consultations automatisées.
8. Les États membres notifient à la Commission, à l'eu-LISA et à Europol les noms de leurs points de contact nationaux désignés en vertu de l'article 30. La Commission dresse une liste des points de contact nationaux dont les noms lui ont été notifiés et met cette liste à la disposition de tous les États membres.

Article 75

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 Europol peuvent commencer à utiliser le routeur, dès que les conditions suivantes sont remplies:
 - a) les mesures prévues à l'article 5, paragraphe 3, à l'article 8, paragraphes 2 et 3, à l'article 13, paragraphes 2 et 3, à l'article 17, paragraphe 3, à l'article 22, paragraphes 2 et 3, à l'article 31 et à l'article 37, paragraphe 6, ont été adoptées;
 - b) l'eu-LISA a déclaré que l'essai complet du routeur qu'elle a mené en coopération avec les autorités compétentes des États membres et Europol a été concluant.

La Commission fixe, par la voie de l'acte d'exécution visé au premier alinéa, la date à compter de laquelle les États membres et Europol 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 Europol 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.

2. Les États membres veillent, deux ans après la mise en service du routeur, à la disponibilité des images faciales visées à l'article 19, aux fins de la consultation automatisée d'images faciales visée à l'article 20.
3. La Commission fixe, par la voie d'un acte d'exécution, la date à compter de laquelle les États membres et Europol doivent commencer à utiliser l'EPRIS, dès que les conditions suivantes sont remplies:
 - a) les mesures visées à l'article 44, paragraphe 6, ont été adoptées;
 - b) Europol a déclaré que l'essai complet de l'EPRIS qu'elle a mené en coopération avec les autorités compétentes des États membres a été concluant.

4. 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 48, dès que les conditions suivantes sont remplies:
 - a) le routeur est en service;
 - b) Europol a déclaré que l'essai complet de sa connexion au routeur qu'elle a mené en coopération avec les autorités compétentes des États membres et l'eu-LISA a été concluant.
5. 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 49, dès que les conditions suivantes sont remplies:
 - a) le routeur est en service;
 - b) Europol a déclaré que l'essai complet de la connexion au routeur qu'elle a mené en coopération avec les autorités compétentes des États membres et l'eu-LISA a été concluant.
6. Les actes d'exécution visés au présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 77, paragraphe 2.

Article 76

Dispositions transitoires et dérogations

1. Les États membres et les agences de l'Union commencent à appliquer les articles 19 à 22, l'article 47 et l'article 49, paragraphe 6, à compter de la date fixée conformément à l'article 75, 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 49, paragraphe 4, à compter de la date fixée conformément à l'article 75, paragraphe 3.
3. Les États membres et les agences de l'Union commencent à appliquer l'article 48 à compter de la date fixée conformément à l'article 75, paragraphe 4.
4. Les États membres et les agences de l'Union commencent à appliquer l'article 49, paragraphes 1, 2, 3, 5 et 7, à compter de la date fixée conformément à l'article 75, paragraphe 5.

Article 77

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 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) n° 182/2011 s'applique.

Article 78

Groupe consultatif sur l'interopérabilité

Les responsabilités du groupe consultatif sur l'interopérabilité, institué par l'article 75 du règlement (UE) 2019/817 et l'article 71 du règlement (UE) 2019/818, 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 79

Manuel pratique

La Commission, en étroite coopération avec les États membres, l'eu-LISA, Europol, et l'Agence européenne des droits fondamentaux, 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 avant la mise en service du routeur et de l'EPRIS. La Commission actualise régulièrement le manuel pratique, et chaque fois que c'est nécessaire.

Article 80

Suivi et évaluation

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

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

2. Au plus tard le ... [*un an après la date d'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. Ces rapports contiennent 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 en vertu de l'article 73.

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 atteints, et qui justifie les éventuels écarts.

3. Au plus tard le ... [*un an après la date d'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 d'avancement du développement de l'EPRIS. Ces rapports contiennent 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 en vertu de l'article 73.

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 atteints, et qui justifie les éventuels écarts.

4. Aux fins de la maintenance technique, l'eu-LISA a accès aux informations nécessaires concernant les opérations de traitement de données effectuées dans le routeur. Aux fins de la maintenance technique, Europol a accès aux informations nécessaires concernant les opérations de traitement de données effectuées dans l'EPRIS.
5. Deux ans après la mise en service du routeur, puis tous les deux ans, 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, 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 conformément à l'article 75, puis tous les quatre ans, la Commission élabore un rapport sur l'évaluation globale du cadre Prüm II.

Un an après la mise en service du routeur, puis tous les deux ans, la Commission élabore un rapport évaluant l'utilisation des images faciales au titre du présent règlement.

Les rapports visés au premier et deuxième alinéas comprennent:

- a) une évaluation de l'application du présent règlement, notamment de son utilisation par chaque État membre et par Europol;
- 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 cadre 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 cadre Prüm II.

La Commission transmet ces rapports 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. Dans les rapports visés au premier alinéa du paragraphe 7, la Commission accorde une attention particulière aux nouvelles catégories de données suivantes: images faciales et fichiers de police. La Commission inclut dans ces rapports l'utilisation faite par chaque État membre et par Europol de ces nouvelles catégories de données, ainsi que leur incidence, leur efficacité et leur efficience. Dans les rapports visés au deuxième alinéa du paragraphe 7, la Commission accorde une attention particulière au risque de fausses concordances et à la qualité des données.
9. Les États membres et Europol fournissent 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 révéler les sources, les membres du personnel ou les enquêtes des autorités compétentes des États membres.
10. Les États membres fournissent à la Commission et à Europol 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 révéler les sources, les membres du personnel ou les enquêtes des autorités compétentes des États membres.
11. Sans préjudice des exigences de confidentialité, les États membres, l'eu-LISA et Europol fournissent à la Commission les informations nécessaires à la réalisation des rapports visés au paragraphe 7. Les États membres communiquent également à la Commission le nombre de concordances confirmées par rapport à la base de données de chaque État membre par catégorie et par type de données. Ces informations ne peuvent porter préjudice aux méthodes de travail ni révéler les sources, les membres du personnel ou les enquêtes des autorités compétentes des États membres.

Article 81

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 Strasbourg, le

Par le Parlement européen

La présidente

Par le Conseil

Le président / La présidente