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

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 74, son article 78, paragraphe 2, point e), son article 79, paragraphe 2, point c), son article 82, paragraphe 1, point d), son article 85, paragraphe 1, son article 87, paragraphe 2, point a), et son article 88, paragraphe 2,

vu la proposition de la Commission européenne,

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

vu l'avis du Comité économique et social européen [1],

après consultation du Comité des régions,

statuant conformément à la procédure législative ordinaire [2],

considérant ce qui suit:

(1) Dans sa communication du 6 avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», la Commission a souligné la nécessité d'améliorer l'architecture de la gestion des données de l'Union appliquée à la gestion des frontières et à la sécurité. La communication a lancé un processus visant à atteindre l'interopérabilité des systèmes d'information de l'UE pour la sécurité, les frontières et la gestion des migrations, dans le but de remédier aux lacunes structurelles de ces systèmes qui ralentissent le travail des autorités nationales et de garantir que les garde-frontières, les autorités douanières, les policiers et les autorités judiciaires disposent des informations dont ils ont besoin.

(2) Dans sa feuille de route en vue de renforcer l'échange d'informations et la gestion de l'information, y compris des solutions d'interopérabilité, dans le domaine de la justice et des affaires intérieures, du 6 juin 2016, le Conseil a recensé plusieurs défis juridiques, techniques et opérationnels en matière d'interopérabilité des systèmes d'information de l'UE et a invité à rechercher des solutions.

(3) Dans sa résolution du 6 juillet 2016 sur les priorités stratégiques pour le programme de

travail de la Commission pour 2017 ([3]), le Parlement européen a invité à présenter des propositions visant à améliorer et à développer les systèmes d'information de l'UE existants, à combler les lacunes en matière d'informations et à progresser vers l'interopérabilité, ainsi que des propositions concernant l'échange obligatoire d'informations au niveau de l'Union, assorti des garanties nécessaires en matière de protection des données.

(4) Dans ses conclusions du 15 décembre 2016, le Conseil européen a appelé à poursuivre les efforts en matière d'interopérabilité des systèmes d'information et des bases de données de l'UE.

(5) Dans son rapport final du 11 mai 2017, le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité a conclu qu'il était nécessaire et techniquement faisable d'œuvrer à des solutions pratiques d'interopérabilité et que l'interopérabilité pouvait, en principe, apporter des bénéfices opérationnels et être mise en place conformément aux exigences en matière de protection des données.

(6) Dans sa communication du 16 mai 2017 intitulée «Septième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective», la Commission a défini, conformément à sa communication du 6 avril 2016 et aux conclusions et recommandations du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité, une nouvelle approche de la gestion des données pour les frontières, la sécurité et les migrations, selon laquelle tous les systèmes d'information de l'UE pour la sécurité, les frontières et la gestion des migrations devaient être interopérables, d'une manière qui respecte pleinement des droits fondamentaux.

(7) Dans ses conclusions du 9 juin 2017 concernant la voie à suivre pour améliorer l'échange d'informations et assurer l'interopérabilité des systèmes d'information de l'UE, le Conseil a invité la Commission à poursuivre les solutions d'interopérabilité proposées par le groupe d'experts de haut niveau.

(8) Dans ses conclusions du 23 juin 2017, le Conseil européen a souligné la nécessité d'améliorer l'interopérabilité des bases de données et a invité la Commission à préparer, dès que possible, un projet de texte législatif sur la base des propositions formulées par le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité.

(9) Dans le but d'améliorer l'efficacité et l'efficience des vérifications aux frontières extérieures, de contribuer à prévenir et combattre l'immigration illégale et de favoriser un niveau élevé de sécurité au sein de l'espace de liberté, de sécurité et de justice de l'Union, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres, d'améliorer la mise en œuvre de la politique commune des visas, d'aider dans l'examen des demandes de protection internationale, de contribuer à la prévention et à la détection des infractions terroristes et d'autres infractions pénales graves et aux enquêtes en la matière, de faciliter l'identification de personnes inconnues qui ne sont pas en mesure de s'identifier elles-mêmes ou des restes humains non identifiés en cas de catastrophe naturelle, d'accident ou d'attaque terroriste, afin de préserver la confiance des citoyens à l'égard du régime d'asile et de migration de l'Union, des mesures de sécurité de l'Union et de la capacité de l'Union à gérer les frontières

extérieures, il convient d'établir l'interopérabilité des systèmes d'information de l'UE, à savoir le système d'entrée/de sortie (EES), le système d'information sur les visas (VIS), le système européen d'information et d'autorisation concernant les voyages (ETIAS), Eurodac, le système d'information Schengen (SIS) et le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN), afin que lesdits systèmes d'information de l'UE et leurs données se complètent mutuellement, tout en respectant les droits fondamentaux des personnes, en particulier le droit à la protection des données à caractère personnel. À cet effet, il convient de créer un portail de recherche européen (ESP), un service partagé d'établissement de correspondances biométriques (BMS partagé), un répertoire commun de données d'identité (CIR) et un détecteur d'identités multiples (MID) en tant qu'éléments d'interopérabilité.

(10) L'interopérabilité des systèmes d'information de l'UE devrait permettre auxdits systèmes de se compléter mutuellement afin de faciliter l'identification correcte des personnes, y compris de personnes inconnues qui ne sont pas en mesure de s'identifier elles-mêmes ou de restes humains non identifiés, de contribuer à la lutte contre la fraude à l'identité, d'améliorer et d'harmoniser les exigences en matière de qualité des données des différents systèmes d'information de l'UE, de faciliter la mise en œuvre technique et opérationnelle par les États membres des systèmes d'information de l'UE, de renforcer les garanties en matière de sécurité des données et de protection des données régissant les différents systèmes d'information de l'UE, de rationaliser l'accès aux fins de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière, à l'EES, au VIS, à ETIAS et à Eurodac et de servir les objectifs de l'EES, du VIS, d'ETIAS, d'Eurodac, du SIS et de l'ECRIS-TCN.

(11) Les éléments d'interopérabilité devraient concerner l'EES, le VIS, ETIAS, Eurodac, le SIS et l'ECRIS-TCN. Ils devraient également concerner les données d'Europol, mais uniquement dans la mesure nécessaire pour permettre que les données d'Europol puissent être interrogées en même temps que ces systèmes d'information de l'UE.

(12) Les éléments d'interopérabilité devraient traiter les données à caractère personnel des personnes dont les données à caractère personnel sont traitées dans les systèmes d'information de l'UE sous-jacents et par Europol,

(13) L'ESP devrait être créé afin de faciliter d'un point de vue technique l'accès rapide, continu, efficace, systématique et contrôlé des autorités des États membres et des agences de l'Union aux systèmes d'information de l'UE, aux données d'Europol et aux bases de données de l'Organisation internationale de police criminelle (Interpol), dans la mesure où cela est nécessaire à l'accomplissement de leurs tâches conformément à leurs droits d'accès. L'ESP devrait être créé pour soutenir les objectifs de l'EES, du VIS, d'ETIAS, d'Eurodac, du SIS, de l'ECRIS-TCN et d'Europol. En permettant d'interroger l'ensemble des systèmes d'information pertinents de l'UE, les données d'Europol et les bases de données d'Interpol en parallèle, l'ESP devrait constituer un guichet unique ou «courtier de messages» afin d'effectuer des recherches dans plusieurs systèmes centraux et de récupérer les informations nécessaires sans discontinuité et dans le plein respect des exigences en matière de contrôle de l'accès et de protection des données des systèmes sous-jacents.

(14)La conception de l'ESP devrait garantir que, lors de l'interrogation des bases de données d'Interpol, les données employées par un utilisateur de l'ESP pour lancer une requête ne sont pas partagées avec les propriétaires des données d'Interpol. La conception de l'ESP devrait également garantir que les bases de données d'Interpol sont seulement interrogées conformément au droit de l'Union et au droit national applicables.

(15)Les utilisateurs de l'ESP qui ont le droit d'accéder aux données d'Europol en vertu du règlement (UE) 2016/794 du Parlement européen et du Conseil [4] devraient pouvoir interroger les données d'Europol en même temps que les systèmes d'information de l'UE auxquels ils ont accès. Tout traitement ultérieur de données faisant suite à une telle interrogation devrait avoir lieu conformément au règlement (UE) 2016/794, y compris les limitations d'accès ou d'utilisation imposées par le fournisseur de données.

(16)L'ESP devrait être développé et configuré de telle sorte qu'il ne permette pas de procéder à de telles interrogations qu'en utilisant des données liées aux personnes ou aux documents de voyage figurant dans un système d'information de l'UE, dans les données d'Europol ou dans les bases de données d'Interpol.

(17)Afin d'assurer l'utilisation systématique des systèmes d'information de l'UE pertinents, l'ESP devrait être utilisé pour interroger le CIR, l'EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN. Toutefois, une connexion nationale aux différents systèmes d'information de l'UE devrait être conservée en tant que solution de secours technique. Les agences de l'Union devraient également utiliser l'ESP afin d'interroger le SIS central, conformément à leurs droits d'accès et afin d'exécuter leurs missions. L'ESP devrait constituer un moyen supplémentaire d'interroger le SIS central, les données d'Europol et les bases de données d'Interpol, en complément des interfaces spécifiques existantes.

(18)Les données biométriques, telles que les empreintes digitales et les images faciales, sont uniques et donc bien plus fiables que les données alphanumériques aux fins de l'identification d'une personne. Le BMS partagé devrait être un outil technique permettant de renforcer et de faciliter le fonctionnement des systèmes d'information de l'UE pertinents et des autres éléments d'interopérabilité. L'objectif principal du BMS partagé devrait être de faciliter l'identification d'une personne qui est enregistrée dans plusieurs bases de données, en utilisant un élément technologique unique pour faire correspondre les données biométriques de cette personne contenues dans différents systèmes plutôt que plusieurs éléments. Le BMS partagé devrait contribuer à la sécurité et procurer des avantages sur les plans financier, opérationnel et de la maintenance. Tous les systèmes automatisés d'identification par empreintes digitales, y compris ceux actuellement utilisés pour Eurodac, le VIS et le SIS, utilisent des modèles biométriques constitués de données résultant d'une extraction des caractéristiques d'échantillons biométriques réels. Le BMS partagé devrait regrouper et stocker tous ces modèles biométriques – séparés logiquement en fonction du système d'information d'où les données proviennent – à un seul endroit, facilitant ainsi les comparaisons de modèles biométriques entre les systèmes et permettant des économies d'échelle dans le développement et la maintenance des systèmes centraux de l'UE.

(19)Les modèles biométriques stockés dans le BMS partagé devraient être constitués de

données résultant d'une extraction des caractéristiques d'échantillons biométriques réels et obtenus de telle manière qu'il ne soit pas possible d'inverser le processus d'extraction. 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. Étant donné que les données sous la forme d'empreintes palmaires et les profils ADN ne sont stockés que dans le SIS et ne peuvent pas être utilisés pour être recoupés avec des données contenues dans d'autres systèmes d'information, en suivant les principes de nécessité et de proportionnalité, le BMS partagé ne devrait pas stocker de profils ADN ou de modèles biométriques obtenus à partir de données sous la forme d'empreintes palmaires.

(20) Les données biométriques sont des données à caractère personnel sensibles. Le présent règlement devrait fixer la base et les garanties du traitement de ces données aux fins d'identifier de manière unique les personnes concernées.

(21) L'EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN nécessitent l'identification précise des personnes dont les données à caractère personnel sont stockées dans ces systèmes. Le CIR devrait donc faciliter l'identification correcte des personnes enregistrées dans ces systèmes.

(22) Les données à caractère personnel stockées dans ces systèmes d'information de l'UE peuvent concerner la même personne, mais sous des identités différentes ou incomplètes. Les États membres disposent de moyens efficaces d'identifier leurs citoyens ou les résidents permanents enregistrés sur leur territoire. L'interopérabilité des systèmes d'information de l'UE devrait contribuer à l'identification correcte des personnes figurant dans ces systèmes. Le CIR devrait stocker les données à caractère personnel qui sont nécessaires pour permettre l'identification plus précise des personnes dont les données sont stockées dans ces systèmes, notamment leurs données d'identité, les données de leur document de voyage et leurs données biométriques, quel que soit le système dans lequel ces informations ont été collectées à l'origine. Seules les données à caractère personnel strictement nécessaires pour procéder à un contrôle d'identité précis devraient être stockées dans le CIR. Les données à caractère personnel enregistrées dans le CIR ne devraient pas être conservées plus longtemps qu'il n'est strictement nécessaire aux fins des systèmes sous-jacents et elles devraient être automatiquement supprimées lorsque les données sont supprimées des systèmes sous-jacents conformément à leur séparation logique.

(23) Une nouvelle opération de traitement consistant à stocker ces données dans le CIR plutôt que dans chacun des systèmes distincts est nécessaire afin d'améliorer la précision de l'identification par la comparaison et la mise en correspondance automatisées des données. Le fait que les données d'identité, les données du document de voyage et les données biométriques soient stockées dans le CIR ne devrait en aucune façon faire obstacle au traitement des données pour les finalités de l'EES, du VIS, d'ETIAS, d'Eurodac ou de l'ECRIS-TCN, étant donné que le CIR devrait être un nouvel élément partagé de ces systèmes sous-jacents.

(24) Il est dès lors nécessaire de créer un dossier individuel dans le CIR pour chaque personne

enregistrée dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN, afin d'atteindre l'objectif consistant à identifier correctement les personnes au sein de l'espace Schengen et de soutenir le MID avec le double objectif de faciliter les contrôles d'identité pour les voyageurs de bonne foi et de lutter contre la fraude à l'identité. Le dossier individuel devrait stocker toutes les informations sur l'identité liées à une personne en un seul endroit et les mettre à la disposition des utilisateurs finaux dûment autorisés.

(25) Le CIR devrait donc faciliter et rationnaliser l'accès des autorités chargées de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière, aux systèmes d'information de l'UE qui ne sont pas exclusivement créés à des fins de prévention ou de détection des infractions graves, ou d'enquêtes en la matière.

(26) Le CIR devrait prévoir un réservoir partagé pour les données d'identité, les données du document de voyage et les données biométriques des personnes enregistrées dans l'EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN. Il devrait faire partie de l'architecture technique de ces systèmes et constituer l'élément partagé entre ceux-ci pour stocker et interroger les données d'identité, les données du document de voyage et les données biométriques qu'ils traitent.

(27) Tous les enregistrements dans le CIR devraient être séparés logiquement au moyen d'un étiquetage automatique de chaque enregistrement indiquant le nom système sous-jacent à qui elle appartient. Les contrôles de l'accès au CIR devraient utiliser ces étiquettes afin de déterminer s'il y a lieu de permettre l'accès ou non à l'enregistrement.

(28) Lorsque les services de police d'un État membre ne sont pas en mesure d'identifier une personne en raison de l'absence d'un document de voyage ou d'un autre document crédible prouvant l'identité de cette personne, ou lorsqu'un doute subsiste quant aux données d'identité fournies par cette personne ou quant à l'authenticité du document de voyage ou l'identité de son titulaire, ou lorsque la personne n'est pas en mesure ou refuse de coopérer, ces services de police devraient avoir la possibilité d'interroger le CIR afin d'identifier la personne en question. À cette fin, les services de police devraient relever les empreintes digitales en utilisant des techniques de numérisation directe d'empreintes digitales, à condition que la procédure ait été initiée en présence de cette personne. Ces interrogations du CIR ne devraient pas être autorisées aux fins de l'identification de mineurs de moins de 12 ans, à moins que ce ne soit dans l'intérêt supérieur de l'enfant.

(29) Lorsque les données biométriques d'une personne ne peuvent pas être utilisées ou si la requête introduite avec ces données échoue, cette dernière devrait être introduite à l'aide des données d'identité de la personne, combinées aux données du document de voyage. Lorsque le résultat de l'interrogation indique que des données concernant cette personne sont stockées dans le CIR, les autorités des États membres devraient avoir accès au CIR pour consulter les données d'identité et les données du document de voyage de cette personne, sans que le CIR ne fournisse d'indications quant au système d'information de l'UE auquel les données appartiennent.

(30) Les États membres devraient adopter des mesures législatives nationales désignant les autorités compétentes pour réaliser des contrôles d'identité à l'aide du CIR et définissant

les procédures, les conditions et les critères de ces contrôles, qui devraient suivre le principe de proportionnalité. En particulier, le droit national devrait prévoir le pouvoir de collecter des données biométriques lors d'un contrôle de l'identité d'une personne présente devant un membre du personnel de ces autorités.

(31) Le présent règlement devrait également introduire, pour les autorités désignées par les États membres chargées de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière et pour Europol, une nouvelle possibilité d'accès rationalisé aux données autres que les données d'identité ou les données du document de voyage contenues dans l'EES, le VIS, ETIAS ou Eurodac. Ces données peuvent être nécessaires à la prévention ou à la détection des infractions terroristes ou d'autres infractions pénales graves, ou aux enquêtes en la matière, lorsqu'il existe des motifs raisonnables permettant de penser que leur consultation contribuera à la prévention ou à la détection des infractions terroristes ou d'autres infractions pénales graves, ou aux enquêtes en la matière, en particulier lorsqu'il y a lieu de suspecter que la personne soupçonnée d'avoir commis une infraction terroriste ou une autre infraction pénale grave, l'auteur ou la victime d'une telle infraction est une personne dont les données sont stockées dans l'EES, le VIS, ETIAS ou Eurodac.

(32) L'accès complet aux données contenues dans les systèmes d'information de l'UE qui est nécessaire à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, en plus de l'accès aux données d'identité ou aux données du document de voyage contenues dans le CIR, devrait continuer à être régi par les instruments juridiques applicables. Les autorités désignées chargées de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière, et Europol ne savent pas à l'avance quels systèmes d'information de l'UE contiennent des données concernant les personnes sur lesquelles ils doivent enquêter. Cela conduit à des retards et à des manques d'efficacité. L'utilisateur final autorisé par l'autorité désignée devrait par conséquent pouvoir voir dans quels systèmes d'information de l'UE les données correspondant au résultat d'une requête sont enregistrées. Le système concerné serait donc signalé après la vérification automatisée de la présence d'une correspondance dans le système (fonctionnalité dite de l'indicateur de correspondance).

(33) Dans ce contexte, une réponse du CIR ne devrait pas être interprétée ni utilisée comme un motif ou une raison de tirer des conclusions au sujet d'une personne ou de prendre des mesures à l'égard de celle-ci mais elle ne devrait être utilisée qu'aux fins de l'introduction d'une demande d'accès aux systèmes d'information de l'UE sous-jacents, sous réserve des conditions et des procédures établies dans les différents instruments juridiques régissant l'accès en question. Une telle demande d'accès devrait être soumise au chapitre VII du présent règlement et, le cas échéant, au règlement (UE) 2016/679 du Parlement européen et du Conseil [5], à la directive (UE) 2016/680 du Parlement européen et du Conseil [6] ou au règlement (UE) 2018/1725 du Parlement européen et du Conseil [7].

(34) En règle générale, lorsqu'un indicateur de correspondance montre que les données sont enregistrées dans Eurodac, les autorités désignées ou Europol devraient demander un accès complet à au moins un des systèmes d'information de l'UE concernés. Si, à titre

exceptionnel, cet accès complet n'est pas demandé, par exemple parce que les autorités désignées ou Europol ont déjà obtenu les données par d'autres moyens, ou parce que l'obtention des données n'est plus autorisée par le droit national, il convient de consigner les raisons justifiant la décision de ne pas demander l'accès.

(35) Les registres des requêtes dans le CIR devraient indiquer l'objectif des requêtes. Lorsque la requête a été introduite selon l'approche de la consultation des données en deux étapes, les registres devraient comporter une référence au dossier national de l'enquête ou de l'affaire, en indiquant si la requête a été lancée à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière.

(36) L'interrogation du CIR par les autorités désignées et Europol en vue d'obtenir une réponse de type indicateur de correspondance, signalant que les données sont enregistrées dans l'EES, le VIS, ETIAS ou Eurodac, nécessite un traitement automatisé de données à caractère personnel. Un indicateur de correspondance ne devrait pas révéler les données à caractère personnel de la personne concernée mais devrait seulement indiquer que certaines de ses données sont stockées dans l'un des systèmes. L'utilisateur final autorisé ne devrait prendre aucune décision défavorable à l'égard de la personne concernée en se fondant uniquement sur la simple existence d'un indicateur de correspondance. L'accès de l'utilisateur final à un indicateur de correspondance constituera dès lors une atteinte très limitée au droit à la protection des données à caractère personnel de la personne concernée, tout en permettant aux autorités désignées et à Europol de demander l'accès aux données à caractère personnel de manière plus efficace.

(37) Le MID devrait être créé afin de soutenir le fonctionnement du CIR et les objectifs de l'EES, du VIS, d'ETIAS, d'Eurodac, du SIS et de l'ECRIS-TCN. Afin d'être efficaces dans la poursuite de leurs objectifs respectifs, tous ces systèmes d'information de l'UE nécessitent l'identification précise des personnes dont les données à caractère personnel sont stockées dans ces systèmes.

(38) En vue de mieux atteindre les objectifs des systèmes d'information de l'UE, les autorités utilisant ces systèmes devraient être en mesure de réaliser des contrôles d'identité suffisamment fiables des personnes dont les données sont stockées dans différents systèmes. L'ensemble de données d'identité ou de données du document de voyage stocké dans un système individuel donné peut être incorrect, incomplet ou frauduleux, et il n'existe à l'heure actuelle aucun moyen de détecter les données d'identité ou les données du document de voyage incorrectes, incomplètes ou frauduleuses en les comparant aux données stockées dans un autre système. Pour remédier à cette situation, il est nécessaire de disposer d'un instrument technique au niveau de l'Union qui permette l'identification précise des personnes à ces fins.

(39) Le MID devrait créer et stocker des liens entre les données contenues dans les différents systèmes d'information de l'UE afin de détecter les identités multiples, dans le double objectif de faciliter les contrôles d'identité pour les voyageurs de bonne foi et de lutter contre la fraude à l'identité. Le MID ne devrait contenir que des liens entre les données relatives à des personnes figurant dans plus d'un système d'information de l'UE. Les

données liées devraient être strictement limitées aux données nécessaires pour vérifier si une personne est enregistrée de manière justifiée ou injustifiée sous différentes identités dans différents systèmes, ou pour démontrer que deux personnes ayant des données d'identité similaires peuvent ne pas être une seule et même personne. Le traitement des données au moyen de l'ESP et du BMS partagé en vue de relier des dossiers individuels entre différents systèmes devrait être limité au strict minimum et se limiter par conséquent à la détection d'identités multiples au moment où de nouvelles données sont ajoutées à l'un des systèmes qui a des données stockées dans le CIR ou ajoutées dans le SIS. Le MID devrait prévoir des garanties contre des discriminations et des décisions défavorables potentielles à l'égard de personnes ayant des identités licites multiples.

(40) Le présent règlement prévoit de nouvelles opérations de traitement des données ayant pour but d'identifier correctement les personnes concernées. Cela constitue une atteinte aux droits fondamentaux protégés par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Étant donné que la mise en œuvre effective des systèmes d'information de l'UE dépend de l'identification correcte des personnes concernées, une telle atteinte est justifiée par les mêmes objectifs que ceux pour lesquels chacun de ces systèmes a été créé, à savoir la gestion efficace des frontières de l'Union, la sécurité intérieure de l'Union et la mise en œuvre efficace des politiques de l'Union en matière d'asile et de visas.

(41) L'ESP et le BMS partagé devraient comparer les données concernant les personnes figurant dans le CIR et dans le SIS lorsqu'une autorité nationale ou une agence de l'Union crée ou insère de nouveaux enregistrements. Cette comparaison devrait être automatisée. Le CIR et le SIS devraient utiliser le BMS partagé afin de détecter les liens possibles sur la base des données biométriques. Le CIR et le SIS devraient utiliser l'ESP afin de détecter les liens possibles sur la base des données alphanumériques. Le CIR et le SIS devraient être en mesure de détecter les données identiques ou similaires relatives à une personne stockées dans plusieurs systèmes. Lorsque tel est le cas, un lien indiquant qu'il s'agit de la même personne devrait être établi. Le CIR et le SIS devraient être configurés de manière à ce que les erreurs de translittération ou d'orthographe mineures soient détectées afin d'éviter des obstacles injustifiés pour la personne concernée.

(42) L'autorité nationale ou l'agence de l'Union qui a enregistré les données dans le système d'information de l'UE concerné devrait confirmer ou modifier ces liens. Cette autorité nationale ou cette agence de l'Union devrait avoir accès aux données stockées dans le CIR ou dans le SIS ainsi que dans le MID afin de procéder à une vérification manuelle des différentes identités.

(43) Une vérification manuelle des différentes identités devrait être effectuée par l'autorité qui crée ou met à jour les données qui ont donné lieu à une correspondance entraînant l'établissement d'un lien avec des données stockées dans un autre système d'information de l'UE. L'autorité chargée de la vérification manuelle des différentes identités devrait évaluer s'il existe des identités multiples renvoyant à la même personne de manière justifiée ou injustifiée. Lorsque cela est possible, cette évaluation devrait avoir lieu en présence des personnes concernées et, lorsque cela est nécessaire, des explications ou des informations complémentaires devraient être demandées. Il convient de procéder à cette

évaluation sans retard, conformément aux exigences légales prévues par le droit national et de l'Union en matière de précision des informations.

(44) En ce qui concerne les liens obtenus par le SIS portant sur des signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition, des personnes disparues ou des personnes vulnérables, des personnes recherchées dans le but de rendre possible leur concours dans le cadre d'une procédure judiciaire ou des personnes aux fins de contrôles discrets, de contrôles d'investigation ou de contrôles spécifiques, l'autorité chargée de la vérification manuelle des différentes identités devrait être le bureau SIRENE de l'État membre qui a créé le signalement. Ces catégories de signalements dans le SIS sont sensibles et ne devraient pas nécessairement être partagées avec les autorités qui créent ou mettent à jour les données qui sont liées à ces signalements et qui figurent dans l'un des autres systèmes d'information de l'UE. La création d'un lien avec les données du SIS devrait se faire sans préjudice des conduites à tenir conformément aux règlements (UE) 2018/1860 [8], (UE) 2018/1861 [9] et (UE) 2018/1862 [10] du Parlement européen et du Conseil.

(45) La création de ces liens exige la transparence à l'égard des personnes concernées. Afin de faciliter la mise en œuvre des garanties nécessaires conformément aux règles de l'Union applicables en matière de protection des données, les personnes qui sont concernées par un lien rouge ou un lien blanc à la suite d'une vérification manuelle des différentes identités devraient être informées par écrit, sans préjudice des restrictions nécessaires pour protéger la sécurité et l'ordre public, prévenir la criminalité et garantir que les enquêtes nationales ne soient compromises. Ces personnes devraient recevoir un numéro d'identification unique leur permettant de savoir à quelle autorité s'adresser pour exercer leurs droits.

(46) Lorsqu'un lien jaune est créé, l'autorité chargée de la vérification manuelle des différentes identités devrait avoir accès au MID. Lorsqu'un lien rouge existe, les autorités des États membres et les agences de l'Union qui ont accès à au moins un système d'information de l'UE inclus dans le CIR ou au SIS devraient avoir accès au MID. Un lien rouge devrait indiquer qu'une personne utilise différentes identités de manière injustifiée ou qu'une personne utilise l'identité d'une autre personne.

(47) Lorsqu'un lien blanc ou un lien vert existe entre des données provenant de deux systèmes d'information de l'UE, les autorités des États membres et les agences de l'Union devraient avoir accès au MID lorsque l'autorité ou l'agence concernée a accès à ces deux systèmes d'information. Un tel accès devrait être accordé à la seule fin de permettre à cette autorité ou cette agence de détecter d'éventuels cas dans lesquels des données ont été liées de manière incorrecte ou traitées dans le MID, le CIR et le SIS en violation du présent règlement, et de prendre les mesures qui s'imposent pour remédier à la situation et mettre à jour ou supprimer le lien.

(48) 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) devrait mettre en place des mécanismes automatisés de contrôle de la qualité des données et des indicateurs communs de qualité des données. Elle devrait être chargée de

développer une capacité centrale de suivi de la qualité des données et de produire des rapports réguliers d'analyse des données afin d'améliorer le contrôle de la mise en œuvre des systèmes d'information de l'UE par les États membres. Les indicateurs communs de qualité des données devraient inclure des normes de qualité minimales pour le stockage de données dans les systèmes d'information de l'UE ou des éléments d'interopérabilité. Ces normes de qualité des données devraient avoir pour objectif de permettre aux systèmes d'information de l'UE et aux éléments d'interopérabilité d'identifier automatiquement les communications de données manifestement incorrectes ou incohérentes afin que l'État membre qui en est à l'origine puisse vérifier les données et adopter les mesures correctives nécessaires.

(49) La Commission devrait évaluer les rapports de l'eu-LISA sur la qualité et, le cas échéant, adresser des recommandations aux États membres. Les États membres devraient être chargés de préparer un plan d'action décrivant les mesures visant à remédier à toute lacune dans la qualité des données et ils devraient établir des rapports réguliers à cet égard.

(50) Le format universel pour les messages (UMF) devrait servir en tant que norme pour l'échange structuré d'informations transfrontières entre les systèmes d'information, les autorités ou les organisations dans le domaine de la justice et des affaires intérieures. L'UMF devrait définir un vocabulaire commun et des structures logiques pour les informations habituellement échangées, dans le but de faciliter l'interopérabilité en permettant la création et la lecture des contenus des échanges d'une manière cohérente et sémantiquement équivalente.

(51) La mise en œuvre de la norme UMF peut être envisagée dans le VIS, le SIS et dans tout autre modèle d'échange d'informations et système d'information transfrontière, existant ou nouveau, dans le domaine de la justice et des affaires intérieures, mis au point par les États membres.

(52) Un répertoire central des rapports et statistiques (CRRS) devrait être créé afin de générer des données statistiques intersystèmes et des rapports analytiques à des fins stratégiques, opérationnelles et de qualité des données conformément aux instruments juridiques applicables. L'eu-LISA devrait établir, mettre en œuvre et héberger le CRRS sur ses sites techniques. Il devrait contenir des données statistiques anonymisées issues des systèmes d'information de l'UE, du CIR, du MID et du BMS partagé. Les données contenues dans le CRRS ne devraient pas permettre d'identifier les personnes. L'eu-LISA devrait rendre les données anonymes de manière automatisée et enregistrer ces données anonymisées dans le CRRS. Le processus d'anonymisation des données devrait être automatisé et le personnel de l'eu-LISA ne devrait pas pouvoir accéder directement aux données à caractère personnel stockées dans les systèmes d'information de l'UE ou dans les éléments d'interopérabilité.

(53) Le règlement (UE) 2016/679 s'applique au traitement des données à caractère personnel effectué à des fins d'interopérabilité dans le cadre du présent règlement par les autorités nationales, à moins que ce traitement ne soit effectué par les autorités désignées ou par les points d'accès centraux des États membres à des fins de prévention ou de détection des

infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière.

(54)Lorsque le traitement de données à caractère personnel par les États membres à des fins d'interopérabilité dans le cadre du présent règlement est effectué par les autorités compétentes à des fins de prévention out de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, la directive (UE) 2016/680 s'applique.

(55)Le règlement (UE) 2016/679, le règlement (UE) 2018/1725 ou, le cas échéant, la directive (UE) 2016/680 s'appliquent aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales effectués dans le cadre du présent règlement. Sans préjudice des motifs de transfert en vertu du chapitre V du règlement (UE) 2016/679 ou, le cas échéant, de la directive (UE) 2016/680, toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne devrait être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international en vigueur entre le pays tiers demandeur et l'Union ou un État membre.

(56)Les dispositions spécifiques en matière de protection des données du règlement (UE) 2018/1862 et du règlement (UE) 2019/816 ([11]) du Parlement européen et du Conseil s'appliquent au traitement des données à caractère personnel dans les systèmes régis par ces règlements.

(57)Le règlement (UE) 2018/1725 s'applique au traitement des données à caractère personnel par l'eu-LISA et par d'autres institutions et organes de l'Union dans l'exercice de leurs missions dans le cadre du présent règlement, sans préjudice du règlement (UE) 2016/794, qui s'applique au traitement des données à caractère personnel par Europol.

(58)Les autorités de contrôle visées dans le règlement (UE) 2016/679 ou la directive (UE) 2016/680 devraient contrôler la licéité du traitement des données à caractère personnel par les États membres. Le Contrôleur européen de la protection des données devrait contrôler les activités des institutions et organes de l'Union concernant le traitement des données à caractère personnel. Le Contrôleur européen de la protection des données et les autorités de contrôle devraient coopérer en ce qui concerne le contrôle du traitement des données à caractère personnel par les éléments d'interopérabilité. Des ressources suffisantes, y compris humaines et financières, sont nécessaires pour que le Contrôleur européen de la protection des données puisse s'acquitter des tâches qui lui sont confiées en vertu du présent règlement.

(59)Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 du Parlement européen et du Conseil ([12]) et a rendu son avis le 16 avril 2018 ([13]).

(60)Le groupe de travail «article 29» sur la protection des données a émis un avis le 11 avril 2018.

(61)Les États membres et l'eu-LISA devraient disposer de plans de sécurité afin de faciliter la mise en œuvre des obligations en matière de sécurité, et ils devraient coopérer pour

remédier aux problèmes de sécurité. L'eu-LISA devrait également s'assurer de l'utilisation continue des dernières évolutions technologiques afin de garantir l'intégrité des données en ce qui concerne le développement, la conception et la gestion des éléments d'interopérabilité. Les obligations de l'eu-LISA à cet égard devraient comprendre l'adoption des mesures nécessaires afin d'empêcher l'accès de personnes non autorisées, telles que le personnel des prestataires de services extérieurs, aux données à caractère personnel traitées au moyen des éléments d'interopérabilité. Lors de l'attribution de marchés concernant la prestation de services, les États membres et l'eu-LISA devraient envisager toutes les mesures nécessaires pour assurer le respect des lois ou réglementations relatives à la protection des données à caractère personnel et de la vie privée des personnes et pour protéger les intérêts essentiels en matière de sécurité, en application du règlement (UE) 2018/1046 du Parlement européen et du Conseil ([14]) et des conventions internationales applicables. L'eu-LISA devrait appliquer les principes de respect de la vie privée dès la conception et de respect de la vie privée par défaut au cours du développement des éléments d'interopérabilité.

62) Aux fins de l'établissement de statistiques et de rapports, il est nécessaire de permettre au personnel autorisé des autorités compétentes, des institutions et des agences de l'Union visées dans le présent règlement de consulter certaines données liées à certains éléments d'interopérabilité, sans permettre l'identification des personnes.

(63) Afin de permettre aux autorités des États membres et aux agences de l'Union de s'adapter aux nouvelles exigences concernant l'utilisation de l'ESP, il est nécessaire de prévoir une période transitoire. De même, afin de permettre le fonctionnement cohérent et optimal du MID, il convient de définir des mesures transitoires pour le début de ses activités.

(64) Étant donné que l'objectif du présent règlement, à savoir l'établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE, ne peut pas être atteint de manière suffisante par les États membres mais peut, 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 tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(65) Le montant restant du budget alloué aux frontières intelligentes dans le règlement (UE) n° 515/2014 du Parlement européen et du Conseil ([15]) devrait être réattribué au présent règlement, en application de l'article 5, paragraphe 5, point b), du règlement (UE) n° 515/2014, pour couvrir les coûts du développement des éléments d'interopérabilité.

(66) Afin de compléter certains aspects techniques détaillés du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne:

— la prolongation de la période transitoire pour l'utilisation de l'ESP,

—la prolongation de la période transitoire pour la détection des identités multiples réalisée par l'unité centrale ETIAS l'unité centrale ETIAS,

—les procédures pour déterminer les cas dans lesquels les données d'identité peuvent être considérées comme étant les mêmes ou similaires,

—les règles relatives au fonctionnement du CRRS, y compris les garanties spécifiques pour le traitement des données à caractère personnel et les règles en matière de sécurité applicables au répertoire, et

— les règles détaillées relatives au fonctionnement du portail en ligne.

Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer» ([16]). En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(67)Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission lui permettant de fixer les dates de la mise en service de l'ESP, du BMS partagé, du CIR, du MID et du CRS.

(68)Il convient également de conférer des compétences d'exécution à la Commission relatives à l'adoption de règles détaillées concernant: les détails techniques des profils des utilisateurs de l'ESP; les spécifications de la solution technique permettant l'interrogation des systèmes d'information de l'UE, des données d'Europol et des bases de données d'Interpol par l'intermédiaire de l'ESP et le format des réponses de l'ESP; les règles techniques permettant de créer des liens dans le MID entre les données de différents systèmes d'information de l'UE; le contenu et la présentation du formulaire à utiliser pour informer la personne concernée lorsqu'un lien rouge est créé; les exigences relatives aux performances du BMS partagé et le suivi de ces performances; les mécanismes, procédures et indicateurs automatisés de contrôle de la qualité des données; le développement de la norme UMF; la procédure de coopération à utiliser en cas d'incident de sécurité; les spécifications de la solution technique permettant aux États membres de gérer les demandes d'accès des utilisateurs. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([17]).

(69)Étant donné que les éléments d'interopérabilité impliqueront le traitement de quantités importantes de données à caractère personnel sensibles, il importe que les personnes dont les données sont traitées au moyen de ces éléments puissent exercer effectivement leurs droits en tant que personnes concernées, comme l'exigent le règlement (UE) 2016/679, la directive (UE) 2016/680 et le règlement (UE) 2018/1725. Il convient de mettre à disposition des personnes concernées un portail en ligne qui facilite l'exercice par celles-ci de leurs droits d'accès à leurs données à caractère personnel et de leurs droits de rectification, d'effacement et de limitation du traitement de ces données. La mise en place et la gestion dudit portail devraient incomber à l'eu-LISA.

(70)L'un des principes fondamentaux de la protection des données est la minimisation des

données: en vertu de l'article 5, paragraphe 1, point c), du règlement (UE) 2016/679, le traitement des données à caractère personnel doit être adéquat, pertinent et limité à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Pour cette raison, les éléments d'interopérabilité ne devraient pas prévoir le stockage de quelque nouvelle donnée à caractère personnel que ce soit, à l'exception des liens qui seront stockés dans le MID et qui représentent le minimum nécessaire aux fins du présent règlement.

(71) Le présent règlement devrait prévoir des dispositions claires concernant la responsabilité et le droit à réparation en cas de traitement illicite de données à caractère personnel ou en cas de tout autre acte incompatible avec le présent règlement. De telles dispositions devraient s'entendre sans préjudice du droit à réparation de la part du responsable du traitement ou du sous-traitant et de la responsabilité de ceux-ci au titre du règlement (UE) 2016/679, de la directive (UE) 2016/680 et du règlement (UE) 2018/1725. L'eu-LISA devrait être tenue pour responsable de tout dommage qu'elle cause en sa qualité de sous-traitant des données dans les cas où elle n'a pas respecté les obligations qui lui incombent spécifiquement en vertu du présent règlement, ou lorsqu'elle a agi en dehors des instructions licites de l'État membre responsable du traitement des données ou contrairement à ces instructions.

(72) Le présent règlement est sans préjudice de l'application de la directive 2004/38/CE du Parlement européen et du Conseil [18].

(73) Conformément aux articles 1er et 2 du protocole no 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ni soumis à son application. Étant donné que le présent règlement, dans la mesure où ses dispositions portent sur le SIS tel qu'il est régi par le règlement (UE) 2018/1862, développe l'acquis de Schengen, le Danemark décide, conformément à l'article 4 dudit protocole, dans un délai de six mois à partir de la décision du Conseil sur le présent règlement, s'il le transpose dans son droit interne.

(74) Dans la mesure où les dispositions du présent règlement portent sur le SIS tel qu'il est régi par le règlement (UE) 2018/1862, le Royaume-Uni participe au présent règlement, conformément à l'article 5, paragraphe 1, du protocole no 19 sur l'acquis de Schengen intégré dans le cadre de l'Union européenne, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne (ci-après dénommé «protocole sur l'acquis de Schengen»), et à l'article 8, paragraphe 2, de la décision 2000/365/CE du Conseil [19]. En outre, dans la mesure où les dispositions du présent règlement portent sur Eurodac et l'ECRIS-TCN, conformément à l'article 3 du protocole no 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Royaume-Uni a notifié, par lettre du 18 mai 2018, son souhait de participer à l'adoption et à l'application du présent règlement.

(75) Dans la mesure où les dispositions du présent règlement portent sur le SIS tel qu'il est régi par le règlement (UE) 2018/1862, l'Irlande pourrait, en principe, participer au présent règlement, conformément à l'article 5, paragraphe 1, du protocole no 19 sur l'acquis de

Schengen intégré dans le cadre de l'Union européenne, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et à l'article 6, paragraphe 2, de la décision 2002/192/CE du Conseil ([20]). En outre, dans la mesure où les dispositions du présent règlement portent sur Eurodac et l'ECRIS-TCN, conformément aux articles 1er et 2 du protocole no 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande ne participe pas à l'adoption du présent règlement et n'est pas liée par celui-ci ni soumise à son application. Dans la mesure où il n'est pas possible, dans ces conditions, de garantir que le présent règlement s'applique intégralement à l'Irlande, comme le requiert l'article 288 du traité sur le fonctionnement de l'Union européenne, l'Irlande ne participe pas à l'adoption du présent règlement et n'est pas liée par celui-ci, ni soumise à son application, sans préjudice de ses droits en vertu des protocoles no 19 et no 21.

(76) En ce qui concerne l'Islande et la Norvège, le présent règlement constitue, dans la mesure où ses dispositions portent sur le SIS tel qu'il est régi par le règlement (UE) 2018/1862, un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([21]), qui relèvent du domaine visé à l'article 1er, point G, de la décision 1999/437/CE du Conseil ([22]).

(77) En ce qui concerne la Suisse, le présent règlement constitue, dans la mesure où ses dispositions portent sur le SIS tel qu'il est régi par le règlement (UE) 2018/1862, un développement des dispositions de l'acquis de Schengen au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([23]) qui relèvent du domaine visé à l'article 1er, point G, de la décision 1999/437/CE, lue en liaison avec l'article 3 de la décision 2008/149/JAI du Conseil ([24]).

(78) En ce qui concerne le Liechtenstein, le présent règlement constitue, dans la mesure où ses dispositions portent sur le SIS tel qu'il est régi par le règlement (UE) 2018/1862, un développement des dispositions de l'acquis de Schengen au sens du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([25]) qui relèvent du domaine visé à l'article 1er, point G, de la décision 1999/437/CE, lue en liaison avec l'article 3 de la décision 2011/350/UE du Conseil ([26]).

(79) Le présent règlement respecte les droits fondamentaux et observe les principes consacrés notamment par la Charte des droits fondamentaux de l'Union européenne et devrait être appliqué conformément à ces droits et principes.

(80) Afin que le présent règlement s'intègre dans le cadre juridique existant, il y a lieu de modifier en conséquence le règlement (UE) 2018/1726 du Parlement européen et du Conseil [27] et les règlements (UE) 2018/1862 et (UE) 2019/816,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
Dispositions générales

Article premier

Objet

1. Le présent règlement, conjointement avec le règlement (UE) 2019/817 du Parlement européen et du Conseil [28], crée un cadre visant à garantir l'interopérabilité entre le système d'entrée/de sortie (EES), le système d'information sur les visas (VIS), le système européen d'information et d'autorisation concernant les voyages (ETIAS), Eurodac, le système d'information Schengen (SIS) et le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN).

2. Le cadre comprend les éléments d'interopérabilité suivants:

a) un portail de recherche européen (ESP);

b) un service partagé d'établissement de correspondances biométriques (BMS partagé);

c) un répertoire commun de données d'identité (CIR);

d) un détecteur d'identités multiples (MID).

3. Le présent règlement établit également des dispositions concernant les exigences en matière de qualité des données, le format universel pour les messages (UMF), le répertoire central des rapports et statistiques (CRRS), et les responsabilités des États membres et de l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) à l'égard de la conception, du développement et du fonctionnement des éléments d'interopérabilité.

4. Le présent règlement adapte également les procédures et les conditions d'accès des autorités désignées et de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) à l'EES, au VIS, à ETIAS et à Eurodac aux fins de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière.

5. Le présent règlement établit également un cadre permettant de vérifier l'identité des personnes et d'identifier des personnes.

Article 2

Objectifs

1. En garantissant l'interopérabilité, le présent règlement poursuit les objectifs suivants:

a) améliorer l'efficacité et l'efficience des vérifications aux frontières extérieures;

b) contribuer à la prévention de l'immigration illégale et à la lutte contre celle-ci;

c) contribuer à l'établissement d'un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union, y compris au maintien de la sécurité publique et de l'ordre public et à la préservation de la sécurité sur le territoire des États membres;

d) améliorer la mise en œuvre de la politique commune en matière de visas;

e) aider dans l'examen des demandes de protection internationale;

f) contribuer à la prévention et à la détection des infractions terroristes et d'autres infractions pénales graves, et aux enquêtes en la matière;

g) faciliter l'identification de personnes inconnues qui ne sont pas en mesure de s'identifier elles-mêmes ou de restes humains non identifiés en cas de catastrophe naturelle, d'accident ou d'attaque terroriste.

2. Les objectifs visés au paragraphe 1 sont atteints:

a) en assurant l'identification correcte des personnes;

b) en contribuant à la lutte contre la fraude à l'identité;

c) en améliorant la qualité des données et en harmonisant les exigences relatives à la qualité pour les données stockées dans les systèmes d'information de l'UE tout en respectant les exigences en matière de traitement des données prévues dans les instruments juridiques des différents systèmes ainsi que les normes et les principes en matière de protection des données;

d) en facilitant et en soutenant la mise en œuvre technique et opérationnelle, par les États membres, des systèmes d'information de l'UE;

e) en renforçant, en simplifiant et en rendant plus uniformes les conditions de sécurité des données et de protection des données régissant les différents systèmes d'information de l'UE, sans porter atteinte à la protection et aux garanties spéciales accordées à certaines catégories de données;

f) en rationalisant les conditions d'accès des autorités désignées à l'EES, au VIS, à ETIAS et à Eurodac, tout en garantissant les conditions nécessaires et proportionnées de cet accès;

g) en soutenant les objectifs de l'EES, du VIS, d'ETIAS, d'Eurodac, du SIS et de l'ECRIS-TCN.

Article 3

Champ d'application

1. Le présent règlement s'applique à Eurodac, au SIS et à l'ECRIS-TCN.

2. Le présent règlement s'applique également aux données d'Europol dans la mesure nécessaire pour permettre à celles-ci d'être interrogées simultanément avec les systèmes d'information de l'UE visés au paragraphe 1.

3. Le présent règlement s'applique aux personnes à l'égard desquelles des données à caractère personnel peuvent être traitées dans les systèmes d'information de l'UE visés au paragraphe 1 et dans les données d'Europol visées au paragraphe 2.

Article 4

Définitions

Aux fins du présent règlement, on entend par:

1) **«frontières extérieures»**: les frontières extérieures telles qu'elles sont définies à l'article 2, point 2), du règlement (UE) 2016/399 du Parlement européen et du Conseil ([29]);

2) **«vérifications aux frontières»**: les vérifications aux frontières telles qu'elles sont définies à l'article 2, point 11), du règlement (UE) 2016/399;

3) **«autorité frontalière»**: le garde-frontière chargé, conformément au droit national, d'effectuer des vérifications aux frontières;

4) **«autorités de contrôle»**: l'autorité de contrôle visée à l'article 51, paragraphe 1, du règlement (UE) 2016/679 et l'autorité de contrôle visée à l'article 41, paragraphe 1, de la directive (UE) 2016/680;

5) **«vérification»**: le processus consistant à comparer des séries de données en vue d'établir la validité d'une identité déclarée (contrôle par comparaison de deux échantillons);

6) **«identification»**: le processus consistant à déterminer l'identité d'une personne par interrogation d'une base de données et comparaison avec plusieurs séries de données (contrôle par comparaison de plusieurs échantillons);

7) **«données alphanumériques»**: les données représentées par des lettres, des chiffres, des caractères spéciaux, des espaces et des signes de ponctuation;

8) **«données d'identité»**: les données visées à l'article 27, paragraphe 3, points a) à e);

9) **«données dactyloscopiques»**: les images d'empreintes digitales et les images d'empreintes digitales latentes qui, en raison de leur caractère unique et des points de référence qu'elles contiennent, permettent de réaliser des comparaisons précises et concluantes en ce qui concerne l'identité d'une personne;

10) **«image faciale»**: les images numériques du visage;

11) **«données biométriques»**: les données dactyloscopiques ou les images faciales ou les deux;

12) **«modèle biométrique»**: une représentation mathématique obtenue par l'extraction de caractéristiques des données biométriques, se limitant aux caractéristiques nécessaires pour procéder à des identifications et à des vérifications;

13) **«document de voyage»**: un passeport ou autre document équivalent, autorisant son titulaire à franchir les frontières extérieures et sur lequel un visa peut être apposé;

14) **«données du document de voyage»**: le type, le numéro et le pays de délivrance du document de voyage, la date d'expiration de sa validité et le code à trois lettres du pays de délivrance du document de voyage;

15) **«systèmes d'information de l'UE»**: l'EES, le VIS, ETIAS, Eurodac, le SIS et l'ECRIS-TCN;

16) **«données d'Europol»**: les données à caractère personnel traitées par Europol pour les finalités visées à l'article 18, paragraphe 2, points a), b) et c), du règlement (UE) 2016/794;

17) **«bases de données d'Interpol»**: la base de données d'Interpol sur les documents de voyage volés et perdus (base de données SLTD) et la base de données d'Interpol sur les documents de voyage associés aux notices (base de données TDAWN);

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

19) **«service de police»**: l'autorité compétente telle qu'elle est définie à l'article 3, point 7), de la directive (UE) 2016/680;

20) **«autorités désignées»**: les autorités désignées par les États membres telles qu'elles sont définies à l'article 3, paragraphe 1, point 26), du règlement (UE) 2017/2226 du Parlement européen et du Conseil [30], à l'article 2, paragraphe 1, point e), de la décision 2008/633/JAI du Conseil [31] et à l'article 3, paragraphe 1, point 21, du règlement (UE) 2018/1240 du Parlement européen et du Conseil [32];

21) **«infraction terroriste»**: une infraction prévue par le droit national qui correspond ou est équivalente à l'une des infractions visées dans la directive (UE) 2017/541 du Parlement européen et du Conseil [33];

22) **«infraction pénale grave»**: une infraction qui correspond ou est équivalente à l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil [34], si elle est punie en droit national d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans;

23) **«système d'entrée/de sortie» ou «EES»**: le système d'entrée/de sortie créé par le règlement (UE) 2017/2226;

24) **«système d'information sur les visas» ou «VIS»**: le système d'information sur les visas établi par le règlement (CE) nº 767/2008 du Parlement européen et du Conseil ([35]);

25) **«système européen d'information et d'autorisation concernant les voyages» ou «ETIAS»**: le système européen d'information et d'autorisation concernant les voyages créé par le règlement (UE) 2018/1240;

26) **«Eurodac»**: Eurodac créé par le règlement (UE) nº 603/2013 du Parlement européen et du Conseil ([36]);

27) **«système d'information Schengen» ou «SIS»**: le système d'information Schengen établi par les règlements (UE) 2018/1860, (UE) 2018/1861 et (UE) 2018/1862;

28) **«ECRIS-TCN»**: le système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides créé par le règlement (UE) 2019/816 du Parlement européen et du Conseil.

Article 5

Non-discrimination et droits fondamentaux

Le traitement de données à caractère personnel aux fins du présent règlement ne donne lieu à aucune discrimination à l'encontre des personnes, fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. Il respecte pleinement la dignité humaine, l'intégrité des personnes et les droits fondamentaux, notamment le droit au respect de la vie privée et le droit à la protection des données à caractère personnel. Une attention particulière est accordée aux enfants, aux personnes âgées, aux personnes handicapées et aux personnes nécessitant une protection internationale. L'intérêt supérieur de l'enfant est une considération primordiale.

CHAPITRE II

Portail de recherche européen

Article 6

Portail de recherche européen

1. Un portail de recherche européen (ESP) est créé afin de faciliter l'accès rapide, continu, efficace, systématique et contrôlé des autorités des États membres et des agences de l'Union aux systèmes d'information de l'UE, aux données d'Europol et aux bases de données d'Interpol pour l'accomplissement de leurs tâches et

conformément à leurs droits d'accès ainsi qu'aux objectifs et finalités de l'EES, du VIS, d'ETIAS, d'Eurodac, du SIS et de l'ECRIS-TCN.

2. L'ESP se compose des éléments suivants:

a) une infrastructure centrale comportant un portail de recherche permettant d'interroger simultanément l'EES, le VIS, ETIAS, Eurodac, le SIS, l'ECRIS-TCN ainsi que les données d'Europol et les bases de données d'Interpol;

b) un canal de communication sécurisé entre l'ESP, les États membres et les agences de l'Union qui sont autorisées à utiliser l'ESP;

c) une infrastructure de communication sécurisée entre l'ESP et l'EES, le VIS, ETIAS, Eurodac, le SIS central, l'ECRIS-TCN, les données d'Europol et les bases de données d'Interpol ainsi qu'entre l'ESP et les infrastructures centrales du CIR et du MID.

3. L'eu-LISA développe l'ESP et en assure la gestion technique.

Article 7

Utilisation du portail de recherche européen

1. L'utilisation de l'ESP est réservée aux autorités des États membres et aux agences de l'Union ayant accès à au moins l'un des systèmes d'information de l'UE conformément aux instruments juridiques régissant ces systèmes d'information de l'UE, au CIR et au MID conformément au présent règlement, aux données d'Europol conformément au règlement (UE) 2016/794, ou aux bases de données d'Interpol conformément au droit de l'Union ou au droit national régissant cet accès.

Ces autorités des États membres et ces agences de l'Union peuvent utiliser l'ESP et les données qu'il fournit uniquement pour les objectifs et finalités prévus dans les instruments juridiques régissant ces systèmes d'information de l'UE, dans le règlement (UE) 2016/794 et dans le présent règlement.

2. Les autorités des États membres et les agences de l'Union visées au paragraphe 1 utilisent l'ESP pour effectuer des recherches dans les données relatives à des personnes ou à leurs documents de voyage dans les systèmes centraux d'Eurodac et de l'ECRIS-TCN conformément aux droits d'accès que leur confèrent les instruments juridiques régissant ces systèmes d'information de l'UE et le droit national. Elles utilisent aussi l'ESP pour interroger le CIR conformément aux droits d'accès dont elles bénéficient dans le cadre du présent règlement aux fins visées aux articles 20, 21 et 22.

3. Les autorités des États membres visées au paragraphe 1 peuvent utiliser l'ESP pour effectuer des recherches dans les données relatives à des personnes ou à leurs documents de voyage dans le SIS central visé dans les règlements (UE) 2018/1860 et (UE) 2018/1861.

4. Lorsque le droit de l'Union le prévoit, les agences de l'Union visées au paragraphe 1 utilisent l'ESP pour effectuer des recherches dans les données relatives à des personnes ou à leurs documents de voyage dans le SIS central.

5. Les autorités des États membres et les agences de l'Union visées au paragraphe 1 peuvent utiliser l'ESP pour effectuer des recherches dans les données relatives à des personnes ou à leurs documents de voyage dans les données d'Europol conformément aux droits d'accès que leur confèrent le droit de l'Union et le droit national.

Article 8

Profils des utilisateurs du portail de recherche européen

1. Afin de permettre l'utilisation de l'ESP, l'eu-LISA crée, en collaboration avec les États membres, un profil basé sur chaque catégorie d'utilisateurs de l'ESP et sur les finalités des requêtes, conformément aux détails techniques et aux droits d'accès visés au paragraphe 2. Chaque profil comprend, indiquant, conformément au droit de l'Union et au droit national, les informations suivantes:

a) les champs de données à utiliser pour les interrogations;

b) les systèmes d'information de l'UE, les données d'Europol et les bases de données d'Interpol qui sont interrogées, ceux qui peuvent être interrogés et ceux qui fournissent une réponse à l'utilisateur;

c) les données spécifiques qui peuvent être interrogées dans les systèmes d'information de l'UE, les données d'Europol et les bases de données d'Interpol;

d) les catégories de données qui peuvent être fournies dans chaque réponse.

2. La Commission adopte des actes d'exécution afin de préciser les détails techniques des profils visés au paragraphe 1 conformément aux droits d'accès des utilisateurs de l'ESP prévus dans les instruments juridiques régissant les systèmes d'information de l'UE et dans le droit national. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

3. Les profils visés au paragraphe 1 sont réexaminés régulièrement, au moins une fois par an, par l'eu-LISA, en collaboration avec les États membres, et, si nécessaire, mis à jour.

Article 9

Requêtes

1. Les utilisateurs de l'ESP lancent une requête en soumettant des données alphanumériques ou biométriques à l'ESP. Lorsqu'une requête a été lancée, l'ESP interroge l'EES, ETIAS, le VIS, le SIS, Eurodac, l'ECRIS-TCN et le CIR ainsi que les données d'Europol et les bases de données d'Interpol simultanément, à l'aide des données envoyées par l'utilisateur et conformément au profil d'utilisateur.

2. Les catégories de données utilisés pour lancer une requête par l'intermédiaire de l'ESP correspondent aux catégories de données relatives à des personnes ou à des documents de voyage qui peuvent être utilisés pour interroger les différents

systèmes d'information de l'UE, les données d'Europol et les bases de données d'Interpol conformément aux instruments juridiques qui les régissent.

3. L'eu-LISA met en œuvre pour l'ESP, en collaboration avec les États membres, un document de contrôle des interfaces basé sur l'UMF visé à l'article 38.

4. Lorsqu'une requête est lancée par un utilisateur de l'ESP, l'EES, ETIAS, le VIS, le SIS, Eurodac, l'ECRIS-TCN, le CIR et le MID, ainsi que les données d'Europol et les bases de données d'Interpol, fournissent en réponse à la requête les données qu'ils détiennent.

Sans préjudice de l'article 20, la réponse fournie par l'ESP indique à quel système d'information de l'UE ou à quelle base de données les données appartiennent.

L'ESP ne fournit aucune information concernant des données contenues dans des systèmes d'information de l'UE, les données d'Europol et les bases de données d'Interpol auxquels l'utilisateur n'a pas accès en vertu du droit de l'Union ou du droit national applicable.

5. Toute interrogation des bases de données d'Interpol lancée via l'ESP est effectuée de telle manière qu'aucune information n'est révélée au propriétaire du signalement Interpol.

6. L'ESP fournit des réponses à l'utilisateur dès que des données sont disponibles dans un des systèmes d'information de l'UE, dans les données d'Europol ou dans les bases de données d'Interpol. Ces réponses comportent uniquement les données auxquelles l'utilisateur a accès en vertu du droit de l'Union ou du droit national.

7. La Commission adopte un acte d'exécution afin de préciser la procédure technique permettant à l'ESP d'interroger les systèmes d'information de l'UE, les données d'Europol et les bases de données d'Interpol et déterminer le format des réponses de l'ESP. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

Article 10

Tenue de registres

1. Sans préjudice des articles 12 et 18 du règlement (UE) 2018/1862, de l'article 29 du règlement (UE) 2019/816 et de l'article 40 du règlement (UE) 2016/794, l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans l'ESP. Ces registres contiennent les informations suivantes:

a) l'État membre ou l'agence de l'Union qui lance la requête et le profil ESP utilisé;

b) la date et l'heure de la requête;

c) les systèmes d'information de l'UE et les données d'Europol qui ont été interrogés.

2. Chaque État membre tient des registres des requêtes introduites par ses autorités et le personnel de ces autorités dûment autorisé à utiliser l'ESP. Chaque agence de

l'Union tient des registres des requêtes introduites par son personnel dûment autorisé.

3. Les registres visés aux paragraphes 1 et 2 ne peuvent être utilisés que pour contrôler la protection des données, y compris vérifier la recevabilité d'une requête et la licéité du traitement des données, et pour garantir la sécurité et l'intégrité des données. Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création. Cependant, s'ils sont nécessaires à des procédures de contrôle qui ont déjà été engagées, ils sont effacés dès qu'ils ne sont plus nécessaires aux procédures de contrôle.

Article 11

Procédures de secours en cas d'impossibilité technique d'utiliser le portail de recherche européen

1. Lorsqu'il est techniquement impossible d'utiliser l'ESP pour interroger un ou plusieurs des systèmes d'information de l'UE ou le CIR, en raison d'une défaillance de l'ESP, l'eu-LISA le notifie, de manière automatisée, aux utilisateurs de l'ESP.

2. Lorsqu'il est techniquement impossible d'utiliser l'ESP pour interroger un ou plusieurs des systèmes d'information de l'UE ou le CIR en raison d'une défaillance de l'infrastructure nationale d'un État membre, cet État membre le notifie, de manière automatisée, à l'eu-LISA et à la Commission.

3. Dans les cas visés au paragraphe 1 ou 2 du présent article, et jusqu'à ce qu'il soit remédié à la défaillance technique, l'obligation visée à l'article 7, paragraphes 2 et 4, ne s'applique pas et les États membres ont accès aux systèmes d'information de l'UE ou au CIR directement lorsque le droit de l'Union ou le droit national l'exige.

4. Lorsqu'il est techniquement impossible d'utiliser l'ESP pour interroger un ou plusieurs des systèmes d'information de l'UE ou le CIR, en raison d'une défaillance de l'infrastructure d'une agence de l'Union, ladite agence le notifie, de manière automatisée, à l'eu-LISA et à la Commission.

CHAPITRE III

Service partagé d'établissement de correspondances biométriques

Article 12

Service partagé d'établissement de correspondances biométriques

1. Un service partagé d'établissement de correspondances biométriques (BMS partagé) stockant des modèles biométriques obtenus à partir des données biométriques visées à l'article 13, qui sont stockées dans le CIR et le SIS, et permettant d'effectuer des recherches à l'aide de données biométriques dans plusieurs systèmes d'information de l'UE est mis en place afin de soutenir le CIR et

le MID ainsi que les objectifs de l'EES, du VIS, d'Eurodac, du SIS et de l'ECRIS-TCN.

2. Le BMS partagé se compose des éléments suivants:

a) une infrastructure centrale qui remplace les systèmes centraux de l'EES, du VIS, du SIS, d'Eurodac et de l'ECRIS-TCN, respectivement, dans la mesure où elle stocke des modèles biométriques et permet d'effectuer des recherches à l'aide de données biométriques;

b) une infrastructure de communication sécurisée entre le BMS partagé, le SIS central et le CIR.

3. L'eu-LISA développe le BMS partagé et en assure la gestion technique.

Article 13

Stockage de modèles biométriques dans le service partagé d'établissement de correspondances biométriques

1. Le BMS partagé stocke les modèles biométriques qu'il obtient à partir des données biométriques suivantes:

a) les données visées à l'article 20, paragraphe 3, points w) et y), à l'exception des données relatives aux empreintes palmaires, du règlement (UE) 2018/1862;

b) les données visées à l'article 5, paragraphe 1, point b), et à l'article 5, paragraphe 2, du règlement (UE) 2019/816.

Les modèles biométriques sont stockés dans le BMS partagé sous une forme séparée logiquement en fonction du système d'information de l'UE d'où les données proviennent.

2. Pour chaque ensemble de données visé au paragraphe 1, le BMS partagé inclut, dans chaque modèle biométrique, une référence aux systèmes d'information de l'UE dans lesquels les données biométriques correspondantes sont stockées et une référence aux enregistrements concrets dans ces systèmes d'information de l'UE.

3. Les modèles biométriques sont introduits dans le BMS partagé uniquement après que le BMS partagé a effectué un contrôle automatisé de la qualité des données biométriques ajoutées à l'un des systèmes d'information de l'UE, pour s'assurer du respect d'une norme minimale de qualité des données.

4. Le stockage des données visées au paragraphe 1 respecte les normes de qualité visées à l'article 37, paragraphe 2.

5. La Commission définit, par la voie d'un acte d'exécution, les exigences relatives aux performances du BMS partagé et les modalités pratiques pour le suivi des performances du BMS partagé, afin de veiller à ce que l'efficacité des recherches biométriques soit adaptée à la rapidité requise par des procédures telles que les vérifications aux frontières et les identifications. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

Article 14

Recherche dans des données biométriques à l'aide du service partagé d'établissement de correspondances biométriques

Afin que des recherches puissent être effectuées dans les données biométriques stockées dans le CIR et le SIS, le CIR et le SIS utilisent les modèles biométriques stockés dans le BMS partagé. Les recherches effectuées à l'aide de données biométriques sont effectuées conformément aux finalités prévues dans le présent règlement et dans les règlements (CE) n° 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 et (UE) 2019/816.

Article 15

Conservation des données dans le service partagé d'établissement de correspondances biométriques

Les données visées à l'article 13, paragraphes 1 et 2, ne sont stockées dans le BMS partagé qu'aussi longtemps que les données biométriques correspondantes sont stockées dans le CIR ou le SIS. Les données sont effacées du BMS partagé de manière automatisée.

Article 16

Tenue de registres

1. Sans préjudice des articles 12 et 18 du règlement (UE) 2018/1862 et de l'article 29 du règlement (UE) 2019/816, l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le BMS partagé. Ces registres contiennent les informations suivantes:

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

b) l'historique de la création et du stockage des modèles biométriques;

c) les systèmes d'information de l'UE interrogés à l'aide des modèles biométriques stockés dans le BMS partagé;

d) la date et l'heure de la requête;

e) le type de données biométriques utilisées pour lancer la requête;

f) les résultats de la requête ainsi que la date et l'heure des résultats.

2. Chaque État membre tient des registres des requêtes introduites par ses autorités et le personnel de ces autorités dûment autorisé à utiliser le BMS partagé. Chaque agence de l'Union tient des registres des requêtes introduites par son personnel dûment autorisé.

3. Les registres visés aux paragraphes 1 et 1 *bis* ne peuvent être utilisés que pour contrôler la protection des données, y compris vérifier l'admissibilité d'une requête et la licéité du traitement des données, et pour garantir la sécurité et l'intégrité des données. Ces registres sont protégés par des mesures appropriées empêchant tout

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

CHAPITRE IV
Répertoire commun de données d'identité

Article 17

Répertoire commun de données d'identité

1. Un répertoire commun de données d'identité (CIR), créant un dossier individuel pour chaque personne enregistrée dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN contenant les données visées à l'article 18, est établi afin de faciliter l'identification correcte des personnes enregistrées dans l'EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN et d'aider à cette identification conformément à l'article 20, de soutenir le fonctionnement du MID conformément à l'article 21 et de faciliter et de rationaliser l'accès des autorités désignées et d'Europol à l'EES, au VIS, à ETIAS et à Eurodac, lorsque cela est nécessaire à des fins de prévention ou de détection d'infractions terroristes ou d'autres infractions pénales graves ou d'enquêtes en la matière, conformément à l'article 22.

2. Le CIR se compose des éléments suivants:

a) une infrastructure centrale qui remplace les systèmes centraux de l'EES, du VIS, d'ETIAS, d'Eurodac et de l'ECRIS-TCN, dans la mesure où elle stocke les données visées à l'article 18;

b) un canal de communication sécurisé entre le CIR, les États membres et les agences de l'Union qui sont autorisés à utiliser le CIR conformément au droit de l'Union et au droit national;

c) une infrastructure de communication sécurisée entre le CIR et l'EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN, ainsi que les infrastructures centrales de l'ESP, du BMS partagé et du MID.

3. L'eu-LISA développe le CIR et en assure la gestion technique.

4. Lorsqu'il est techniquement impossible, en raison d'une défaillance du CIR, d'interroger le CIR aux fins de l'identification d'une personne en vertu de l'article 20, de la détection d'identités multiples en vertu de l'article 21 ou à des fins de prévention ou de détection d'infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, en vertu de l'article 22, l'eu-LISA le notifie aux utilisateurs du CIR, de manière automatisée.

5. L'eu-LISA met en œuvre pour le CIR, en collaboration avec les États membres, un document de contrôle des interfaces basé sur l'UMF visé à l'article 38.

Article 18

Données du répertoire commun de données d'identité

1. Le CIR stocke les données suivantes séparées logiquement en fonction du système d'information d'où elles proviennent: les données visées à l'article 5, paragraphe 1, point b), et à l'article 5, paragraphe 2, ainsi que les données suivantes mentionnées à l'article 5, paragraphe 1, point a), du règlement (UE) 2019/816: le nom (nom de famille), les prénoms, la date de naissance, le lieu de naissance (ville et pays), la ou les nationalités, le genre, les noms précédents, le cas échéant, lorsqu'ils sont disponibles, les pseudonymes ou noms d'emprunt, ainsi que, lorsqu'elles sont disponibles, les informations sur les documents de voyage.

2. Pour chaque ensemble de données visé au paragraphe 1, le CIR comporte une référence aux systèmes d'information de l'UE auxquels appartiennent les données.

3. Les autorités qui disposent d'un accès au CIR y accèdent conformément à leurs droits d'accès prévus dans les instruments juridiques qui régissent les systèmes d'information de l'UE, au droit national et à leurs droits d'accès prévus au présent règlement pour les fins visées aux articles 20, 21 et 22.

4. Pour chaque ensemble de données visé au paragraphe 1, le CIR comporte une référence à l'enregistrement effectivement réalisé dans les systèmes d'information de l'UE auxquels appartiennent les données.

5. Le stockage des données visées au paragraphe 1 respecte les normes de qualité visées à l'article 37, paragraphe 2.

Article 19

Ajout, modification et suppression de données dans le répertoire commun de données d'identité

1. Lorsque des données sont ajoutées, modifiées ou supprimées dans Eurodac ou dans l'ECRIS-TCN, les données visées à l'article 18 qui sont stockées dans le dossier individuel du CIR font l'objet, de manière automatisée, d'un ajout, d'une modification ou d'une suppression en conséquence.

2. Lorsqu'un lien blanc ou rouge est créé dans le MID conformément à l'article 32 ou 33 entre les données de deux ou plusieurs des systèmes d'information de l'UE alimentant le CIR, au lieu de créer un nouveau dossier individuel, le CIR ajoute les nouvelles données au dossier individuel des données liées.

Article 20

Accès au répertoire commun de données d'identité pour identification

1. Les interrogations du CIR sont effectuées par un service de police conformément aux paragraphes 2 et 5 uniquement dans les circonstances suivantes:

a) lorsqu'un service de police n'est pas en mesure d'identifier une personne en raison de l'absence d'un document de voyage ou d'un autre document crédible prouvant l'identité de cette personne;

b) lorsqu'un doute subsiste quant aux données d'identité fournies par une personne;

c) lorsqu'un doute subsiste quant à l'authenticité du document de voyage ou d'un autre document crédible fourni par une personne;

d) lorsqu'un doute subsiste quant à l'identité du titulaire d'un document de voyage ou d'un autre document crédible; ou

e) lorsqu'une personne n'est pas en mesure ou refuse de coopérer.

Ces interrogations ne peuvent viser des mineurs de moins de 12 ans, à moins que ce ne soit dans l'intérêt supérieur de l'enfant.

2. Lorsqu'une des circonstances énumérées au paragraphe 1 se produit et qu'un service de police y a été habilité par les mesures législatives nationales visées au paragraphe 5, elle peut, uniquement aux fins de l'identification d'une personne, interroger le CIR à l'aide des données biométriques de cette personne relevées en direct lors d'un contrôle d'identité, à condition que la procédure ait été initiée en présence de ladite personne.

3. Lorsque le résultat de l'interrogation indique que des données concernant cette personne sont stockées dans le CIR, le service de police a accès en consultation aux données visées à l'article 18, paragraphe 1.

Lorsque les données biométriques de la personne ne peuvent pas être utilisées ou lorsque la requête introduite avec ces données échoue, cette dernière est introduite à l'aide des données d'identité de cette personne, combinées aux données du document de voyage, ou à l'aide des données d'identité fournies par cette personne.

4. Lorsqu'un service de police y a été habilité par des mesures législatives nationales visées au paragraphe 6, il peut, en cas de catastrophe naturelle, d'accident ou d'attaque terroriste, et uniquement aux fins d'identification de personnes inconnues qui ne sont pas en mesure de s'identifier elles-mêmes ou de restes humains non identifiés, interroger le CIR à l'aide des données biométriques de ces personnes.

5. Les États membres qui souhaitent faire usage de la possibilité prévue au paragraphe 2 adoptent des mesures législatives nationales. Ce faisant, les États membres tiennent compte de la nécessité d'éviter toute discrimination à l'encontre de ressortissants de pays tiers. Ces mesures législatives indiquent les finalités précises de l'identification, parmi les finalités visées à l'article 2, paragraphe 1, points b) et c). Elles désignent les services de police compétentes et fixent les procédures, les conditions et les critères relatifs à ces contrôles.

6. Les États membres qui souhaitent faire usage de la possibilité prévue au paragraphe 4 adoptent des mesures législatives nationales fixant les procédures, les conditions et les critères.

Article 21

Accès au répertoire commun de données d'identité pour la détection d'identités multiples

1. Lorsque le résultat d'une interrogation du CIR donne lieu à un lien jaune conformément à l'article 28, paragraphe 4, l'autorité chargée de la vérification manuelle des différentes identités conformément à l'article 29 a accès, aux seules fins de cette vérification, aux données visées à l'article 18, paragraphes 1 et 2, stockées dans le CIR reliées par un lien jaune.

2. Lorsque le résultat d'une interrogation du CIR donne lieu à un lien rouge conformément à l'article 32, les autorités visées à l'article 26, paragraphe 2, ont accès, aux seules fins de lutter contre la fraude à l'identité, aux données visées à l'article 18, paragraphes 1 et 2, stockées dans le CIR reliées par un lien rouge.

Article 22

Interrogation du répertoire commun de données d'identité à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière

1. Dans des cas particuliers, lorsqu'il existe des motifs raisonnables de croire que la consultation des systèmes d'information de l'UE contribuera à la prévention ou à la détection des infractions terroristes ou d'autres infractions pénales graves, ou aux enquêtes en la matière, notamment lorsqu'il y a lieu de penser que la personne soupçonnée d'avoir commis une infraction terroriste ou d'autres infractions pénales graves, ou l'auteur ou la victime de telles infractions est une personne dont les données sont stockées dans Eurodac, les autorités désignées et Europol peuvent consulter le CIR pour savoir si des données sur une personne en particulier figurent dans Eurodac.

2. Lorsque, en réponse à une requête, le CIR indique que des données sur cette personne figurent dans Eurodac, le CIR fournit aux autorités désignées et à Europol une réponse sous la forme d'une référence, telle que visée à l'article 18, paragraphe 2, indiquant que Eurodac contient des données correspondantes. Le CIR fournit une réponse selon des modalités qui ne compromettent pas la sécurité des données.

La réponse indiquant que des données concernant cette personne figurent dans Eurodac n'est utilisée qu'aux fins de l'introduction d'une demande d'accès complet sous réserve des conditions et des procédures fixées dans les différents instruments juridiques régissant l'accès en question.

En cas d'une ou plusieurs correspondances, l'autorité désignée ou Europol demande un accès complet à au moins un des systèmes d'information avec lesquels une correspondance a été établie.

Si, à titre exceptionnel, cet accès complet n'est pas demandé, la justification de cette absence de demande est enregistrée par les autorités désignées de manière à pouvoir être reliée au dossier national s. Europol enregistre la justification dans le dossier concerné.

3. L'accès complet aux données figurant dans Eurodac aux fins de prévenir ou de détecter les infractions terroristes ou les infractions pénales graves, ou d'enquêter sur celles-ci, reste soumis aux conditions et procédures prévues dans l'instrument juridique régissant cet accès.

Article 23

Conservation des données dans le répertoire commun de données d'identité

1. Les données visées à l'article 18, paragraphes 1, 2 et 4, sont supprimées du CIR, de manière automatisée, conformément aux dispositions relatives à la conservation des données du règlement (UE) 2019/816.

2. Le dossier individuel n'est stocké dans le CIR qu'aussi longtemps que les données correspondantes sont stockées dans au moins un des systèmes d'information de l'UE dont les données figurent dans le CIR. La création d'un lien n'a aucune incidence sur la période de conservation de chaque élément des données liées.

Article 24

Tenue de registres

1. Sans préjudice de l'article 29 du règlement (UE) 2019/816, l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le CIR conformément aux paragraphes 2, 3 et 4 du présent article.

2. L'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le CIR en vertu de l'article 20. Ces registres contiennent les informations suivantes:

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

b) la finalité de l'accès par l'utilisateur qui introduit la requête par l'intermédiaire du CIR;

c) la date et l'heure de la requête;

d) le type de données utilisées pour lancer la requête;

e) les résultats de la requête.

3. L'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le CIR en vertu de l'article 21. Ces registres contiennent les informations suivantes:

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

b) la finalité de l'accès par l'utilisateur qui introduit la requête par l'intermédiaire du CIR;

c) la date et l'heure de la requête;

d) lorsqu'un lien est créé, les données utilisées pour lancer la requête et les résultats de la requête indiquant le système d'information de l'UE d'où proviennent les données.

4. L'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le CIR en vertu de l'article 22. Ces registres contiennent les informations suivantes:

a) la date et l'heure de la requête;

b) les données utilisées pour lancer la requête;

c) les résultats de la requête;

d) l'État membre ou l'agence de l'Union qui interroge le CIR.

L'autorité de contrôle compétente, conformément à l'article 41 de la directive (UE) 2016/680, ou le Contrôleur européen de la protection des données, conformément à l'article 43 du règlement (UE) 2016/794, vérifient régulièrement les registres de ces accès, à des intervalles ne dépassant pas six mois, afin de vérifier si les procédures et conditions prévues à l'article 22, paragraphes 1 et 2 du présent règlement sont respectées.

5. Chaque État membre tient des registres des requêtes introduites en vertu des articles 20, 21 et 22 par ses autorités et le personnel de ces autorités dûment autorisé à utiliser le CIR. Chaque agence de l'Union tient des registres des requêtes introduites par son personnel dûment autorisé en vertu des articles 21 et 22.

En outre, pour tout accès au CIR autorisé en vertu de l'article 22, chaque État membre tient les registres suivants:

a) la référence du dossier national;

b) la finalité de l'accès;

c) conformément aux règles nationales, l'identifiant unique de l'agent qui a introduit la recherche et celui de l'agent qui a ordonné la recherche.

6. Conformément au règlement (UE) 2016/794, pour tout accès au CIR accordé en vertu de l'article 22 du présent règlement, Europol tient des registres de l'identifiant unique de l'agent qui a introduit la requête et de celui de l'agent qui a ordonné la requête.

7. Les registres visés aux paragraphes 2 à 6 ne peuvent être utilisés que pour contrôler la protection des données, y compris vérifier l'admissibilité d'une requête et la licéité du traitement des données, et pour garantir la sécurité et l'intégrité des données. Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création. Cependant, s'ils sont nécessaires à des procédures de contrôle qui sont déjà engagées, ils sont effacés dès qu'ils ne sont plus nécessaires aux procédures de contrôle.

8. L'eu-LISA conserve les registres relatifs à l'historique des données dans les dossiers individuels. L'eu-LISA efface ces registres, de manière automatisée, une fois les données effacées.

CHAPITRE V

Détecteur d'identités multiples

Article 25

Détecteur d'identités multiples

1. Un détecteur d'identités multiples (MID) qui crée et stocke les dossiers de confirmation d'identité visés à l'article 34, contenant des liens entre les données des systèmes d'information de l'UE figurant dans le CIR et dans le SIS et permettant la détection des identités multiples, avec le double objectif de faciliter les contrôles d'identité et de lutter contre la fraude à l'identité, est établi afin de soutenir le fonctionnement du CIR et les objectifs de l'EES, du VIS, d'ETIAS, d'Eurodac, du SIS et de l'ECRIS-TCN.

2. Le MID se compose des éléments suivants:

a) une infrastructure centrale qui stocke des liens et des références aux systèmes d'information de l'UE;

b) une infrastructure de communication sécurisée pour connecter le MID au SIS et aux infrastructures centrales de l'ESP et du CIR.

3. L'eu-LISA développe le MID et en assure la gestion technique.

Article 26

Accès au détecteur d'identités multiples

1. Aux fins de la vérification manuelle des différentes identités visée à l'article 29, l'accès aux données visées à l'article 34 stockées dans le MID est accordé:

a) au bureau SIRENE de l'État membre qui crée ou actualise un signalement conformément au règlement (UE) 2018/1862;

b) aux autorités centrales de l'État membre de condamnation lorsqu'elles enregistrent ou modifient des données dans l'ECRIS-TCN conformément à l'article 5 ou 9 du règlement (UE) 2019/816.

2. Les autorités des États membres et les agences de l'Union ayant accès à au moins un système d'information de l'UE alimentant le CIR ou au SIS ont accès aux données visées à l'article 34, points a) et b), en ce qui concerne les liens rouges visés à l'article 32.

3. Les autorités des États membres et les agences de l'Union ont accès aux liens blancs visés à l'article 33 lorsqu'elles ont accès aux deux systèmes d'information de l'UE contenant des données entre lesquelles le lien blanc a été créé.

4. Les autorités des États membres et les agences de l'Union ont accès aux liens verts visés à l'article 31 lorsqu'elles ont accès aux deux systèmes d'information de l'UE contenant des données entre lesquelles le lien vert a été créé et qu'une interrogation de ces systèmes d'information a révélé une correspondance avec les deux séries de données liées.

Article 27

Détection d'identités multiples

1. Une détection d'identités multiples dans le CIR et le SIS est lancée lorsque:

a) un signalement concernant une personne est créé ou actualisé dans le SIS conformément aux chapitres VI à IX du règlement (UE) 2018/1862;

b) un enregistrement de données est créé ou modifié dans l'ECRIS-TCN conformément à l'article 5 ou 9 du règlement (UE) 2019/816.

2. Lorsque les données figurant dans un système d'information de l'UE visé au paragraphe 1 comportent des données biométriques, le CIR et le SIS central utilisent le BMS partagé pour détecter les identités multiples. Le BMS partagé compare les modèles biométriques obtenus à partir de toute nouvelle donnée biométrique avec les modèles biométriques figurant déjà dans le BMS partagé afin de vérifier si des données appartenant à la même personne sont déjà stockées dans le CIR ou dans le SIS central.

3. Outre le processus visé au paragraphe 2, le CIR et le SIS central utilisent l'ESP pour effectuer des recherches dans les données stockées, respectivement, dans le SIS central et le CIR, à l'aide des données suivantes:

a) les noms, les prénoms, les noms à la naissance, les noms utilisés antérieurement et les pseudonymes,, le lieu de naissance, la date de naissance, le genre et toutes les nationalités possédées, tels que visés à l'article 20, paragraphe 3, du règlement (UE) 2018/1862;

b) le nom (nom de famille), les prénoms, la date de naissance, le lieu de naissance (ville et pays), la ou les nationalités et le genre, tels que visés à l'article 5, paragraphe 1, point a), du règlement (UE) 2019/816.

4. Outre le processus visé aux paragraphes 2 et 3, le CIR et le SIS central utilisent l'ESP pour effectuer des recherches dans les données stockées, respectivement, dans le SIS central et le CIR, à l'aide des données du document de voyage.

5. La détection d'identités multiples n'est lancée que pour comparer les données disponibles dans un système d'information de l'UE à celles qui sont disponibles dans d'autres systèmes d'information de l'UE.

Article 28

Résultats de la détection d'identités multiples

1. Lorsque la recherche visée à l'article 27, paragraphes 2, 3 et 4, ne génère aucune correspondance, les procédures visées à l'article 27, paragraphe 1, se poursuivent conformément aux instruments juridiques qui les régissent.

2. Lorsque la recherche visée à l'article 27, paragraphes 2, 3 et 4, génère une ou plusieurs correspondances, le CIR et, s'il y a lieu, le SIS créent un lien entre les données utilisées pour lancer la recherche et les données ayant déclenché la correspondance.

Lorsque plusieurs correspondances sont générées, un lien est créé entre toutes les données ayant déclenché la correspondance. Lorsque les données étaient déjà liées, le lien existant est étendu aux données utilisées pour lancer la recherche.

3. Lorsque la recherche visée à l'article 27, paragraphes 2, 3 et 4, génère une ou plusieurs correspondances et que les données d'identité des dossiers liés sont les mêmes ou similaires, un lien blanc est créé conformément à l'article 33.

4. Lorsque la recherche visée à l'article 27, paragraphes 2, 3 et 4, génère une ou plusieurs correspondances et que les données d'identité des dossiers liés ne peuvent pas être considérées comme similaires, un lien jaune est créé conformément à l'article 30 et la procédure visée à l'article 29 s'applique.

5. La Commission adopte des actes délégués conformément à l'article 69 fixant les procédures permettant de déterminer les cas dans lesquels les données d'identité peuvent être considérées comme étant les mêmes ou similaires

6. Les liens sont stockés dans le dossier de confirmation d'identité visé à l'article 34.

7. La Commission fixe, par voie d'actes d'exécution, en coopération avec l'eu-LISA, les règles techniques permettant de créer des liens entre les données de différents systèmes d'information de l'UE. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

Article 29

Vérification manuelle des différentes identités et autorités responsables

1. Sans préjudice du paragraphe 2, l'autorité chargée de la vérification manuelle des différentes identités est:

a)le bureau SIRENE de l'État membre en ce qui concerne les correspondances générées lors de la création ou de l'actualisation d'un signalement SIS conformément au règlement (UE) 2018/1862;

b)les autorités centrales de l'État membre de condamnation en ce qui concerne les correspondances générées lors de l'enregistrement ou de la modification de données dans l'ECRIS-TCN conformément à l'article 5 ou 9 du règlement (UE) 2019/816.

Le MID indique l'autorité chargée de de la vérification manuelle des différentes identités dans le dossier de confirmation d'identité.

2. L'autorité chargée de la vérification manuelle des différentes identités dans le dossier de confirmation d'identité est le bureau SIRENE de l'État membre qui a créé le signalement lorsqu'un lien est créé vers les données contenues dans un signalement concernant:

a)des personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition, visé à l'article 26 du règlement (UE) 2018/1862;

b)des personnes disparues ou vulnérables, visé à l'article 32 du règlement (UE) 2018/1862;

c)des personnes recherchées dans le but de rendre possible leur concours dans le cadre d'une procédure judiciaire, visé à l'article 34 du règlement (UE) 2018/1862;

d)des personnes aux fins de contrôles discrets, de contrôles d'investigation ou de contrôles spécifiques, visé à l'article 36 du règlement (UE) 2018/1862.

3. L'autorité chargée de la vérification manuelle des différentes identités a accès aux données liées figurant dans le dossier de confirmation d'identité pertinent et aux données d'identité liées figurant dans le CIR et, s'il y a lieu, dans le SIS. Elle évalue sans retard les différentes identités. Une fois cette évaluation réalisée, elle met à jour le lien conformément aux articles 31, 32 et 33, et l'ajoute sans retard au dossier de confirmation d'identité.

4. En cas de création de plusieurs liens, l'autorité chargée de la vérification manuelle des différentes identités évalue chaque lien séparément.

5. Lorsque des données générant une correspondance étaient déjà liées, l'autorité chargée de la vérification manuelle des différentes identités tient compte des liens existants lorsqu'elle envisage d'en créer de nouveaux.

Article 30

Lien jaune

1. Lorsque la vérification manuelle des différentes identités n'a pas encore eu lieu, un lien entre des données provenant d'au moins deux systèmes d'information de l'UE est classé comme jaune dans les cas suivants:

a)les données liées comportent les mêmes données biométriques mais ont des données d'identité similaires ou différentes;

b)les données liées ont des données d'identité différentes mais les données du document de voyage sont les mêmes, et au moins l'un des systèmes d'information de l'UE ne contient pas de données biométriques sur la personne concernée;

c)les données liées comportent les mêmes données d'identité mais ont des données biométriques différentes;

d)les données liées comportent des données d'identité similaires ou différentes, et ont les mêmes données du document de voyage, mais comportent des données biométriques différentes.

2. Lorsqu'un lien est classé comme jaune conformément au paragraphe 1, la procédure prévue à l'article 29 s'applique.

Article 31

Lien vert

1. Un lien entre des données provenant d'au moins deux systèmes d'information de l'UE est classé comme vert lorsque:

a)les données liées ont des données biométriques différentes mais comportent les mêmes données d'identité et l'autorité chargée de la vérification manuelle des différentes identités a conclu que les données liées désignent deux personnes différentes;

b)les données liées ont des données biométriques différentes, elles comportent des données d'identité similaires ou différentes, les données du document de voyage sont les mêmes et l'autorité chargée de la vérification manuelle des différentes identités a conclu que les données liées désignent deux personnes différentes;

c)les données liées ont des données d'identité différentes mais les données du document de voyage sont les mêmes, au moins un des systèmes d'information de l'UE ne contient pas de données biométriques sur la personne concernée, et l'autorité chargée de la vérification manuelle des différentes identités a conclu que les données liées désignent deux personnes différentes.

2. Lorsque le CIR ou le SIS sont interrogés et qu'il existe un lien vert entre des données figurant dans au moins deux systèmes d'information de l'UE, le MID indique que les données d'identité des données liées ne correspondent pas à la même personne.

3. Si une autorité d'un État membre dispose d'éléments de preuve suggérant qu'un lien vert a été enregistré de manière incorrecte dans le MID ou qu'un lien vert n'est pas à jour, ou que des données ont été traitées dans le MID ou les systèmes d'information de l'UE en violation du présent règlement, elle vérifie les données pertinentes stockées dans le CIR et le SIS et, si nécessaire, rectifie ou efface sans retard le lien du MID. L'autorité de l'État membre en question informe sans retard l'État membre responsable de la vérification manuelle des différentes identités.

Article 32

Lien rouge

1. Un lien entre des données provenant d'au moins deux systèmes d'information de l'UE est classé comme rouge dans les cas suivants:

a)les données liées comportent les mêmes données biométriques mais ont des données d'identité similaires ou différentes et l'autorité chargée de la vérification manuelle des différentes identités a conclu que les données liées désignent la même personne d'une manière injustifiée;

b)les données liées comportent les mêmes données d'identité ou des données d'identité similaires ou différentes et les mêmes données du document de voyage, mais les données biométriques sont différentes, et l'autorité chargée de la vérification manuelle des différentes identités a conclu que les données liées désignent deux personnes différentes, dont une au moins utilise le même document de voyage d'une manière injustifiée;

c)les données liées comportent les mêmes données d'identité mais ont des données biométriques différentes et les données du document de voyage sont différentes ou manquantes, et l'autorité chargée de la vérification manuelle des différentes identités a

conclu que les données liées désignent deux personnes différentes d'une manière injustifiée;

d) les données liées ont des données d'identité différentes, mais les données du document de voyage sont les mêmes, au moins un des systèmes d'information de l'UE ne contient pas de données biométriques sur la personne concernée et l'autorité chargée de la vérification manuelle des différentes identités a conclu que les données liées désignent la même personne d'une manière injustifiée.

2. Lorsque le CIR ou le SIS sont interrogés et qu'il existe un lien rouge entre des données figurant dans au moins deux systèmes d'information de l'UE, le MID indique les données visées à l'article 34. Les mesures à prendre pour donner suite à un lien rouge sont exécutées conformément au droit de l'Union et au droit national, toute conséquence juridique pour la personne concernée ne reposant que sur les données pertinentes concernant cette personne. Aucune conséquence juridique pour la personne concernée ne peut découler de la seule existence d'un lien rouge.

3. Lorsqu'un lien rouge est créé entre des données dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN, le dossier individuel stocké dans le CIR est mis à jour conformément à l'article 19, paragraphe 2.

4. Sans préjudice des dispositions relatives au traitement des signalements dans le SIS prévues dans les règlements (UE) 2018/1860, (UE) 2018/1861 et (UE) 2018/1862, et sans préjudice des restrictions nécessaires pour protéger la sécurité et l'ordre public, prévenir la criminalité et garantir qu'aucune enquête nationale ne sera compromise, lorsqu'un lien rouge est créé, l'autorité chargée de la vérification manuelle des différentes identités informe la personne concernée de la présence de données d'identités multiples illicites et lui fournit le numéro d'identification unique visé à l'article 34, point c), du présent règlement la référence de l'autorité chargée de la vérification manuelle des différentes identités visée à l'article 34, point d), du présent règlement et l'adresse internet du portail en ligne établi conformément à l'article 49 du présent règlement.

5. Les informations visées au paragraphe 4 sont fournies par écrit au moyen d'un formulaire type par l'autorité chargée de la vérification manuelle des différentes identités. La Commission détermine le contenu et la présentation de ce formulaire par la voie d'actes d'exécution. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

6. Lorsqu'un lien rouge est créé, le MID le notifie, de manière automatisée, aux autorités responsables des données liées.

7. Si une autorité d'un État membre ou une agence de l'Union ayant accès au CIR ou au SIS détient une preuve suggérant qu'un lien rouge a été enregistré de manière incorrecte dans le MID ou que les données ont été traitées dans le MID, le CIR ou le SIS en violation du présent règlement, cette autorité ou cette agence vérifie les données pertinentes stockées dans le CIR et le SIS et:

a) lorsque le lien se rapporte à l'un des signalements dans le SIS visés à l'article 29, paragraphe 2, informe immédiatement le bureau SIRENE de l'État membre concerné qui a

créé le signalement dans le SIS;

b) dans tous les autres cas, rectifie ou efface immédiatement le lien du MID.

Si un bureau SIRENE est contacté en vertu du premier alinéa, point a), il vérifie les preuves fournies par l'autorité de l'État membre ou l'agence de l'Union et, s'il y a lieu, rectifie ou efface immédiatement le lien du MID.

L'autorité de l'État membre qui a obtenu la preuve informe sans retard l'État membre responsable de la vérification manuelle des différentes identités de toute rectification ou suppression pertinente d'un lien rouge.

Article 33

Lien blanc

1. Un lien entre des données provenant d'au moins deux systèmes d'information de l'UE est classé comme blanc dans les cas suivants:

a) les données liées comportent les mêmes données biométriques et les mêmes données d'identité ou des données d'identité similaires;

b) les données liées comportent les mêmes données d'identité ou des données d'identité similaires, les mêmes données du document de voyage et au moins l'un des systèmes d'information de l'UE ne contient pas de données biométriques sur la personne concernée;

c) les données liées comportent les mêmes données biométriques, les mêmes données du document de voyage et des données d'identité similaires;

d) les données liées comportent les mêmes données biométriques mais ont des données d'identité similaires ou différentes et l'autorité chargée de la vérification manuelle des différentes identités a conclu que les données liées désignent la même personne d'une manière justifiée;

2. Lorsque le CIR ou le SIS sont interrogés et qu'il existe un lien blanc entre des données figurant au moins deux systèmes d'information de l'UE, le MID indique que les données d'identité des données liées correspondent à la même personne. Les systèmes d'information de l'UE interrogés fournissent une réponse indiquant, le cas échéant, toutes les données liées sur la personne, déclenchant ainsi une correspondance au regard des données liées par le lien blanc, si l'autorité qui a lancé la recherche a accès aux données liées en vertu du droit de l'Union ou du droit national.

3. Lorsqu'un lien blanc est créé entre des données dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN, le dossier individuel stocké dans le CIR est mis à jour conformément à l'article 19, paragraphe 2.

4. Sans préjudice des dispositions relatives au traitement des signalements dans le SIS contenues dans les règlements (UE) 2018/1860, (UE) 2018/1861 et (UE) 2018/1862, et sans préjudice des restrictions nécessaires pour protéger la sécurité et l'ordre public, prévenir la criminalité et garantir qu'aucune enquête nationale ne sera compromise, lorsqu'un lien blanc est créé à la suite d'une vérification manuelle

des différentes identités, l'autorité chargée de la vérification manuelle des différentes identités informe la personne concernée de la présence de données d'identité similaires ou différentes et lui fournit le numéro d'identification unique visé à l'article 34, point c), du présent règlement, la référence de l'autorité chargée de la vérification manuelle des différentes identités visée à l'article 34, point d), du présent règlement et l'adresse internet du portail en ligne établi conformément à l'article 49 du présent règlement.

5. Si une autorité d'un État membre dispose d'éléments de preuve suggérant qu'un lien blanc a été enregistré dans le MID de manière incorrecte ou qu'un lien blanc n'est pas à jour, ou que des données ont été traitées dans le MID ou les systèmes d'information de l'UE en violation du présent règlement, elle vérifie les données pertinentes stockées dans le CIR et le SIS et, si nécessaire, rectifie ou efface sans retard le lien du MID. L'autorité de l'État membre en question informe sans retard l'État membre responsable de la vérification manuelle des différentes identités.

6. Les informations visées au paragraphe 4 sont fournies par écrit au moyen d'un formulaire type par l'autorité chargée de la vérification manuelle des différentes identités. La Commission détermine le contenu et la présentation de ce formulaire par la voie d'actes d'exécution. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

Article 34

Dossier de confirmation d'identité

Le dossier de confirmation d'identité contient les données suivantes:

a) les liens visés aux articles 30 à 33;

b) une référence aux systèmes d'information de l'UE contenant les données liées;

c) un numéro d'identification unique permettant d'extraire, des systèmes d'information de l'UE correspondants, les données liées;

d) l'autorité responsable de la vérification manuelle des différentes identités;

e) la date de création du lien ou toute mise à jour de celui-ci.

Article 35

Conservation des données dans le détecteur d'identités multiples

Les dossiers de confirmation d'identité et leurs données, y compris les liens, ne sont stockés dans le MID qu'aussi longtemps que les données liées sont stockées dans au moins deux systèmes d'information de l'UE. Ils sont effacés du MID de manière automatisée.

Article 36

Tenue de registres

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

a) l'État membre qui lance la requête;

b) la finalité de l'accès par l'utilisateur;

c) la date et l'heure de la requête;

d) le type de données utilisées pour lancer la requête;

e) la référence aux données liées;

f) l'historique du dossier de confirmation d'identité.

2. Chaque État membre tient des registres des requêtes introduites par ses autorités et le personnel de ces autorités dûment autorisé à utiliser le MID. Chaque agence de l'Union tient des registres des requêtes introduites par son personnel dûment autorisé.

3. Les registres visés aux paragraphes 1 et 2 ne peuvent être utilisés que pour contrôler la protection des données, y compris vérifier l'admissibilité d'une requête et la licéité du traitement des données, et pour garantir la sécurité et l'intégrité des données. Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création. Cependant, s'ils sont nécessaires à des procédures de contrôle qui ont déjà été engagées, ils sont effacés dès qu'ils ne sont plus nécessaires aux procédures de contrôle.

CHAPITRE VI

Mesures soutenant l'interopérabilité

Article 37

Qualité des données

1. Sans préjudice des responsabilités des États membres en ce qui concerne la qualité des données introduites dans les systèmes, l'eu-LISA met en place des mécanismes et des procédures automatisés de contrôle de la qualité des données pour les données stockées dans le SIS, Eurodac, l'ECRIS-TCN, le BMS partagé et le CIR.

2. L'eu-LISA met en œuvre des mécanismes d'évaluation de l'exactitude du BMS partagé, des indicateurs communs de qualité des données et des normes de qualité minimales pour le stockage de données dans le SIS, Eurodac, l'ECRIS-TCN, le BMS partagé et le CIR.

Seules les données répondant aux normes de qualité minimales peuvent être introduites dans le SIS, Eurodac, l'ECRIS-TCN, le BMS partagé, le CIR et le MID.

3. L'eu-LISA présente aux États membres des rapports réguliers sur les mécanismes et procédures automatisés de contrôle de la qualité des données et les

indicateurs communs de qualité des données. L'eu-LISA fournit également à la Commission un rapport régulier sur les problèmes rencontrés et les États membres concernés. L'eu-LISA fournit également ce rapport au Parlement européen et au Conseil à leur demande. Aucun des rapports visés au présent paragraphe ne contient de données à caractère personnel.

4. Les détails des mécanismes et procédures automatisés de contrôle de la qualité des données, des indicateurs communs de qualité des données et des normes de qualité minimales pour le stockage de données dans le SIS, Eurodac, l'ECRIS-TCN, le BMS partagé et le CIR, notamment en ce qui concerne les données biométriques, sont définis dans des actes d'exécution. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

5. Un an après la mise en place des mécanismes et procédures automatisés de contrôle de la qualité des données, des indicateurs communs de qualité des données et des normes minimales de qualité des données, puis tous les ans, la Commission évalue la mise en œuvre de la qualité des données par les États membres et formule les recommandations nécessaires en la matière. Les États membres fournissent à la Commission un plan d'action visant à remédier aux manquements constatés dans le rapport d'évaluation et, notamment, aux problèmes de qualité des données découlant de données erronées figurant dans les systèmes d'information de l'UE. Les États membres font régulièrement rapport à la Commission sur les progrès réalisés au regard de ce plan d'action jusqu'à ce que celui-ci soit entièrement mis en œuvre.

La Commission transmet le rapport d'évaluation au Parlement européen, au Conseil, au Contrôleur européen de la protection des données, au comité européen de la protection des données et à l'Agence des droits fondamentaux de l'Union européenne instituée par le règlement (CE) nº 168/2007 du Conseil [37].

Article 38

Format universel pour les messages

1. La norme de format universel pour les messages (UMF) est établie. L'UMF définit les normes applicables à certains éléments du contenu des échanges d'informations transfrontières entre les systèmes d'information, les autorités ou les organismes dans le domaine de la justice et des affaires intérieures.

2. La norme UMF est utilisée pour le développement d'Eurodac, de l'ECRIS-TCN, de l'ESP, du CIR, du MID et, au besoin, pour l'élaboration, par l'eu-LISA ou par toute autre agence de l'Union, de nouveaux modèles d'échange d'informations et systèmes d'information dans le domaine de la justice et des affaires intérieures.

3. La Commission adopte un acte d'exécution pour définir et élaborer la norme UMF visée au paragraphe 1 du présent article. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

Article 39

Répertoire central des rapports et statistiques

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.

2. L'eu-LISA établit, met en œuvre et héberge sur ses sites techniques le CRRS, contenant les données et les statistiques visées à l'article 74 du règlement (UE) 2018/1862 et à l'article 32 du règlement (UE) 2019/816, séparées logiquement par système d'information de l'UE. L'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 et à l'article 32 du règlement (UE) 2019/816.

3. L'eu-LISA anonymise les données et enregistre ces données anonymisées dans le CRRS. Le processus d'anonymisation des données est automatisé.

Les données contenues dans le CRRS ne permettent pas l'identification des personnes.

4. Le CRRS se compose des éléments suivants:

a) les outils nécessaires à l'anonymisation des données;

b) une infrastructure centrale, comprenant un répertoire de données anonymes;

c) une infrastructure de communication sécurisée pour connecter le CRRS au SIS, à Eurodac et à l'ECRIS-TCN, ainsi qu'aux infrastructures centrales du BMS partagé, du CIR et du MID.

5. La Commission adopte un acte délégué conformément à l'article 69 fixant des règles détaillées concernant le fonctionnement du CRRS, notamment des garanties spécifiques pour le traitement des données à caractère personnel dans le cadre des paragraphes 2 et 3 du présent article, ainsi que des règles de sécurité applicables au répertoire.

CHAPITRE VII

Protection des données

Article 40

Responsable du traitement des données

1. En ce qui concerne le traitement des données dans le BMS partagé, les autorités des États membres qui sont responsables du traitement pour Eurodac, le SIS et l'ECRIS-TCN, respectivement, sont les responsables du traitement au sens de l'article 4, point 7), du règlement (UE) 2016/679 ou de l'article 3, point 8), de la

directive (UE) 2016/680 en ce qui concerne les modèles biométriques obtenus à partir des données visées à l'article 13 du présent règlement qu'elles introduisent dans les systèmes sous-jacents et sont chargées du traitement des modèles biométriques dans le BMS partagé.

2. En ce qui concerne le traitement des données dans le CIR, les autorités des États membres qui sont responsables du traitement pour Eurodac et l'ECRIS-TCN, respectivement, sont les responsables du traitement au sens de l'article 4, point 7), du règlement (UE) 2016/679 ou de l'article 3, point 8), de la directive (UE) 2016/680 en ce qui concerne les données visées à l'article 18 du présent règlement qu'elles introduisent dans les systèmes sous-jacents et sont chargées du traitement de ces données à caractère personnel dans le CIR.

3. En ce qui concerne le traitement des données dans le MID:

a) l'Agence européenne de garde-frontières et de garde-côtes est le responsable du traitement au sens de l'article 3, point 8), du règlement (UE) 2018/1725 en ce qui concerne le traitement des données à caractère personnel par l'unité centrale ETIAS.

b) les autorités des États membres qui ajoutent des données dans le dossier de confirmation d'identité ou en modifient les données sont les responsables du traitement au sens de l'article 4, point 7), du règlement (UE) 2016/679 ou de l'article 3, point 8), de la directive (UE) 2016/680 et sont chargées du traitement des données à caractère personnel dans le MID.

4. Aux fins du contrôle de la protection des données, y compris la vérification de l'admissibilité d'une requête et de la licéité du traitement des données, les responsables du traitement ont accès aux registres visés aux articles 10, 16, 24 et 36 en vue de l'autocontrôle visé à l'article 44.

Article 41

Sous-traitant

En ce qui concerne le traitement des données à caractère personnel dans le BMS partagé, le CIR et le MID, l'eu-LISA est le sous-traitant au sens de l'article 3, point 12) a), du règlement (UE) 2018/1725.

Article 42

Sécurité du traitement

1. L'eu-LISA, l'unité centrale ETIAS, Europol et les autorités des États membres veillent à la sécurité des opérations de traitement de données à caractère personnel effectuées en vertu du présent règlement. L'eu-LISA, l'unité centrale ETIAS, Europol et les autorités des États membres coopèrent pour l'exécution des tâches liées à la sécurité.

2. Sans préjudice de l'article 33 du règlement (UE) 2018/1725, l'eu-LISA prend les mesures nécessaires pour assurer la sécurité des éléments d'interopérabilité et de leurs infrastructures de communication qui y sont liées.

3. En particulier, l'eu-LISA adopte les mesures nécessaires, y compris un plan de sécurité, un plan de continuité des activités et un plan de rétablissement après sinistre, afin:

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

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

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

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

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

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

g) de garantir que les personnes autorisées à avoir accès aux éléments d'interopérabilité n'ont accès qu'aux données couvertes par leur autorisation d'accès, uniquement grâce à l'attribution d'identifiants individuels et à des modes d'accès confidentiels;

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

i) de garantir la possibilité de vérifier et d'établir quelles données ont été traitées dans les éléments d'interopérabilité, à quel moment, par qui et dans quel but;

j) d'empêcher toute lecture, copie, modification ou tout effacement non autorisés de données à caractère personnel pendant leur transmission à partir des éléments d'interopérabilité ou vers ceux-ci, ou durant le transport de supports de données, en particulier au moyen de 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 des éléments d'interopérabilité 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 avancées technologiques.

4. Les États membres, Europol et l'unité centrale ETIAS prennent des mesures équivalentes à celles visées au paragraphe 3 en ce qui concerne la sécurité du

traitement des données à caractère personnel par les autorités ayant un droit d'accès à l'un des éléments d'interopérabilité.

Article 43

Incidents de sécurité

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

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

3. Sans préjudice de la notification et de la communication de toute violation de données à caractère personnel en application de l'article 33 du règlement (UE) 2016/679, de l'article 30 de la directive (UE) 2016/680 ou de ces deux dispositions, les États membres notifient sans retard tout incident de sécurité à la Commission, à l'eu-LISA, aux autorités de contrôle compétentes et au Contrôleur européen de la protection des données.

Sans préjudice des articles 34 et 35 du règlement (UE) 2018/1725 et de l'article 34 du règlement (UE) 2016/794, l'unité centrale ETIAS et Europol notifient sans retard tout incident de sécurité à la Commission, à l'eu-LISA et au Contrôleur européen de la protection des données.

En cas d'incident de sécurité concernant l'infrastructure centrale des éléments d'interopérabilité, l'eu-LISA le notifie à la Commission et au Contrôleur européen de la protection des données sans retard.

4. Les informations relatives à un incident de sécurité ayant ou pouvant avoir un impact sur le fonctionnement des éléments d'interopérabilité, ou sur la disponibilité, l'intégrité et la confidentialité des données, sont communiquées sans retard aux États membres, à l'unité centrale ETIAS et à Europol et consignées conformément au plan de gestion des incidents qui doit être élaboré par l'eu-LISA.

5. Les États membres concernés, l'unité centrale ETIAS, Europol et l'eu-LISA coopèrent en cas d'incident de sécurité. La Commission établit les modalités de cette procédure de coopération au moyen d'actes d'exécution. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

Article 44

Autocontrôle

Les États membres et les agences de l'Union concernées veillent à ce que chaque autorité habilitée à avoir accès aux éléments d'interopérabilité prenne les mesures nécessaires pour vérifier qu'elle respecte le présent règlement et coopère, au besoin, avec l'autorité de contrôle.

Les responsables du traitement visés à l'article 40 prennent les mesures nécessaires afin de contrôler la conformité des opérations de traitement des données au regard du présent règlement, notamment en vérifiant fréquemment les registres visés aux articles 10, 16, 24 et 36, et coopèrent, au besoin, avec les autorités de contrôle et avec le Contrôleur européen de la protection des données.

Article 45

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 46

Responsabilité

1. Sans préjudice du droit à réparation de la part du responsable du traitement ou du sous-traitant et de la responsabilité de ceux-ci au titre du règlement (UE) 2016/679, de la directive (UE) 2016/680 et du règlement (UE) 2018/1725:

a) toute personne ou tout État membre ayant subi un dommage matériel ou moral du fait d'une opération illicite de traitement de données à caractère personnel ou de tout autre acte incompatible avec le présent règlement de la part d'un État membre a le droit d'obtenir réparation dudit État membre;

b) toute personne ou tout État membre ayant subi un dommage matériel ou moral du fait de tout acte d'Europol, de l'Agence européenne de garde-frontières et de garde-côtes ou de l'eu-LISA incompatible avec le présent règlement a le droit d'obtenir réparation de l'agence en question.

L'État membre concerné, Europol, l'Agence européenne de garde-frontières et de garde-côtes ou l'eu-LISA sont exonérés, totalement ou partiellement, de leur responsabilité en vertu du premier alinéa s'ils prouvent que le fait générateur du dommage ne leur est pas imputable.

2. Si le non-respect, par un État membre, des obligations qui lui incombent au titre du présent règlement cause un dommage aux éléments d'interopérabilité, cet État membre en est tenu pour responsable, sauf si, et dans la mesure où, l'eu-LISA 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.

3. Les actions en réparation intentées à l'encontre d'un État membre pour les dommages visés aux paragraphes 1 et 2 sont régies par le droit national de l'État membre défendeur. Les actions en réparation intentées contre le responsable du traitement ou l'eu-LISA pour les dommages visés aux paragraphes 1 et 2 s'entendent sous réserve des conditions prévues dans les traités.

Article 47

Droit à l'information

1. L'autorité qui collecte les données à caractère personnel à stocker dans le BMS partagé, le CIR ou le MID fournit aux personnes dont les données sont collectées les informations requises en vertu des articles 13 et 14 du règlement (UE) 2016/679, des articles 12 et 13 de la directive (UE) 2016/680 et des articles 15 et 16 du règlement (UE) 2016/1725. L'autorité fournit les informations au moment de la collecte de ces données.

2. Toutes les informations sont mises à disposition, en des termes clairs et simples, dans une version linguistique que la personne concernée comprend ou dont on peut raisonnablement supposer qu'elle la comprend. Cela s'applique également à la fourniture d'informations de manière appropriée en fonction de l'âge des personnes concernées mineures.

3. Les règles relatives au droit à l'information figurant dans les règles applicables de l'Union en matière de protection des données s'appliquent aux données à caractère personnel qui sont enregistrées dans l'ECRIS-TCN et qui font l'objet d'un traitement aux fins du présent règlement.

Article 48

Droit d'accès aux données à caractère personnel stockées dans le MID et droits de rectification, d'effacement et de limitation du traitement de ces données

1. Pour exercer ses droits au titre des articles 15 à 18 du règlement (UE) 2016/679, des articles 17 à 20 du règlement (UE) 2018/1725 et des articles 14, 15 et 16 de la directive (UE) 2016/680, toute personne a le droit de s'adresser à l'autorité compétente de tout État membre qui examine la demande et y répond.

2. L'État membre qui examine cette demande répond sans retard injustifié et, en tout état de cause, dans un délai de quarante-cinq jours à compter de la réception de celle-ci. Au besoin, ce délai peut être prolongé de 15 jours, compte tenu de la complexité et du nombre de demandes. L'État membre qui examine la demande informe la personne concernée de cette prolongation et des motifs du report dans un délai de quarante-cinq jours à compter de la réception de la demande. Les États membres peuvent décider que les réponses sont données par des services centraux.

3. Si une demande de rectification ou d'effacement de données à caractère personnel est présentée à un État membre autre que l'État membre responsable de la vérification manuelle des différentes identités, l'État membre auquel la demande a

été présentée prend contact avec les autorités de l'État membre responsable de la vérification manuelle des différentes identités dans un délai de sept jours. L'État membre responsable de la vérification manuelle des différentes identités vérifie l'exactitude des données et la licéité du traitement des données sans retard injustifié et, en tout état de cause, dans un délai de trente jours à compter de cette prise de contact. Au besoin, ce délai peut être prolongé de 15 jours, compte tenu de la complexité et du nombre de demandes. L'État membre responsable de la vérification manuelle des différentes identités informe l'État membre qui l'a contacté de toute prolongation et des motifs du report. La personne concernée est informée de la suite de la procédure par l'État membre qui a contacté l'autorité de l'État membre responsable de la vérification manuelle des différentes identités.

4. Si une demande de rectification ou d'effacement de données à caractère personnel est présentée à un État membre dans lequel l'unité centrale ETIAS était responsable de la vérification manuelle des différentes identités, l'État membre auquel la demande a été présentée prend contact avec l'unité centrale ETIAS dans un délai de sept jours et demande son avis. L'unité centrale ETIAS donne son avis sans retard injustifié et, en tout état de cause, dans un délai de trente jours à compter de cette prise de contact. Au besoin, ce délai peut être prolongé de 15 jours, compte tenu de la complexité et du nombre de demandes. La personne concernée est informée de la suite de la procédure par l'État membre qui a contacté l'unité centrale ETIAS.

5. Lorsque, à la suite d'un examen, il apparaît que les données stockées dans le MID sont erronées ou y ont été enregistrées de façon illicite, l'État membre responsable de la vérification manuelle des différentes identités ou, lorsqu'aucun État membre n'était responsable de la vérification manuelle des différentes identités ou que l'unité centrale ETIAS était responsable de la vérification manuelle des différentes identités, l'État membre auquel la demande a été présentée rectifie ou efface ces données sans retard injustifié. La personne concernée est informée par écrit de la rectification ou de l'effacement de ses données.

6. Lorsque des données stockées dans le MID sont modifiées par un État membre au cours de leur période de conservation, cet État membre procède au traitement prévu à l'article 27 et, selon le cas, à l'article 29 afin de déterminer si les données modifiées doivent être liées. Lorsque le traitement ne génère aucune correspondance, cet État membre efface les données du dossier de confirmation d'identité. Lorsque le traitement automatisé génère une ou plusieurs correspondances, cet État membre crée ou met à jour le lien correspondant conformément aux dispositions pertinentes du présent règlement.

7. Lorsque l'État membre responsable de la vérification manuelle des différentes identités ou, le cas échéant, l'État membre auquel la demande a été présentée n'estime pas que les données stockées dans le MID sont erronées ou y ont été enregistrées de façon illicite, il prend une décision de nature administrative indiquant par écrit et sans retard à la personne concernée les raisons pour lesquelles il n'est pas disposé à rectifier ou à effacer les données la concernant.

8. La décision visée au paragraphe 7 fournit également à la personne concernée des précisions sur la possibilité de contester la décision prise au sujet de la demande d'accès aux données à caractère personnel, de rectification, d'effacement ou de limitation du traitement de ces données et, s'il y a lieu, des informations sur les modalités de recours ou de plainte devant les autorités ou les juridictions compétentes, ainsi que sur toute aide disponible, y compris de la part des autorités de contrôle.

9. Toute demande d'accès aux données à caractère personnel, de rectification, d'effacement ou de limitation du traitement de ces données comporte les informations nécessaires à l'identification de la personne concernée. Ces informations sont utilisées exclusivement pour permettre l'exercice des droits visés au présent article et sont ensuite immédiatement effacées.

10. L'État membre responsable de la vérification manuelle des différentes identités ou, le cas échéant, l'État membre auquel la demande a été présentée consigne, dans un document écrit, le fait qu'une demande d'accès à des données à caractère personnel, de rectification, d'effacement ou de limitation du traitement de telles données a été présentée et la manière dont cette demande a été traitée, et met sans retard ce document à la disposition des autorités de contrôle.

11. Le présent article s'applique sans préjudice des limitations et restrictions aux droits énoncés dans le présent article prévues par le règlement (UE) 2016/679 et la directive (UE) 2016/680.

Article 49

Portail en ligne

1. Un portail en ligne est créé pour faciliter l'exercice des droits d'accès aux données à caractère personnel, de rectification, d'effacement ou de limitation du traitement de telles données.

2. Le portail en ligne comporte des informations sur les droits et les procédures visés aux articles 47 et 48 ainsi qu'une interface utilisateur permettant aux personnes dont les données sont traitées dans le MID et qui ont été informées de la présence d'un lien rouge conformément à l'article 32, paragraphe 4, de recevoir les coordonnées de l'autorité compétente de l'État membre responsable de la vérification manuelle des différentes identités.

3. Pour obtenir les coordonnées de l'autorité compétente de l'État membre responsable de la vérification manuelle des différentes identités, la personne dont les données sont traitées dans le MID devrait indiquer la référence de l'autorité responsable de la vérification manuelle des différentes identités visée à l'article 34, point d). Le portail en ligne utilise cette référence pour extraire les coordonnées de l'autorité compétente de l'État membre responsable de la vérification manuelle des différentes identités. Le portail en ligne comporte également un modèle de courriel destiné à faciliter la communication entre l'utilisateur du portail et l'autorité compétente de l'État membre responsable de la vérification manuelle des

différentes identités. Ce courriel comporte un champ destiné au numéro d'identification unique visé à l'article 34, point c), afin de permettre à l'autorité compétente de l'État membre responsable de la vérification manuelle des différentes identités d'identifier les données concernées.

4. Les États membres communiquent à l'eu-LISA les coordonnées de toutes les autorités compétentes pour examiner toute demande visée aux articles 47 et 48 et pour y répondre et vérifient régulièrement que ces coordonnées sont à jour.

5. L'eu-LISA développe le portail en ligne et en assure la gestion technique.

6. La Commission adopte un acte délégué conformément à l'article 69 afin de fixer des règles détaillées sur le fonctionnement du portail en ligne, y compris l'interface utilisateur, les langues dans lesquelles le portail est disponible ainsi que le modèle de courriel.

Article 50

Communication de données à caractère personnel vers des pays tiers, à des organisations internationales et à des entités privées

Sans préjudice de l'article 31 du règlement (CE) n° 767/2008, des articles 25 et 26 du règlement (UE) 2016/794, de l'article 41 du règlement (UE) 2017/2226, de l'article 65 du règlement (UE) 2018/1240 et de l'interrogation des bases de données d'Interpol via l'ESP conformément à l'article 9, paragraphe 5, du présent règlement, qui respectent les dispositions du chapitre V du règlement (UE) 2018/1725 et du chapitre V du règlement (UE) 2016/679, les données à caractère personnel stockées dans les éléments d'interopérabilité, traitées ou accessibles par ces éléments, ne peuvent être transférées vers un pays tiers, à une organisation internationale ou à une entité privée, ni être mises à leur disposition.

Article 51

Contrôle par les autorités de contrôle

1. Chaque État membre veille à ce que les autorités de contrôle contrôlent en toute indépendance la licéité du traitement des données à caractère personnel dans le cadre du présent règlement par l'État membre concerné, y compris de leur transmission à partir des éléments d'interopérabilité et vers ceux-ci.

2. Chaque État membre veille à ce que les dispositions législatives, réglementaires et administratives nationales qu'il a adoptées en application de la directive (UE) 2016/680 s'appliquent aussi, s'il y a lieu, à l'accès aux éléments d'interopérabilité par les services de police et les autorités désignées, y compris pour ce qui est des droits des personnes aux données desquelles l'accès a ainsi été donné.

3. Les autorités de contrôle veillent à ce que les autorités nationales responsables réalisent, tous les quatre ans au minimum, aux fins du présent règlement, un audit

des opérations de traitement des données à caractère personnel, conformément aux normes internationales d'audit applicables.

Les autorités de contrôle publient chaque année le nombre de demandes visant à faire rectifier ou effacer des données à caractère personnel, ou à en faire limiter le traitement, les mesures prises par la suite et le nombre de rectifications et d'effacements auxquels il a été procédé et de limitations apportées au traitement, en réponse aux demandes des personnes concernées.

4. Les États membres veillent à ce que leurs autorités de contrôle disposent de ressources et d'expertise suffisantes pour s'acquitter des tâches qui leur sont confiées en vertu du présent règlement.

5. Les États membres communiquent toutes les informations demandées par une autorité de contrôle visée à l'article 51, paragraphe 1, du règlement (UE) 2016/679 et lui fournissent, en particulier, des informations relatives aux activités menées dans l'exercice de leurs fonctions au titre du présent règlement. Les États membres octroient aux autorités de contrôle visées à l'article 51, paragraphe 1, du règlement (UE) 2016/679 l'accès à leurs registres visés aux articles 10, 16, 24 et 36 du présent règlement, aux justifications visées à l'article 22, paragraphe 2, du présent règlement et leur permettent d'accéder, à tout moment, à l'ensemble de leurs locaux utilisés à des fins d'interopérabilité.

Article 52

Audits par le Contrôleur européen de la protection des données

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, l'unité centrale ETIAS et Europol, conformément aux normes internationales applicables en matière d'audit. Ce rapport d'audit est communiqué au Parlement européen, au Conseil, à l'eu-LISA, à la Commission, aux États membres et aux agences de l'Union concernées. L'eu-LISA, l'unité centrale ETIAS et Europol ont la possibilité de formuler des observations avant l'adoption des rapports.

L'eu-LISA et l'unité centrale ETIAS fournissent 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 10, 16, 24 et 36, et lui permettent d'accéder, à tout moment, à l'ensemble de leurs locaux.

Article 53

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

1. Les autorités de contrôle et le Contrôleur européen de la protection des données, agissant chacun dans les limites de leurs compétences respectives, coopèrent activement dans le cadre de leurs responsabilités respectives et assurent

un contrôle coordonné de l'utilisation des éléments d'interopérabilité et de l'application d'autres dispositions 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 des éléments d'interopérabilité.

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

3. Le comité européen de la protection des données envoie un rapport d'activités conjoint au Parlement européen, au Conseil, à la Commission, à Europol, à l'Agence européenne de garde-frontières et de garde-côtes et à l'eu-LISA au plus tard le 12 juin 2021 puis tous les deux ans. Ce rapport comporte un chapitre sur chaque État membre, établi par l'autorité de contrôle de l'État membre concerné.

CHAPITRE VIII
Responsabilités

Article 54

Responsabilités de l'eu-LISA durant la phase de conception et de développement

1. L'eu-LISA veille à ce que le fonctionnement des infrastructures centrales des éléments d'interopérabilité soit conforme au présent règlement.

2. Les éléments d'interopérabilité sont hébergés par l'eu-LISA sur ses sites techniques et fournissent les fonctionnalités prévues dans le présent règlement conformément aux conditions de sécurité, de disponibilité, de qualité et de performance visées à l'article 55, paragraphe 1.

3. L'eu-LISA est responsable du développement des éléments d'interopérabilité, de toutes les adaptations nécessaires pour établir l'interopérabilité entre les systèmes centraux de l'EES, du VIS, de l'ETIAS, du SIS, d'Eurodac, et de l'ECRIS-TCN ainsi que de l'ESP, du BMS partagé, du CIR, du MID et du CRRS.

Sans préjudice de l'article 62, l'eu-LISA n'a accès à aucune des données à caractère personnel traitées via l'ESP, le BMS partagé, le CIR ou le MID.

L'eu-LISA définit la conception de l'architecture matérielle des éléments d'interopérabilité, y compris leur infrastructure de communication, ainsi que les spécifications techniques et leur évolution en ce qui concerne l'infrastructure centrale et l'infrastructure de communication sécurisée, qui est adoptée par le conseil d'administration après avis favorable de la Commission. L'eu-LISA met également en œuvre tout aménagement éventuellement nécessaire du SIS, d'Eurodac ou de l'ECRIS-TCN, résultant de l'établissement de l'interopérabilité et prévu par le présent règlement.

L'eu-LISA développe et met en œuvre les éléments d'interopérabilité dès que possible après l'entrée en vigueur du présent règlement et l'adoption par la Commission des mesures prévues à l'article 8, paragraphe 2, à l'article 9, paragraphe 7, à l'article 28, paragraphes 5 et 7, à l'article 37, paragraphe 4, à l'article 38, paragraphe 3, à l'article 39, paragraphe 5, à l'article 43, paragraphe 5 et à l'article 74, paragraphe 10.

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

4. Pendant la phase de conception et de développement, un conseil de gestion du programme, composé d'un maximum de 10 membres, est créé. Il est constitué de sept membres nommés par le conseil d'administration de l'eu-LISA parmi ses membres ou ses suppléants, du président du groupe consultatif sur l'interopérabilité visé à l'article 71, d'un membre représentant l'eu-LISA désigné par son directeur exécutif et d'un membre désigné par la Commission. Les membres nommés par le conseil d'administration de l'eu-LISA sont choisis uniquement parmi les États membres qui sont pleinement liés, en vertu du droit de l'Union, par les instruments juridiques régissant le développement, la création, le fonctionnement et l'utilisation de tous les systèmes d'information de l'UE et qui participeront aux éléments d'interopérabilité.

5. Le conseil de gestion du programme se réunit régulièrement et au moins trois fois par trimestre. Il veille à la bonne gestion de la phase de conception et de développement des éléments d'interopérabilité.

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.

6. Le conseil d'administration de l'eu-LISA définit le règlement intérieur du conseil de gestion du programme, qui comprend notamment des règles sur:

a) la présidence;

b) les lieux de réunion;

c) la préparation des réunions;

d) l'admission d'experts aux réunions;

e) les plans de communication garantissant que les membres du conseil d'administration non participants soient pleinement informés.

La présidence est exercée par un État membre qui est pleinement lié, en vertu du droit de l'Union, par les instruments juridiques régissant le développement, la création, le fonctionnement et l'utilisation de tous les systèmes d'information de l'UE et qui participera aux éléments d'interopérabilité.

Tous les frais de voyage et de séjour exposés par les membres du conseil de gestion du programme sont pris en charge par l'eu-LISA et l'article 10 du règlement intérieur de l'eu-LISA s'applique mutatis mutandis. Le secrétariat du conseil de gestion du programme est assuré par l'eu-LISA.

Le groupe consultatif sur l'interopérabilité visé à l'article 71 se réunit régulièrement jusqu'à la mise en service des éléments d'interopérabilité. 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 55

Responsabilités de l'eu-LISA après la mise en service

1. Après la mise en service de chaque élément d'interopérabilité, l'eu-LISA est responsable de la gestion technique de l'infrastructure centrale des éléments d'interopérabilité, y compris leur maintenance et leurs 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 visée aux articles 6, 12, 17, 25 et 39.

La gestion technique des éléments d'interopérabilité comprend toutes les tâches et solutions techniques nécessaires au fonctionnement des éléments d'interopérabilité et la fourniture continue de services aux États membres et aux agences de l'Union, 24 heures sur 24, 7 jours sur 7, conformément au présent règlement. Elle comprend, en particulier, les travaux de maintenance et les perfectionnements techniques indispensables pour que les éléments d'interopérabilité fonctionnent à un niveau satisfaisant de qualité technique, notamment quant au temps de réponse pour l'interrogation des infrastructures centrales, conformément aux spécifications techniques.

Tous les éléments d'interopérabilité sont élaborés et gérés de manière à assurer un accès rapide, continu, efficace et contrôlé aux éléments et données stockés dans le MID, le BMS partagé et le CIR ainsi que leur disponibilité totale et ininterrompue, et un temps de réponse adapté aux besoins opérationnels des autorités des États membres et des agences de l'Union.

2. Sans préjudice de l'article 17 du statut des fonctionnaires de l'Union européenne, 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 les données stockées dans les éléments d'interopérabilité. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après la cessation de leur activité.

Sans préjudice de l'article 62, l'eu-LISA n'a accès à aucune des données à caractère personnel traitées via l'ESP, le BMS partagé, le CIR et le MID.

3. L'eu-LISA élabore et gère un mécanisme et des procédures de contrôle de la qualité des données stockées dans le BMS partagé et dans le CIR, conformément à l'article 37.

4. L'eu-LISA s'acquitte aussi des tâches liées à l'offre d'une formation relative à l'utilisation technique des éléments d'interopérabilité.

Article 56

Responsabilités des États membres

1. Chaque État membre est responsable:

a) de la connexion à l'infrastructure de communication de l'ESP et du CIR;

b) de l'intégration des systèmes et infrastructures nationaux existants avec l'ESP, le CIR et le MID;

c) de l'organisation, de la gestion, du fonctionnement et de la maintenance de son infrastructure nationale existante et de sa connexion aux éléments d'interopérabilité;

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

e) de l'adoption des mesures législatives visées à l'article 20, paragraphes 5 et 6, afin d'octroyer l'accès au CIR à des fins d'identification;

f) de la vérification manuelle des différentes identités, visée à l'article 29;

g) du respect des exigences en matière de qualité des données établies au titre du droit de l'Union;

h) du respect des règles applicables à chaque système d'information de l'UE en ce qui concerne la sécurité et l'intégrité des données à caractère personnel;

i) de la correction des manquements constatés dans le rapport d'évaluation de la Commission concernant la qualité des données visé à l'article 37, paragraphe 5.

2. Chaque État membre connecte au CIR ses autorités désignées.

Article 57

Responsabilités d'Europol

1. Europol assure le traitement des interrogations des données d'Europol par l'ESP. Europol adapte en conséquence son interface d'interrogation des systèmes d'Europol (Querying Europol Systems – QUEST) pour les données nécessitant un niveau de protection de base (basic protection level – BPL).

2. Europol est responsable de la gestion de l'accès et des modalités de l'accès à l'ESP et au CIR et de leur utilisation par son personnel dûment autorisé, dans le

cadre du 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.

Article 58

Responsabilités de l'unité centrale ETIAS

L'unité centrale ETIAS est responsable:

a) de la vérification manuelle des différentes identités conformément à l'article 29;

b) de la détection d'identités multiples entre les données stockées dans l'EES, le VIS, Eurodac et le SIS, visée à l'article 65.

CHAPITRE IX
Modifications d'autres instruments de l'Union

Article 59

Modifications du règlement (UE) 2018/1726

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

1) L'article 12 est remplacé par le texte suivant:

«*Article 12*

Qualité des données

1. Sans préjudice des responsabilités des États membres en ce qui concerne les données enregistrées dans les systèmes relevant de la responsabilité opérationnelle de l'Agence, l'Agence met en place, en étroite collaboration avec les groupes consultatifs, pour tous les systèmes relevant de sa responsabilité opérationnelle, des mécanismes et procédures automatisés de contrôle de la qualité des données, des indicateurs communs de qualité des données et des normes de qualité minimales pour le stockage de données, conformément aux dispositions pertinentes des instruments juridiques régissant ces systèmes d'information et de l'article 37 des règlements (UE) 2019/817 (*1) et (UE) 2019/818 (*2) du Parlement européen et du Conseil.

2. L'Agence crée un répertoire central ne contenant que des données anonymisées à des fins de rapports et de statistiques, conformément à l'article 39 des règlements (UE) 2019/817 et (UE) 2019/818 du Parlement européen et du Conseil, sous réserve des dispositions spécifiques des instruments juridiques régissant le développement, la création, le fonctionnement et l'utilisation des systèmes d'information à grande échelle gérés par l'Agence.

(*1) Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil

(JO L 135 du 22.5.2019, p. 27)."

(*2) 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).»."

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

a)le point suivant est inséré:

«ee *bis*) adopte les rapports sur l'état d'avancement du développement des éléments d'interopérabilité en vertu de l'article 78, paragraphe 2, du règlement (UE) 2019/817 et de l'article 74, paragraphe 2, du règlement (UE) 2019/818;»;

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

«ff) adopte les rapports sur le fonctionnement technique du SIS conformément à l'article 60, paragraphe 7, du règlement (UE) 2018/1861 du Parlement européen et du Conseil (*3) et à l'article 74, paragraphe 8, du règlement (UE) 2018/1862 du Parlement européen et du Conseil (*4), du VIS conformément à l'article 50, paragraphe 3, du règlement (CE) nº 767/2008 et à l'article 17, paragraphe 3, de la décision 2008/633/JAI, de l'EES conformément à l'article 72, paragraphe 4, du règlement (UE) 2017/2226, d'ETIAS conformément à l'article 92, paragraphe 4, du règlement (UE) 2018/1240, de l'ECRIS-TCN et de l'application de référence de l'ECRIS conformément à l'article 36, paragraphe 8, du règlement (UE) 2019/816 du Parlement et du Conseil (*5) et des 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;

(*3) 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) nº 1987/2006 (JO L 312 du 7.12.2018, p. 14)."

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

(*5) Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).»;"

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) nº 767/2008, à l'article 31, paragraphe 2, du règlement (UE) nº 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 et à l'article 52 des règlements (UE) 2019/817 et (UE) 2019/818 et veille à ce qu'il soit donné dûment suite à ces audits;»;

d)le point mm) est remplacé par le texte suivant:

«mm) veille à la publication annuelle de la liste des autorités compétentes autorisées à consulter directement les données introduites dans le SIS en vertu de l'article 41, paragraphe 8, du règlement (UE) 2018/1861 et de l'article 56, paragraphe 7, du règlement (UE) 2018/1862, de la liste des offices des systèmes nationaux du SIS (N.SIS) et des bureaux SIRENE visés, respectivement, à l'article 7, paragraphe 3, du règlement (UE) 2018/1861 et à l'article 7, paragraphe 3, du règlement (UE) 2018/1862, de la liste des autorités compétentes visées à l'article 65, paragraphe 2, du règlement (UE) 2017/2226, de la liste des autorités compétentes visées à l'article 87, paragraphe 2, du règlement (UE) 2018/1240, de la liste des autorités centrales visées à l'article 34, paragraphe 2, du règlement (UE) 2019/816 ainsi que de la liste des autorités visées à l'article 71, paragraphe 1, du règlement (UE) 2019/817 et à l'article 67, paragraphe 1, du règlement (UE) 2019/818»;

3)À l'article 22, le paragraphe 4 est remplacé par le texte suivant:

«4. Europol et Eurojust peuvent assister aux réunions du conseil d'administration en tant qu'observateurs lorsqu'une question concernant le SIS II, liée à l'application de la décision 2007/533/JAI, figure à l'ordre du jour.

L'Agence européenne de garde-frontières et de garde-côtes peut assister aux réunions du conseil d'administration en tant qu'observateur lorsqu'une question concernant le SIS, liée à l'application du règlement (UE) 2016/1624, figure à l'ordre du jour.

Europol peut assister aux réunions du conseil d'administration en tant qu'observateur lorsqu'une question concernant le VIS, liée à l'application de la décision 2008/633/JAI, ou lorsqu'une question concernant Eurodac, liée à l'application du règlement (UE) n° 603/2013, est à l'ordre du jour.

Europol peut assister aux réunions du conseil d'administration en tant qu'observateur lorsqu'une question concernant l'EES, liée à l'application du règlement (UE) 2017/2226, figure à l'ordre du jour ou lorsqu'une question concernant ETIAS, liée à l'application du règlement (UE) 2018/1240, figure à l'ordre du jour.

L'Agence européenne de garde-frontières et de garde-côtes peut assister aux réunions du conseil d'administration en tant qu'observateur lorsqu'une question concernant ETIAS liée à l'application du règlement (UE) 2018/1240 figure à l'ordre du jour.

Eurojust, Europol et le Parquet européen peuvent assister aux réunions du conseil d'administration en tant qu'observateurs lorsqu'une question concernant le règlement (UE) 2019/816 figure à l'ordre du jour.

Eurojust, Europol et l'Agence européenne de garde-frontières et de garde-côtes peuvent assister aux réunions du conseil d'administration en tant qu'observateurs lorsqu'une question concernant les règlements (UE) 2019/817 et (UE) 2019/818 figure à l'ordre du jour.

Le conseil d'administration peut inviter toute autre personne dont l'avis peut présenter un intérêt à assister à ses réunions en qualité d'observateur.».

4)À l'article 24, paragraphe 3, le point p) est remplacé par le texte suivant:

«p) sans préjudice de l'article 17 du statut des fonctionnaires, de déterminer les exigences de confidentialité à respecter pour se conformer à l'article 17 du règlement (CE) nº 1987/2006, à l'article 17 de la décision 2007/533/JAI, à l'article 26, paragraphe 9, du règlement (CE) nº 767/2008, à l'article 4, paragraphe 4, du règlement (UE) nº 603/2013, à l'article 37, paragraphe 4, du règlement (UE) 2017/2226, à l'article 74, paragraphe 2, du règlement (UE) 2018/1240, à l'article 11, paragraphe 16, du règlement (UE) 2019/816 et à l'article 55, paragraphe 2, des règlements (UE) 2019/817 et (UE) 2019/818;»;

5) L'article 27 est modifié comme suit:

a) au paragraphe 1, le point suivant est inséré:

«d *bis*) le groupe consultatif sur l'interopérabilité;»;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes peuvent chacun désigner un représentant au sein du groupe consultatif sur le SIS II.

Europol peut également désigner un représentant au sein des groupes consultatifs sur le VIS, sur Eurodac et sur l'EES-ETIAS.

L'Agence européenne de garde-frontières et de garde-côtes peut également désigner un représentant au sein du groupe consultatif sur l'EES-ETIAS.

Eurojust, Europol et le Parquet européen peuvent chacun désigner un représentant au sein du groupe consultatif sur l'ECRIS-TCN.

Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes peuvent chacun désigner un représentant au sein du groupe consultatif sur l'interopérabilité.».

Article 60

Modifications du règlement (UE) 2018/1862

Le règlement (UE) 2018/1862 est modifié comme suit:

1) À l'article 3, les points suivants sont ajoutés:

«18) **“ESP”**: le portail de recherche européen créé par l'article 6, paragraphe 1, du règlement (UE) 2019/818 du Parlement européen et du Conseil (*6);

19) **«BMS partagé»**: le service partagé d'établissement de correspondances biométriques établi par l'article 12, paragraphe 1, du règlement (UE) 2019/818;

20) **«CIR»**: le répertoire commun de données d'identité établi par l'article 17, paragraphe 1, du règlement (UE) 2019/818;

21) **«MID»**: le détecteur d'identités multiples établi par l'article 25, paragraphe 1, du règlement (UE) 2019/818;

(*6) 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).»."

2)L'article 4 est modifié comme suit:

a)au paragraphe 1, les points b) et c) sont remplacés par le texte suivant:

«b)d'un système national (ci-après dénommé "N.SIS") dans chaque État membre, constitué des systèmes de données nationaux reliés au SIS central, y compris au moins un N.SIS de secours national ou partagé;

c)d'une infrastructure de communication entre le CS-SIS, le CS-SIS de secours et le NI-SIS de secours (ci-après dénommée "infrastructure de communication"), fournissant un réseau virtuel crypté consacré aux données du SIS et à l'échange de données entre les bureaux SIRENE visés à l'article 7, paragraphe 2; et

d)d'une infrastructure de communication sécurisée entre le CS-SIS et les infrastructures centrales de l'ESP, du BMS partagé et du MID.»;

b)Les paragraphes suivants sont ajoutés:

«8. Sans préjudice des paragraphes 1 à 5, les données du SIS relatives aux personnes et aux documents d'identité peuvent également faire l'objet de recherches par l'intermédiaire de l'ESP.

9. Sans préjudice des paragraphes 1 à 5, les données du SIS relatives aux personnes et aux documents d'identité peuvent également être transmises par l'intermédiaire de l'infrastructure de communication sécurisée visée au paragraphe 1, point d). Ces transmissions sont limitées dans la mesure dans laquelle les données sont nécessaires pour les finalités du règlement (UE) 2019/818.».

3)À l'article 7, le paragraphe suivant est inséré:

«2 *bis*. Les bureaux SIRENE assurent également la vérification manuelle des identités différentes conformément à l'article 29 du règlement (UE) 2019/818. Dans la mesure nécessaire à l'accomplissement de cette tâche, les bureaux SIRENE ont accès aux données stockées dans le CIR et le MID aux fins prévues aux articles 21 et 26 du règlement (UE) 2019/818.».

4)À l'article 12, paragraphe 1, l'alinéa suivant est ajouté:

«Les États membres veillent à ce que chaque accès à des données à caractère personnel par l'intermédiaire de l'ESP soit également consigné afin de pouvoir contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle, ainsi que l'intégrité et la sécurité des données.».

5)À l'article 44, paragraphe 1, le point suivant est ajouté:

«f)de la vérification des identités différentes et de la lutte contre la fraude à l'identité conformément au chapitre V du règlement (UE) 2019/818.».

6)À l'article 74, le paragraphe 7 est remplacé par le texte suivant:

«7. Aux fins de l'article 15, paragraphe 4, et des paragraphes 3, 4 et 6 du présent article, l'eu-LISA stocke les données visées à l'article 15, paragraphe 4, et au paragraphe 3 du présent article qui ne permettent pas l'identification des personnes dans le répertoire central

des rapports et statistiques visé à l'article 39 du règlement (UE) 2019/818.

L'eu-LISA permet à la Commission et aux organismes visés au paragraphe 6 du présent article d'obtenir des rapports et des statistiques sur mesure. Sur demande, l'eu-LISA accorde l'accès au répertoire central des rapports et statistiques conformément à l'article 39 du règlement (UE) 2019/818 aux États membres, à la Commission, à Europol et à l'Agence européenne de garde-frontières et de garde-côtes.».

Article 61

Modifications du règlement (UE) 2019/816

Le règlement (UE) 2019/816 est modifié comme suit:

1)À l'article 1er, le point suivant est ajouté:

«c) les conditions dans lesquelles l'ECRIS-TCN contribue à faciliter l'identification correcte des personnes enregistrées dans l'ECRIS-TCN et aide à cette identification aux conditions et pour les finalités prévues à l'article 20 du règlement (UE) 2019/818 du Parlement européen et du Conseil (*7), en stockant des données d'identité, des données de documents de voyage et des données biométriques dans le CIR.

(*7) 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).»."

2)L'article 2 est remplacé par le texte suivant:

«Article 2

Champ d'application

Le présent règlement s'applique au traitement des données d'identité des ressortissants de pays tiers qui ont fait l'objet de condamnations dans les États membres aux fins d'identifier les États membres dans lesquels ces condamnations ont été prononcées. À l'exception de l'article 5, paragraphe 1, point b) ii), les dispositions du présent règlement qui s'appliquent aux ressortissants de pays tiers s'appliquent aussi aux citoyens de l'Union qui ont également la nationalité d'un pays tiers et qui ont fait l'objet de condamnations dans les États membres. Le présent règlement facilite également l'identification correcte des personnes et aide à cette identification, conformément au présent règlement et au règlement (UE) 2019/818.».

3)L'article 3 est modifié comme suit:

a) le point 8) est supprimé;

b)les points suivants sont ajoutés:

«19) **“CIR”**: le répertoire commun de données d'identité établi par l'article 17, paragraphe 1, du règlement (UE) 2019/818;

20) **“données de l'ECRIS-TCN”**: toutes les données stockées dans le système central et dans le CIR conformément à l'article 5;

21) **“ESP”**: le portail européen de recherche créé par l'article 6, paragraphe 1, du règlement (UE) 2019/818».

4)À l'article 4, le paragraphe 1 est modifié comme suit:

a) le point a) est remplacé par le texte suivant:

«a) un système central;»;

b) le point suivant est inséré:

«a *bis*) le CIR;»;

c)le point suivant est ajouté:

«e) une infrastructure de communication entre le système central et les infrastructures centrales de l'ESP et du CIR.».

5)L'article 5, est modifié comme suit:

a)au paragraphe 1, la phrase introductive est remplacée par le texte suivant:

«1. Pour chaque ressortissant d'un pays tiers condamné, l'autorité centrale de l'État membre de condamnation crée un fichier de données dans l'ECRIS-TCN. Ce fichier de données contient:»;

b)le paragraphe suivant est inséré:

«1 *bis*. Le CIR contient les données visées au paragraphe 1, point b), et les données suivantes du paragraphe 1, point a): le nom (nom de famille), les prénoms, la date de naissance, le lieu de naissance (ville et pays), la ou les nationalités, le genre, les noms précédents, le cas échéant, lorsqu'ils sont disponibles, les pseudonymes ou noms d'emprunt, lorsqu'ils sont disponibles, le type et numéro des documents de voyage de la personne, ainsi que le nom de l'autorité de délivrance de ces documents. Le CIR peut également contenir les données visées au paragraphe 3. Le reste des données de l'ECRIS-TCN sont stockées dans le système central.».

6)L'article 8 est modifié comme suit:

a)le paragraphe 1 est remplacé par le texte suivant:

«1. Chaque fichier de données est conservé dans le système central et dans le CIR tant que les données relatives aux condamnations de la personne concernée sont conservées dans le casier judiciaire.»;

b)le paragraphe 2 est remplacé par le texte suivant:

«2. À l'expiration de la durée de conservation visée au paragraphe 1, l'autorité centrale de l'État membre de condamnation procède à l'effacement du fichier de données, y compris les données concernant les empreintes digitales ou les images faciales, du système central et du CIR. L'effacement se fait automatiquement, si possible, et en tout état de cause au plus tard un mois après l'expiration de la durée de conservation.».

7)L'article 9 est modifié comme suit:

a)au paragraphe 1, le terme «dans l'ECRIS-TCN» est remplacé par les termes «dans le

système central et dans le CIR»;

b)aux paragraphes 2, 3 et 4, les termes «dans le système central» et «du système central» sont remplacés, respectivement, par les termes «dans le système central et dans le CIR» et «du système central et du CIR».

8) À l'article 10, paragraphe 1, le point j) est supprimé.

9)À l'article 12, paragraphe 2, les termes «dans le système central» sont remplacés par les termes «dans le système central et dans le CIR».

10)À l'article 13, paragraphe 2, les termes «du système central» sont remplacés par les termes «du système central, du CIR».

11)À l'article 23, paragraphe 2, les termes «dans le système central» sont remplacés par les termes «dans le système central et dans le CIR».

12)L'article 24 est modifié comme suit:

a)Le paragraphe 1 est remplacé par le texte suivant:

«1. Les données introduites dans le système central et dans le CIR ne font l'objet d'un traitement qu'aux fins de l'identification des États membres détenant des informations sur les casiers judiciaires de ressortissants de pays tiers. Les données introduites dans le CIR sont également traitées conformément au règlement (UE) 2019/818 dans le but de faciliter l'identification correcte des personnes enregistrées dans l'ECRIS-TCN et d'aider à cette identification conformément au présent règlement.»;

b)Le paragraphe suivant est ajouté:

«3. Sans préjudice du paragraphe 2, l'accès en consultation aux données stockées dans le CIR est également réservé au personnel dûment autorisé des autorités nationales de chaque État membre et au personnel dûment autorisé des agences de l'Union qui sont compétents pour les finalités prévues aux articles 20 et 21 du règlement (UE) 2019/818. Cet accès est limité en fonction de la mesure dans laquelle les données sont nécessaires à l'exécution de leurs tâches pour ces finalités, et est proportionné aux objectifs poursuivis.».

13)À l'article 30, le paragraphe 2 est remplacé par le texte suivant:

«2. Aux fins du paragraphe 1 du présent article, l'eu-LISA stocke les données visées audit paragraphe dans le répertoire central des rapports et statistiques visé à l'article 39 du règlement (UE) 2019/818.».

14)À l'article 33, paragraphe 1, les termes «du système central» sont remplacés par les termes «du système central, du CIR et».

15)À l'article 41, le paragraphe 2 est remplacé par le texte suivant:

«2. Pour les condamnations prononcées avant la date de début de l'inscription des données conformément à l'article 35, paragraphe 1, les autorités centrales créent les fichiers de données individuels dans le système central et dans le CIR comme suit:

a)les données alphanumériques à inscrire dans le système central et dans le CIR à la fin de

la période visée à l'article 35, paragraphe 2;

b)les données dactyloscopiques à inscrire dans le CIR dans les deux ans suivant la mise en service conformément à l'article 35, paragraphe 4.».

CHAPITRE X
Dispositions finales

Article 62

Établissement de rapports et de statistiques

1. Le personnel dûment autorisé des autorités compétentes des États membres, de la Commission et de l'eu-LISA a accès en consultation, uniquement aux fins de l'établissement de rapports et de statistiques, au nombre de requêtes par profil d'utilisateur de l'ESP.

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

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

a) le nombre de requêtes aux fins des articles 20, 21 et 22;

b) la nationalité, le genre et l'année de naissance de la personne;

c) le type de document de voyage et le code à trois lettres du pays de délivrance;

d) le nombre de recherches effectuées avec et sans données biométriques.

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

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

a) le nombre de recherches effectuées avec et sans données biométriques;

b)le nombre de chaque type de lien et les systèmes d'information de l'UE contenant les données liées;

c) la durée pendant laquelle un lien jaune et rouge est demeuré dans le système.

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

4. Le personnel dûment autorisé de l'Agence européenne de garde-frontières et de garde-côtes a accès en consultation aux données visées aux paragraphes 1, 2 et 3 du présent articles pour effectuer les analyses des risques et les évaluations de la vulnérabilité visées aux articles 11 et 13 du règlement (UE) 2016/1624 du Parlement européen et du Conseil [38].

5. Le personnel dûment autorisé d'Europol a accès en consultation aux données visées aux paragraphes 2 et 3 du présent article pour effectuer les analyses de nature stratégique ou thématique et les analyses opérationnelles prévues à l'article 18, paragraphe 2, points b) et c), du règlement (UE) 2016/794.

6. Aux fins des paragraphes 1, 2 et 3, l'eu-LISA stocke les données visées auxdits paragraphes dans le CRRS. Il n'est pas possible d'identifier des personnes à partir des données figurant dans le CRRS mais les données doivent permettre aux autorités énumérées aux paragraphes 1, 2 et 3 d'obtenir des rapports et des statistiques personnalisables afin d'améliorer l'efficacité des vérifications aux frontières, d'aider les autorités à traiter les demandes de visa et de favoriser l'élaboration, au niveau de l'Union, de politiques en matière de migration et de sécurité fondées sur des données concrètes.

7. Sur demande, la Commission met les informations pertinentes à la disposition de l'Agence des droits fondamentaux de l'Union européenne afin que celle-ci évalue l'incidence du présent règlement sur les droits fondamentaux.

Article 63

Période transitoire pour l'utilisation du portail de recherche européen

1. Pendant une période de deux ans à compter de la date de la mise en service de l'ESP, les obligations visées à l'article 7, paragraphes 2 et 4, ne s'appliquent pas et l'utilisation de l'ESP est facultative.

2. La Commission est habilitée à adopter un acte délégué conformément à l'article 69 afin de modifier le présent règlement en prolongeant une seule fois, d'une année maximum, la période visée au paragraphe 1 du présent article, lorsqu'une évaluation de la mise en œuvre de l'ESP a mis en évidence la nécessité de prolonger ce délai, particulièrement en raison de l'incidence de la mise en service de l'ESP sur l'organisation et la durée des contrôles aux frontières.

Article 64

Période transitoire applicable aux dispositions relatives à l'accès au répertoire commun de données d'identité à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière

L'article 22 s'applique à partir de la date de mise en service du CIR visée à l'article 68, paragraphe 3.

Article 65

Période transitoire pour la détection d'identités multiples

1. Pendant une période d'un an suivant la notification par l'eu-LISA de l'achèvement de l'essai du MID visé à l'article 68, paragraphe 4, point b), et avant la

mise en service du MID, l'unité centrale ETIAS est responsable de la détection d'identités multiples à l'aide des données stockées dans l'EES, le VIS, Eurodac et le SIS. Les détections d'identités multiples ne sont effectuées qu'à l'aide de données biométriques.

2. Lorsque la recherche génère une ou plusieurs correspondances et que les données d'identité dans les dossiers liés sont les mêmes ou similaires, un lien blanc est créé conformément à l'article 33.

Lorsque la recherche génère une ou plusieurs correspondances et que les données d'identité dans les dossiers liés ne peuvent pas être considérées comme similaires, un lien jaune est créé conformément à l'article 30 et la procédure visée à l'article 29 s'applique.

Lorsque plusieurs correspondances sont générées, un lien est créé entre chaque élément de donnée ayant donné lieu à la correspondance.

3. Lorsqu'un lien jaune est créé, le MID accorde à l'unité centrale ETIAS l'accès aux données d'identité figurant dans les différents systèmes d'information de l'UE.

4. Lorsqu'un lien est créé avec un signalement figurant dans le SIS, autre qu'un signalement créé dans le cadre de l'article 3 du règlement (UE) 2018/1860, des articles 24 et 25 du règlement (UE) 2018/1861 ou de l'article 38 du règlement (UE) 2018/1862, le MID accorde au bureau SIRENE de l'État membre qui a créé le signalement l'accès aux données d'identité figurant dans les différents systèmes d'information de l'UE.

5. L'unité centrale ETIAS ou, dans les cas visé au paragraphe 4 du présent article, le bureau SIRENE de l'État membre qui a créé le signalement a accès aux données figurant dans le dossier de confirmation d'identité, évalue les différentes identités et met à jour le lien conformément aux articles 31, 32 et 33, et l'ajoute au dossier de confirmation d'identité.

6. L'unité centrale ETIAS n'informe la Commission conformément à l'article 67, paragraphe 3, qu'une fois que tous les liens jaunes ont été vérifiés manuellement et que leur statut a été mis à jour en tant que liens verts, blancs ou rouges.

7. Les États membres aident, au besoin, l'unité centrale ETIAS à effectuer la détection d'identités multiples visée au présent article.

8. La Commission est habilitée à adopter un acte délégué conformément à l'article 69 afin de modifier le présent règlement en prolongeant la période visée au paragraphe 1 du présent article de six mois, renouvelables deux fois, chaque fois pour six mois. Une telle prolongation n'est accordée qu'après qu'une évaluation du délai estimé nécessaire pour achever la détection d'identités multiples visée au présent article a démontré que la détection d'identités multiples ne peut être achevée avant l'expiration soit de la période restante prévue au paragraphe 1 du présent article soit de toute prolongation en cours, pour des raisons indépendantes de l'unité centrale ETIAS, et qu'il n'est pas possible de recourir à des mesures

correctives. L'évaluation est effectuée au plus tard trois mois avant l'expiration du délai visé au paragraphe 1 ou de la prolongation en cours.

Article 66

Coûts

1. Les coûts afférents à la création et au fonctionnement de l'ESP, du BMS partagé, du CIR et du MID 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 aux interfaces uniformes nationales, ainsi qu'à l'hébergement des interfaces uniformes nationales, sont à la charge du budget général de l'Union.

Les coûts suivants ne sont pas admissibles:

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

b) hébergement des systèmes d'information nationaux (espace, mise en œuvre, électricité, refroidissement);

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

d) conception, développement, mise en œuvre, fonctionnement et maintenance des réseaux de communication nationaux.

3. Sans préjudice d'un financement supplémentaire à cette fin à partir d'autres sources du budget général de l'Union européenne, un montant de 32 077 000 EUR est mobilisé dans l'enveloppe de 791 000 000 EUR prévue à l'article 5, paragraphe 5, point b), du règlement (UE) n° 515/2014 pour couvrir les coûts de mise en œuvre du présent règlement, comme le prévoient les paragraphes 1 et 2 du présent article.

4. À partir de l'enveloppe visée au paragraphe 3, 22 861 000 EUR sont alloués à l'eu-LISA, 9 072 000 EUR sont alloués à Europol et 144 000 EUR sont alloués à l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL), afin de soutenir ces agences dans l'exécution de leurs tâches respectives dans le cadre du présent règlement. Ce financement est mis en œuvre en gestion partagée.

5. Les coûts encourus par les autorités désignées sont à la charge de l'État membre qui a procédé à la désignation et d'Europol, respectivement. Les coûts afférents à la connexion de chaque autorité désignée au CIR sont à la charge de chaque État membre.

Les coûts encourus par Europol, y compris ceux afférents à la connexion au CIR, sont à la charge d'Europol.

Article 67

Notifications

1. Les États membres notifient à l'eu-LISA le nom des autorités visées aux articles 7, 20, 21 et 26 qui peuvent, respectivement, utiliser l'ESP, le CIR et le MID ou y avoir accès.

Une liste consolidée de ces autorités est publiée au *Journal officiel de l'Union européenne* dans un délai de trois mois à compter de la date à laquelle chaque élément d'interopérabilité a été mis en service conformément à l'article 68. En cas de modifications apportées à cette liste, l'eu-LISA publie une fois par an une version consolidée actualisée.

2. L'eu-LISA notifie à la Commission les résultats concluants des essais visés à l'article 68, paragraphe 1, point b), paragraphe 2, point b), paragraphe 3, point b), paragraphe 4, point b), paragraphe 5, point b), paragraphe 6, point b).

3. L'unité centrale ETIAS informe la Commission de l'exécution concluante de la période transitoire prévue à l'article 65.

4. La Commission met les informations notifiées en application du paragraphe 1 à la disposition des États membres et du public, par l'intermédiaire d'un site web public actualisé en permanence.

Article 68

Mise en service

1. La Commission détermine, par la voie d'un acte d'exécution, la date de mise en service de l'ESP, dès que les conditions suivantes sont remplies:

a) les mesures visées à l'article 8, paragraphe 2, à l'article 9, paragraphe 7, et à l'article 43, paragraphe 5, ont été adoptées;

b) L'eu-LISA a déclaré que les essais complets de l'ESP, qu'elle a menés en coopération avec les autorités des États membres et les agences de l'Union autorisées à utiliser l'ESP, étaient concluants;

c) l'eu-LISA a validé les aménagements techniques et juridiques nécessaires pour recueillir et transmettre les données visées à l'article 8, paragraphe 1, et les a notifiés à la Commission;

L'ESP interroge les bases de données d'Interpol uniquement lorsque les aménagements techniques permettent de se conformer à l'article 9, paragraphe 5. S'il est impossible de respecter l'article 9, paragraphe 5, l'ESP n'interroge pas les bases de données d'Interpol, sans que la mise en service de l'ESP ne soit pour autant retardée.

La Commission fixe la date visée au premier alinéa dans un délai de trente jours à compter de la date d'adoption de l'acte d'exécution.

2. La Commission détermine, par la voie d'un acte d'exécution, la date de mise en service du BMS partagé, dès que les conditions suivantes sont remplies:

a) les mesures visées à l'article 13, paragraphe 5, et à l'article 43, paragraphe 5, ont été adoptées;

b) l'eu-LISA a déclaré que les essais complets du BMS partagé qu'elle a menés en coopération avec les autorités des États membres étaient concluants;

c) l'eu-LISA a validé les aménagements techniques et juridiques nécessaires pour recueillir et transmettre les données visées à l'article 13 et les a notifiés à la Commission;

d) l'eu-LISA a déclaré que les essais visés au paragraphe 5, point b), étaient concluants.

La Commission fixe la date visée au premier alinéa dans un délai de trente jours à compter de la date de l'adoption de l'acte d'exécution.

3. La Commission détermine, par la voie d'un acte d'exécution, la date de mise en service du CIR, dès que les conditions suivantes sont remplies:

a) les mesures prévues à l'article 43, paragraphe 5, et à l'article 74, paragraphe 10, ont été adoptées;

b) l'eu-LISA a déclaré que les essais complets du CIR qu'elle a menés en coopération avec les autorités des États membres étaient concluants;

c) l'eu-LISA a validé les aménagements techniques et juridiques nécessaires pour recueillir et transmettre les données visées à l'article 18 et les a notifiés à la Commission;

d) l'eu-LISA a déclaré que les essais visés au paragraphe 5, point b), étaient concluants.

La Commission fixe la date visée au premier alinéa dans un délai de trente jours à compter de la date de l'adoption de l'acte d'exécution.

4. La Commission détermine, par la voie d'un acte d'exécution, la date de mise en service du MID, dès que les conditions suivantes sont remplies:

a) les mesures visées à l'article 28, paragraphes 5 et 7, à l'article 32, paragraphe 5, à l'article 33, paragraphe 6, à l'article 43, paragraphe 5, et à l'article 49, paragraphe 6, ont été adoptées;

b) l'eu-LISA a déclaré que les essais complets du MID, qu'elle a menés en coopération avec les autorités des États membres et l'unité centrale ETIAS, étaient concluants;

c) l'eu-LISA a validé les aménagements techniques et juridiques nécessaires pour recueillir et transmettre les données visées à l'article 34 et les a notifiés à la Commission;

d) L'unité centrale ETIAS a adressé à la Commission la notification visée à l'article 67, paragraphe 3;

e) l'eu-LISA a déclaré que les essais visés aux paragraphes 1, point b), 2, point b), 3, point b), et 5, point b), étaient concluants.

La Commission fixe la date visée au premier alinéa dans un délai de trente jours à compter de la date de l'adoption de l'acte d'exécution.

5. La Commission détermine, par la voie d'actes d'exécution, la date à partir de laquelle les mécanismes et procédures automatisés de contrôle de la qualité des données, les indicateurs communs de qualité des données et les normes de qualité minimales doivent être utilisés, dès que les conditions suivantes sont remplies:

a) les mesures visées à l'article 37, paragraphe 4, ont été adoptées;

b) l'eu-LISA a déclaré que les essais complets relatifs aux mécanismes et procédures automatisés de contrôle de la qualité des données, aux indicateurs communs de qualité des données et aux normes de qualité minimales, qu'elle a menés en coopération avec les autorités des États membres, étaient concluants;

La Commission fixe la date visée au premier alinéa dans un délai de trente jours à compter de la date de l'adoption de l'acte d'exécution.

6. La Commission détermine, par la voie d'un acte d'exécution, de la date de mise en service du CRRS, dès que les conditions suivantes sont remplies:

a) les mesures visées à l'article 39, paragraphe 5, et à l'article 43, paragraphe 5, ont été adoptées;

b) l'eu-LISA a déclaré que les essais complets du CRRS qu'elle a menés en coopération avec les autorités des États membres étaient concluants;

c) l'eu-LISA a validé les aménagements techniques et juridiques nécessaires pour recueillir et transmettre les données visées à l'article 39 et les a notifiés à la Commission.

La Commission fixe la date visée au premier alinéa dans un délai de trente jours à compter de la date de l'adoption de l'acte d'exécution.

7. La Commission informe le Parlement européen et le Conseil des résultats des essais effectués en vertu des paragraphes 1, point b), 2, point b), 3, point b), 4, point b), 5, point b), et 6, point b).

8. Les États membres, l'unité centrale ETIAS et Europol commencent à utiliser chacun des éléments d'interopérabilité à partir de la date fixée par la Commission conformément aux paragraphes 2, 3 et 4, respectivement.

Article 69

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 28, paragraphe 5, à l'article 39, paragraphe 5, à l'article 49, paragraphe 6, à l'article 63, paragraphe 2, et à l'article 65, paragraphe 8, est conféré à la Commission pour une période de cinq ans à compter du 11 juin 2019. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 28, paragraphe 5, à l'article 39, paragraphe 5, à l'article 49, paragraphe 6, à l'article 63, paragraphe 2, et à l'article 65, paragraphe 8, peut être révoquée à tout moment par le Parlement

européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 28, paragraphe 5, de l'article 39, paragraphe 5, de l'article 49, paragraphe 6, de l'article 63, paragraphe 2, et de l'article 65, paragraphe 8, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 70

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 71

Groupe consultatif

L'eu-LISA crée un groupe consultatif sur l'interopérabilité. Durant la phase de conception et de développement des éléments d'interopérabilité, l'article 54, paragraphes 4, 5 et 6, s'applique.

Article 72

Formation

L'eu-LISA s'acquitte des tâches liées à l'offre d'une formation relative à l'utilisation technique des éléments d'interopérabilité conformément au règlement (UE) 2018/1726.

Les autorités des États membres et les agences de l'Union proposent, à l'intention des membres de leur personnel autorisés à traiter des données par le biais des éléments d'interopérabilité, un programme de formation approprié sur la sécurité des données, la qualité des données et les règles en matière de protection des données ainsi que sur les procédures applicables au traitement des données et les obligations d'informer prévues à l'article 32, paragraphe 4, à l'article 33, paragraphe 4, et à l'article 47.

Le cas échéant, des formations communes sur ces sujets sont organisées au niveau de l'Union afin de renforcer la coopération et l'échange de meilleures pratiques entre les membres du personnel des autorités des États membres et des agences de l'Union qui sont autorisés à traiter les données par le biais des éléments d'interopérabilité. Une attention particulière est accordée au processus de détection d'identités multiples, y compris la vérification manuelle des différentes identités et le besoin qui s'ensuit de maintenir des garanties en ce qui concerne les droits fondamentaux.

Article 73

Manuel pratique

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

Article 74

Suivi et évaluation

1. L'eu-LISA veille à ce que des procédures soient mises en place pour suivre le développement des éléments d'interopérabilité et leur connexion avec l'interface nationale uniforme par rapport aux objectifs fixés en matière de planification et de coûts et pour suivre le fonctionnement des éléments d'interopérabilité 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 12 décembre 2019, puis tous les six mois pendant la phase de développement des éléments d'interopérabilité, l'eu-LISA présente un rapport au Parlement européen et au Conseil sur l'état d'avancement du développement des éléments d'interopérabilité et leur connexion à l'interface uniforme nationale. Une fois le développement achevé, un rapport est présenté au Parlement européen et au Conseil, qui explique en détail la manière dont les objectifs, en particulier ceux ayant trait à la planification et aux coûts, ont été atteints, et justifie les éventuels écarts.

3. Quatre ans après la mise en service de chaque élément d'interopérabilité conformément à l'article 68, puis tous les quatre ans, l'eu-LISA présente au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique des éléments d'interopérabilité, y compris sur leur sécurité.

4. En outre, un an après chaque rapport de l'eu-LISA, la Commission réalise une évaluation globale des éléments d'interopérabilité, y compris:

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

b) un examen des résultats obtenus par rapport aux objectifs du présent règlement et de son impact sur les droits fondamentaux, notamment une évaluation de l'incidence des éléments d'interopérabilité sur le droit à la non-discrimination;

c) une évaluation du fonctionnement du portail en ligne, y compris des chiffres concernant son utilisation ainsi que le nombre de demandes traitées avec succès;

d) une évaluation permettant de déterminer si les principes de base des éléments d'interopérabilité restent valables;

e) une évaluation de la sécurité des éléments d'interopérabilité;

f) une évaluation de l'utilisation du CIR à des fins d'identification;

g) une évaluation de l'utilisation du CIR à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière;

h) une évaluation de toute conséquence y compris toute incidence disproportionnée sur la fluidité du trafic aux points de passage frontaliers et les conséquences ayant un impact sur le budget général de l'Union;

i) une évaluation des recherches effectuées dans les bases de données d'Interpol via l'ESP, y compris des informations sur le nombre de correspondances dans les bases de données d'Interpol et des informations sur tout problème rencontré;

Les évaluations globales prévues au premier alinéa du présent paragraphe comprennent les éventuelles recommandations nécessaires. La Commission transmet le rapport d'évaluation au Parlement européen, au Conseil, au Contrôleur européen de la protection des données et à l'Agence des droits fondamentaux de l'Union européenne.

5. Au plus tard le 12 juin 2020 puis chaque année jusqu'à l'adoption par la Commission des actes d'exécution visés à l'article 68, la Commission présente au Parlement européen et au Conseil un rapport sur l'état d'avancement des préparations pour la mise en œuvre complète du présent règlement. Ce rapport contient également des informations détaillées sur les coûts encourus ainsi que des informations relatives à tout risque susceptible d'avoir des retombées sur les coûts totaux.

6. Deux ans après la mise en service du MID conformément à l'article 68, paragraphe 4, la Commission examine l'incidence du MID sur le droit à la non-

discrimination. À la suite de ce premier rapport, l'examen de l'incidence du MID sur le droit à la non-discrimination fait partie intégrante de l'examen visé au paragraphe 4, point b) du présent article.

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

8. L'eu-LISA fournit à la Commission les informations nécessaires pour élaborer l'évaluation globale visée au paragraphe 4.

9. Tout en respectant les dispositions du droit national relatives à la publication d'informations sensibles, et sans préjudice des restrictions nécessaires pour protéger la sécurité et l'ordre public, prévenir la criminalité et garantir qu'aucune enquête nationale ne sera compromise, chaque État membre et Europol établissent des rapports annuels sur l'efficacité de l'accès aux données stockées dans le CIR à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, comportant des informations et des statistiques sur:

a) les finalités précises de la consultation, notamment les types d'infractions terroristes ou autres infractions pénales graves;

b) les motifs raisonnables invoqués qui permettent de soupçonner de manière justifiée que le suspect, l'auteur ou la victime relève du règlement (UE) n° 603/2013;

c) le nombre de demandes d'accès au CIR aux fins de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière;

d) le nombre et les types de cas qui ont permis une identification;

e) la nécessité de disposer de procédures exceptionnelles dans les cas d'urgence et l'usage qui en a été fait, y compris lorsque le caractère urgent n'a pas été validé par le point d'accès central lors de la vérification a posteriori.

Les rapports annuels préparés par les États membres et par Europol sont transmis à la Commission au plus tard le 30 juin de l'année suivante.

10. Une solution technique est mise à la disposition des États membres afin de gérer les demandes d'accès des utilisateurs visées à l'article 22 et de faciliter la collecte d'informations au titre des paragraphes 7 et 9 du présent article, en vue de générer les rapports et statistiques visées dans ces paragraphes. La Commission adopte des actes d'exécution pour fixer les spécifications de la solution technique. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 70, paragraphe 2.

Article 75

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.*

Les dispositions du présent règlement relatives à l'ESP s'appliquent à compter de la date déterminée par la Commission conformément à l'article 68, paragraphe 1.

Les dispositions du présent règlement relatives au BMS partagé s'appliquent à compter de la date déterminée par la Commission conformément à l'article 68, paragraphe 2.

Les dispositions du présent règlement relatives au CIR s'appliquent à compter de la date déterminée par la Commission conformément à l'article 68, paragraphe 3.

Les dispositions du présent règlement relatives au MID s'appliquent à compter de la date déterminée par la Commission conformément à l'article 68, paragraphe 4.

Les dispositions du présent règlement relatives aux mécanismes et procédures automatisés de contrôle de la qualité des données, aux indicateurs communs de qualité des données et aux normes minimales de qualité des données s'appliquent, respectivement, à compter des dates déterminées par la Commission conformément à l'article 68, paragraphe 5.

Les dispositions du présent règlement relatives au CRRS s'appliquent à compter de la date déterminée par la Commission conformément à l'article 68, paragraphe 6.

Les articles 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71 et 73, et l'article 74, paragraphe 1, s'appliquent à compter du 11 juin 2019.

En ce qui concerne Eurodac, le présent règlement s'applique à partir de la date d'application de la refonte du règlement (UE) n° 603/2013.
Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Bruxelles, le 20 mai 2019.

Par le Parlement européen

Le président

A. TAJANI

Par le Conseil

Le président

G. CIAMBA

---

(1) JO C 283 du 10.8.2018, p. 48.

(2) Position du Parlement européen du 16 avril 2019 (non encore parue au Journal officiel) et décision du Conseil du 14 mai 2019.

(3) JO C 101 du 16.3.2018, p. 116.

(4) 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).

(5) 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).

(6) 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).

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

(8) Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1).

(9) 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) nº 1987/2006 (JO L 312 du 7.12.2018, p. 14).

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

(11) Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 (voir page 1 du présent Journal officiel).

(12) Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

(13) JO C 233 du 4.7.2018, p. 12.

(14) Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) nº 1296/2013, (UE) nº 1301/2013, (UE) nº 1303/2013, (UE) nº 1304/2013, (UE) nº 1309/2013, (UE)

nº 1316/2013, (UE) nº 223/2014, (UE) nº 283/2014 et la décision nº 541/2014/UE, et abrogeant le règlement (UE, Euratom) nº 966/2012 (JO L 193 du 30.7.2018, p. 1).

([15]) Règlement (UE) nº 515/2014 du Parlement européen et du Conseil du 16 avril 2014 portant création, dans le cadre du Fonds pour la sécurité intérieure, de l'instrument de soutien financier dans le domaine des frontières extérieures et des visas et abrogeant la décision nº 574/2007/CE (JO L 150 du 20.5.2014, p. 143).

([16]) JO L 123 du 12.5.2016, p. 1.

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

([18]) Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) nº 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO L 158 du 30.4.2004, p. 77).

([19]) Décision 2000/365/CE du Conseil du 29 mai 2000 relative à la demande du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de participer à certaines dispositions de l'acquis de Schengen (JO L 131 du 1.6.2000, p. 43).

([20]) Décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen (JO L 64 du 7.3.2002, p. 20).

([21]) JO L 176 du 10.7.1999, p. 36.

([22]) Décision 1999/437/CE du Conseil du 17 mai 1999 relative à certaines modalités d'application de l'accord conclu par le Conseil de l'Union européenne et la République d'Islande et le Royaume de Norvège sur l'association de ces États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 176 du 10.7.1999, p. 31).

([23]) JO L 53 du 27.2.2008, p. 52.

([24]) Décision 2008/149/JAI du Conseil du 28 janvier 2008 relative à la conclusion, au nom de l'Union européenne, de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 53 du 27.2.2008, p. 50).

([25]) JO L 160 du 18.6.2011, p. 21.

([26]) Décision 2011/350/UE du Conseil du 7 mars 2011 relative à la conclusion, au nom de l'Union européenne, du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen en ce qui concerne la suppression des contrôles aux frontières intérieures et la circulation des personnes (JO L 160 du 18.6.2011, p. 19).

([27]) Règlement (UE) 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), modifiant le règlement (CE)

nº 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) nº 1077/2011 (JO L 295 du 21.11.2018, p. 99).

([28]) Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil (voir page 27 du présent Journal officiel).

([29]) Règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO L 77 du 23.3.2016, p. 1).

([30]) Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) nº 767/2008 et (UE) nº 1077/2011 (JO L 327 du 9.12.2017, p. 20).

([31]) Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (JO L 218 du 13.8.2008, p. 129).

([32]) Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 (JO L 236 du 19.9.2018, p. 1).

([33]) Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

([34]) Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

([35]) Règlement (CE) nº 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS) (JO L 218 du 13.8.2008, p. 60).

([36]) Règlement (UE) nº 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) nº 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (JO L 180 du 29.6.2013, p. 1).

(37) Règlement (CE) nº 168/2007 du Conseil du 15 février 2007 portant création d'une Agence des droits fondamentaux de l'Union européenne (JO L 53 du 22.2.2007, p. 1).

(38) Règlement (UE) 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du Parlement européen et du Conseil et abrogeant le règlement (CE) nº 863/2007 du Parlement européen et du Conseil, le règlement (CE) nº 2007/2004 du Conseil et la décision 2005/267/CE du Conseil (JO L 251 du 16.9.2016, p. 1).