

I

(Actes législatifs)

DIRECTIVES

DIRECTIVE (UE) 2023/977 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 10 mai 2023

relative à l'échange d'informations entre les services répressifs des États membres et abrogeant la décision-cadre 2006/960/JAI du Conseil

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

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

vu la proposition de la Commission européenne,

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

statuant conformément à la procédure législative ordinaire ⁽¹⁾,

considérant ce qui suit:

- (1) Les activités criminelles transnationales constituent une menace importante pour la sécurité intérieure de l'Union et nécessitent une réponse coordonnée, ciblée et adaptée. Si les autorités nationales opérant sur le terrain sont en première ligne dans la lutte contre la criminalité et le terrorisme, une action au niveau de l'Union est essentielle pour assurer une coopération efficace et efficiente en ce qui concerne l'échange d'informations. Par ailleurs, la criminalité organisée et le terrorisme, en particulier, sont emblématiques du lien existant entre sécurité intérieure et sécurité extérieure. Les activités criminelles transnationales s'étendent au-delà des frontières et se manifestent sous la forme d'organisations criminelles et de groupes terroristes qui se livrent à un large éventail d'activités criminelles de plus en plus dynamiques et complexes. Il est donc nécessaire d'améliorer le cadre juridique pour faire en sorte que les services répressifs compétents puissent prévenir et détecter les infractions pénales et enquêter en la matière plus efficacement.
- (2) Afin de développer un espace de liberté, de sécurité et de justice, caractérisé par l'absence de contrôles aux frontières intérieures, il est essentiel que les services répressifs compétents d'un État membre puissent, dans le cadre du droit de l'Union et du droit national applicables, bénéficier d'un accès équivalent aux informations dont disposent leurs homologues d'un autre État membre. À cet égard, les services répressifs compétents devraient coopérer efficacement et dans toute l'Union. Aussi la coopération policière en matière d'échange d'informations pertinentes aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière, est-elle une composante essentielle des mesures qui sous-tendent la sécurité publique dans un espace interdépendant sans contrôles aux frontières intérieures. L'échange d'informations sur la criminalité et les activités criminelles, y compris le terrorisme, sert l'objectif général de protection de la sécurité des personnes physiques et de sauvegarde des intérêts majeurs des personnes morales protégés par la loi.

⁽¹⁾ Position du Parlement européen du 15 mars 2023 (non encore parue au Journal officiel) et décision du Conseil du 24 avril 2023.

- (3) La majorité des organisations criminelles sont présentes dans plus de trois pays et sont composées de membres de plusieurs nationalités qui se livrent à diverses activités criminelles. La structure de ces organisations criminelles est de plus en plus sophistiquée et comprend des systèmes de communication solides et efficaces et la coopération entre leurs membres par-delà les frontières.
- (4) Pour lutter efficacement contre la criminalité transfrontière, il est crucial que les services répressifs compétents échangent rapidement des informations et coopèrent sur le plan opérationnel. Bien que la coopération transfrontière entre les services répressifs compétents se soit améliorée ces dernières années, des difficultés pratiques et juridiques subsistent. À cet égard, la recommandation (UE) 2022/915 du Conseil ⁽²⁾ aidera les États membres à renforcer encore la coopération opérationnelle transfrontière.
- (5) Certains États membres ont mis au point des projets pilotes visant à renforcer la coopération transfrontière, par exemple en organisant des patrouilles communes d'agents de police dans des régions frontalières d'États membres voisins. Un certain nombre d'États membres ont également conclu des accords bilatéraux, voire multilatéraux, pour renforcer la coopération transfrontière, y compris l'échange d'informations. La présente directive ne limite pas ces possibilités, pour autant que les règles relatives à l'échange d'informations énoncées dans ces accords soient compatibles avec la présente directive lorsqu'elle s'applique. Au contraire, les États membres sont encouragés à échanger les bonnes pratiques et les enseignements tirés de ces projets pilotes et accords et à avoir recours aux financements de l'Union disponibles à cet égard, en particulier ceux provenant du Fonds pour la sécurité intérieure, établi par le règlement (UE) 2021/1149 du Parlement européen et du Conseil ⁽³⁾.
- (6) L'échange d'informations entre les États membres aux fins de la prévention ou de la détection des infractions pénales est régi par la convention d'application de l'accord de Schengen du 14 juin 1985 ⁽⁴⁾, adoptée le 19 juin 1990, notamment ses articles 39 et 46. La décision-cadre 2006/960/JAI du Conseil ⁽⁵⁾ a remplacé en partie ces dispositions et a introduit de nouvelles règles relatives à l'échange d'informations et de renseignements entre les services répressifs compétents.
- (7) Il ressort des évaluations, y compris de celles réalisées en vertu du règlement (UE) n° 1053/2013 du Conseil ⁽⁶⁾, que la décision-cadre 2006/960/JAI n'est pas suffisamment claire et ne garantit pas l'échange adéquat et rapide d'informations pertinentes entre les États membres. Les évaluations ont également montré que ladite décision-cadre était en fait peu utilisée, en partie en raison du manque de clarté constaté en pratique entre le champ d'application de la convention d'application de l'accord de Schengen et celui de la décision-cadre.
- (8) En conséquence, il conviendrait d'actualiser le cadre juridique existant en vue d'éliminer les divergences et d'établir des règles claires et harmonisées de façon à faciliter et à garantir l'échange adéquat et rapide d'informations entre les services répressifs compétents de différents États membres, ainsi qu'à permettre aux services répressifs compétents de s'adapter à l'évolution et l'expansion rapides de la nature de la criminalité organisée, y compris dans le contexte de la mondialisation et de la numérisation de la société.

⁽²⁾ Recommandation (UE) 2022/915 du Conseil du 9 juin 2022 relative à la coopération opérationnelle des services répressifs (JO L 158 du 13.6.2022, p. 53).

⁽³⁾ Règlement (UE) 2021/1149 du Parlement européen et du Conseil du 7 juillet 2021 établissant le Fonds pour la sécurité intérieure (JO L 251 du 15.7.2021, p. 94).

⁽⁴⁾ Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes (JO L 239 du 22.9.2000, p. 19).

⁽⁵⁾ Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne (JO L 386 du 29.12.2006, p. 89).

⁽⁶⁾ Règlement (UE) n° 1053/2013 du Conseil du 7 octobre 2013 portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen et abrogeant la décision du comité exécutif du 16 septembre 1998 concernant la création d'une commission permanente d'évaluation et d'application de Schengen (JO L 295 du 6.11.2013, p. 27).

- (9) En particulier, la présente directive devrait couvrir l'échange d'informations aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière, afin de remplacer entièrement, dans la mesure où ces échanges sont concernés, les articles 39 et 46 de la convention d'application de l'accord de Schengen et de garantir la sécurité juridique nécessaire. Il conviendrait, en outre, de simplifier et de clarifier les règles applicables afin de faciliter leur application effective dans la pratique.
- (10) Il est nécessaire de définir des règles harmonisées régissant les aspects transversaux de l'échange d'informations entre les États membres au titre de la présente directive à divers stades d'une enquête, depuis la collecte de renseignements en matière pénale jusqu'à l'enquête pénale. Ces règles devraient inclure l'échange d'informations par l'intermédiaire de centres de coopération policière et douanière mis en place entre deux ou plusieurs États membres sur la base de conventions bilatérales ou multilatérales aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière. Toutefois, ces règles ne devraient pas inclure l'échange d'informations bilatéral avec des pays tiers. Les règles définies dans la présente directive ne devraient pas porter atteinte à l'application des règles du droit de l'Union relatives à des systèmes ou cadres spécifiques pour de tels échanges, comme les règlements (UE) 2016/794 ⁽⁷⁾, (UE) 2018/1860 ⁽⁸⁾, (UE) 2018/1861 ⁽⁹⁾ et (UE) 2018/1862 ⁽¹⁰⁾ du Parlement européen et du Conseil, les directives (UE) 2016/681 ⁽¹¹⁾ et (UE) 2019/1153 ⁽¹²⁾ du Parlement européen et du Conseil, ainsi que les décisions 2008/615/JAI ⁽¹³⁾ et 2008/616/JAI ⁽¹⁴⁾ du Conseil.
- (11) L'expression «infraction pénale» est une notion autonome du droit de l'Union tel qu'il est interprété par la Cour de justice de l'Union européenne. Aux fins de la présente directive, dans l'intérêt d'une lutte efficace contre la criminalité, il convient d'entendre par «infraction pénale» tout comportement punissable en vertu du droit pénal de l'État membre qui reçoit des informations, soit à la suite d'une demande, soit à la suite d'une communication d'informations sur propre initiative conformément à la présente directive, quelle que soit la sanction pouvant être infligée dans cet État membre et indépendamment de la question de savoir si le comportement est également punissable en vertu du droit pénal de l'État membre qui communique des informations, sans préjudice des motifs de refus des demandes d'informations énoncés dans la présente directive.
- (12) La présente directive est sans préjudice de la convention établie sur la base de l'article K.3 du traité sur l'Union européenne, relative à l'assistance mutuelle et à la coopération entre les administrations douanières ⁽¹⁵⁾ (Naples II).
- (13) Étant donné que la présente directive ne s'applique pas au traitement d'informations effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union, les activités relatives à la sécurité nationale ne relèvent pas du champ d'application de la présente directive.

⁽⁷⁾ 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).

⁽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) n° 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) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

⁽¹¹⁾ Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (JO L 119 du 4.5.2016, p. 132).

⁽¹²⁾ Directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil (JO L 186 du 11.7.2019, p. 122).

⁽¹³⁾ Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 1).

⁽¹⁴⁾ Décision 2008/616/JAI du Conseil du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 12).

⁽¹⁵⁾ JO C 24 du 23.1.1998, p. 2.

- (14) La présente directive ne régit pas la communication et l'utilisation d'informations comme preuves dans une procédure judiciaire. En particulier, elle ne devrait pas être comprise comme établissant un droit d'utiliser comme preuves les informations communiquées conformément à la présente directive et, par conséquent, elle est sans effet sur toute exigence prévue par le droit applicable relative à l'obtention du consentement de l'État membre qui communique les informations pour une telle utilisation. La présente directive est sans effet sur les actes juridiques de l'Union relatifs aux éléments de preuve, tels que le règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et d'exécution de peines privatives de liberté à l'issue de procédures pénales, la directive 2014/41/UE du Parlement européen et du Conseil ⁽¹⁶⁾ et la directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation d'établissements désignés et la nomination de représentants légaux aux fins de la collecte de preuves électroniques en matière pénale. Par conséquent, même s'ils ne sont pas tenus de le faire en vertu de la présente directive, les États membres communiquant des informations au titre de la présente directive devraient être autorisés à donner leur consentement, au moment de la communication des informations ou ultérieurement, à l'utilisation de ces informations comme preuves dans une procédure judiciaire, y compris lorsque le droit national l'exige, en recourant aux instruments en matière de coopération judiciaire qui sont en vigueur entre les États membres.
- (15) Tous les échanges d'informations au titre de la présente directive devraient être soumis à cinq principes généraux, à savoir le principe de disponibilité, le principe d'accès équivalent, le principe de confidentialité, le principe de propriété des données et le principe de fiabilité des données. Bien que ces principes soient sans préjudice des dispositions plus précises de la présente directive, ils devraient guider son interprétation et son application, s'il y a lieu. Premièrement, le principe de disponibilité devrait être compris comme signifiant que les informations pertinentes dont disposent le point de contact unique ou les services répressifs compétents d'un État membre devraient également être accessibles, dans toute la mesure possible, au point de contact unique ou aux services répressifs compétents d'autres États membres. Ce principe ne devrait toutefois pas porter atteinte à l'application, lorsqu'elle est justifiée, de dispositions spécifiques de la présente directive restreignant la disponibilité d'informations, telles que celles relatives aux motifs de refus de demandes d'informations et aux autorisations judiciaires, ni à l'obligation d'obtenir le consentement de l'État membre ou du pays tiers qui a initialement communiqué les informations avant de les partager. Deuxièmement, selon le principe d'accès équivalent, les États membres devraient veiller à ce que l'accès du point de contact unique et des services répressifs compétents d'autres États membres aux informations pertinentes soit essentiellement le même, et, partant, ni plus ni moins strict, que l'accès de leur propre point de contact unique et de leurs propres services répressifs compétents à ces informations, sous réserve des dispositions plus précises de la directive. Troisièmement, le principe de confidentialité impose aux États membres de respecter leurs règles nationales respectives en matière de confidentialité lorsqu'ils traitent des informations qualifiées de confidentielles qui sont communiquées à leur point de contact unique ou à leurs services répressifs compétents, en garantissant un niveau de confidentialité similaire conformément aux règles de confidentialité énoncées dans le droit national. Quatrièmement, en vertu du principe de propriété des données, les informations initialement obtenues auprès d'un autre État membre ou d'un pays tiers ne devraient être communiquées qu'avec le consentement de cet État membre ou de ce pays tiers et conformément aux conditions imposées par cet État membre ou ce pays tiers. Cinquièmement, en vertu du principe de fiabilité des données, les données à caractère personnel qui se révèlent inexactes, incomplètes ou plus à jour devraient être effacées ou rectifiées ou le traitement de ces données devrait être limité, selon le cas, et tout destinataire de ces données devrait en recevoir notification sans tarder.
- (16) Afin de réaliser l'objectif visant à faciliter et à garantir l'échange adéquat et rapide d'informations entre États membres, la présente directive devrait prévoir la possibilité pour les États membres d'obtenir des informations en adressant une demande d'informations au point de contact unique d'autres États membres, conformément à certaines exigences claires, simplifiées et harmonisées. En ce qui concerne la teneur des demandes d'informations, la présente directive devrait préciser, en particulier, de manière exhaustive et suffisamment détaillée et sans préjudice de la nécessité d'une appréciation au cas par cas, les situations dans lesquelles les demandes d'informations doivent être considérées comme urgentes, les détails qu'elles doivent contenir au minimum et dans quelle langue elles doivent être soumises.
- (17) S'il est vrai que le point de contact unique de chaque État membre devrait, en tout état de cause, pouvoir soumettre des demandes d'informations au point de contact unique d'un autre État membre, pour plus de souplesse, les États membres devraient être autorisés, en outre, à désigner certains de leurs services répressifs compétents, qui pourraient participer à la coopération européenne, en tant que services répressifs désignés aux fins de la soumission de telles demandes aux points de contact uniques d'autres États membres. Chaque État membre devrait soumettre à la Commission une liste de ses services répressifs désignés. Les États membres devraient informer la Commission de

⁽¹⁶⁾ Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (JO L 130 du 1.5.2014, p. 1).

toute modification apportée à cette liste. La Commission devrait publier les listes en ligne. Afin que les points de contact uniques puissent exercer leurs fonctions de coordination au titre de la présente directive, il est toutefois nécessaire que, lorsqu'un État membre décide d'autoriser certains de ses services répressifs compétents à soumettre des demandes d'informations aux points de contact uniques d'autres États membres, cet État membre informe son point de contact unique de toutes les demandes d'informations sortantes ainsi que de toute communication y afférente, en mettant toujours en copie son point de contact unique. Les États membres devraient s'efforcer de limiter au strict minimum la duplication injustifiée de données à caractère personnel.

- (18) Des délais sont nécessaires pour garantir un traitement rapide des demandes d'informations soumises à un point de contact unique. Les délais devraient être clairs et proportionnés et tenir compte du point de savoir si la demande d'informations doit être considérée comme urgente et si elle concerne des informations directement accessibles ou indirectement accessibles. Afin de garantir le respect des délais applicables tout en permettant une certaine souplesse dans les cas objectivement justifiés, il ne devrait être possible, à titre exceptionnel, de déroger à ces délais que si, et dans la mesure où, l'autorité judiciaire compétente de l'État membre qui a reçu la demande a besoin de temps supplémentaire pour se prononcer sur l'octroi de l'autorisation judiciaire nécessaire. Cela pourrait être nécessaire, par exemple, en raison de la large portée ou de la complexité des questions soulevées par la demande d'informations. Afin de veiller, dans toute la mesure possible, à ne pas manquer les occasions cruciales d'intervenir dans des cas spécifiques, l'État membre qui a reçu la demande devrait communiquer toutes les informations demandées dès qu'elles sont détenues par le point de contact unique, même si celles-ci ne sont pas les seules disponibles en rapport avec la demande. Le reste des informations demandées devrait être communiqué par la suite, dès qu'elles sont détenues par le point de contact unique.
- (19) Les points de contact uniques devraient évaluer si les informations demandées sont nécessaires et proportionnées à la réalisation des objectifs de la présente directive et si l'explication des raisons objectives justifiant la demande est suffisamment claire et détaillée pour éviter la communication injustifiée d'informations ou la communication de quantités disproportionnées d'informations.
- (20) Dans des cas exceptionnels, il pourrait être objectivement justifié pour un État membre de refuser une demande d'informations soumise à son point de contact unique. Afin de garantir le bon fonctionnement du système créé par la présente directive dans le respect total de l'état de droit, il convient de définir ces cas de manière exhaustive et de les interpréter de manière restrictive. Toutefois, les règles énoncées dans la présente directive mettent fortement l'accent sur les principes de nécessité et de proportionnalité, offrant ainsi des garanties contre toute utilisation abusive des demandes d'informations, y compris lorsqu'elle entraînerait des violations manifestes des droits fondamentaux. Pour faire preuve de leur diligence générale, les États membres devraient donc toujours vérifier la conformité des demandes qui leur sont soumises au titre de la présente directive avec les principes de nécessité et de proportionnalité et devraient refuser les demandes qu'ils jugent non conformes. Lorsque les motifs du refus de la demande ne concernent que certaines parties des informations demandées, les autres informations devraient être communiquées dans les délais fixés par la présente directive. Afin d'éviter tout refus inutile de demandes d'informations, le point de contact unique ou le service répressif désigné de l'État membre demandeur, selon le cas, devrait fournir, sur demande, les éclaircissements ou les précisions nécessaires au traitement de la demande d'informations. Les délais applicables devraient être suspendus à partir du moment où le point de contact unique ou, le cas échéant, le service répressif désigné de l'État membre demandeur reçoit la demande d'éclaircissements ou de précisions. Toutefois, il ne devrait être possible de demander des éclaircissements ou des précisions que s'ils sont objectivement nécessaires et proportionnés, en ce sens que, s'ils font défaut, la demande d'informations devrait être refusée pour l'un des motifs énumérés dans la présente directive. Dans l'intérêt d'une coopération efficace, il devrait également rester possible de demander les éclaircissements ou les précisions nécessaires dans d'autres situations, sans que cela n'entraîne la suspension des délais.
- (21) Afin de permettre la souplesse nécessaire eu égard aux besoins opérationnels susceptibles de varier dans la pratique, la présente directive devrait prévoir deux autres moyens d'échange d'informations, en plus des demandes d'informations soumises aux points de contact uniques. Le premier est la communication non sollicitée d'informations par un point de contact unique ou un service répressif compétent au point de contact unique ou au service répressif compétent d'un autre État membre sans demande préalable, c'est-à-dire la communication d'informations de sa propre initiative. Le second est la communication d'informations à la suite d'une demande d'informations soumise soit par un point de contact unique, soit par un service répressif compétent, directement au service répressif compétent d'un autre État membre. Pour ces deux moyens d'échange d'informations, la présente directive ne fixe qu'un nombre limité d'exigences minimales, notamment en ce qui concerne l'information des points de contact uniques concernés et, pour ce qui est de la communication d'informations sur propre initiative,

les situations dans lesquelles les informations doivent être communiquées et la langue qu'il convient d'utiliser. Ces exigences devraient également s'appliquer aux situations dans lesquelles un service répressif compétent communique des informations au point de contact unique de son propre État membre afin de communiquer ces informations à un autre État membre, par exemple lorsqu'il est nécessaire de se conformer aux règles énoncées dans la présente directive en ce qui concerne la langue qu'il convient d'utiliser lors de la communication des informations.

- (22) L'exigence d'une autorisation judiciaire préalable pour la communication d'informations, lorsque le droit national la prévoit, constitue une garantie importante qu'il convient de respecter. Cependant, les systèmes juridiques des États membres diffèrent à cet égard et la présente directive ne devrait pas être comprise comme portant atteinte aux règles et aux conditions concernant les autorisations judiciaires préalables prévues par le droit national, outre le fait qu'elle exige que les échanges nationaux et les échanges entre États membres soient traités de manière équivalente, tant sur le fond que sur le plan procédural. En outre, afin de limiter autant que possible les retards et complications éventuels liés à l'application d'une telle exigence, le point de contact unique ou les services répressifs compétents, selon le cas, de l'État membre de l'autorité judiciaire compétente devraient prendre toutes les mesures pratiques et juridiques nécessaires, s'il y a lieu en coopération avec le point de contact unique ou le service répressif désigné de l'État membre demandeur, en vue d'obtenir l'autorisation judiciaire dès que possible. Bien que la base juridique de la présente directive soit limitée à la coopération en matière répressive au titre de l'article 87, paragraphe 2, point a), du traité sur le fonctionnement de l'Union européenne, la présente directive pourrait présenter un intérêt pour les autorités judiciaires.
- (23) Il est particulièrement important que la protection des données à caractère personnel, conformément au droit de l'Union, soit garantie dans le cadre de tous les échanges d'informations effectués au titre de la présente directive. À cette fin, tout traitement de données à caractère personnel par un point de contact unique ou un service répressif compétent au titre de la présente directive devrait être effectué dans le plein respect de la directive (UE) 2016/680 du Parlement européen et du Conseil ⁽¹⁷⁾. En vertu du règlement (UE) 2016/794, l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) doit traiter les données conformément aux règles qui y sont énoncées. Ladite directive et ledit règlement ne sont pas affectés par la présente directive. En particulier, il convient de préciser que toutes les données à caractère personnel échangées par les points de contact uniques et les services répressifs compétents restent limitées aux catégories de données par catégorie de personnes concernées énumérées à l'annexe II, section B, du règlement (UE) 2016/794. Par conséquent, il faut soigneusement distinguer les données relatives aux suspects et celles relatives aux témoins, aux victimes ou aux personnes relevant d'autres catégories, auxquelles s'appliquent des limitations plus strictes. En outre, il convient, dans toute la mesure possible, d'opérer une distinction entre ces données à caractère personnel en fonction de leur degré d'exactitude et de fiabilité. Afin de garantir l'exactitude et la fiabilité, il convient de distinguer les faits des appréciations personnelles. Les points de contact uniques ou, le cas échéant, les services répressifs compétents devraient traiter les demandes d'informations au titre de la présente directive aussi rapidement que possible, pour garantir l'exactitude et la fiabilité des données à caractère personnel, éviter la duplication inutile des données et réduire le risque que ces données soient obsolètes ou qu'ils n'en disposent plus. Lorsqu'il apparaît que les données à caractère personnel sont incorrectes, elles devraient être rectifiées ou effacées ou leur traitement devrait être limité sans retard.
- (24) Afin de permettre une communication adéquate et rapide des informations par les points de contact uniques, soit sur demande, soit de leur propre initiative, il importe que les services répressifs compétents se comprennent. Tous les échanges d'informations, y compris la communication des informations demandées, les refus des demandes d'informations, y compris les motifs de ces refus, et, le cas échéant, les demandes d'éclaircissements ou de précisions et les éclaircissements ou les précisions donnés qui se rapportent à une demande précise, devraient être effectués dans la langue dans laquelle cette demande a été soumise. C'est pourquoi, pour éviter des retards dans la communication des informations demandées en raison des barrières linguistiques et limiter les coûts de traduction, les États membres devraient établir une liste d'une ou de plusieurs langues dans lesquelles leur point de contact unique peut être contacté et dans lesquelles il peut communiquer. Étant donné que l'anglais est une langue largement comprise et utilisée dans la pratique en ce qui concerne la coopération en matière répressive au sein de l'Union, il convient de l'inscrire sur cette liste. Les États membres devraient fournir chacun cette liste, ainsi que ses éventuelles mises à jour, à la Commission. La Commission devrait publier en ligne une compilation de ces listes.

⁽¹⁷⁾ 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).

- (25) Afin de garantir la sûreté et la sécurité des citoyens européens, il est essentiel qu'Europol dispose des informations nécessaires pour remplir son rôle de pôle d'information de l'Union sur la criminalité en soutien des services répressifs compétents. Par conséquent, lorsque des informations sont échangées entre États membres, que ce soit à la suite d'une demande d'informations soumise à un point de contact unique ou à un service répressif compétent ou de la propre initiative de l'un ou l'autre, il convient d'évaluer, au cas par cas, si une copie de la demande d'informations soumise au titre de la présente directive ou des informations échangées au titre de la présente directive devrait être envoyée à Europol conformément à l'article 7, paragraphe 6, du règlement (UE) 2016/794 lorsqu'il s'agit d'une infraction pénale relevant des objectifs d'Europol. Ces évaluations devraient être fondées sur les objectifs d'Europol énoncés dans le règlement (UE) 2016/794 en ce qui concerne le champ d'application de l'infraction pénale. Les États membres ne devraient pas être tenus d'envoyer à Europol une copie de la demande d'informations ou des informations échangées lorsque cela serait contraire aux intérêts essentiels de la sécurité de l'État membre concerné, lorsque cela compromettrait le bon déroulement d'une enquête en cours ou la sécurité d'une personne physique ou lorsque cela divulguerait des informations concernant des organisations ou des activités de renseignement spécifiques dans le domaine de la sûreté nationale. En outre, conformément au principe de la propriété des données et sans préjudice de l'obligation énoncée dans le règlement (UE) 2016/794 concernant la détermination de la finalité du traitement des informations par Europol et des limitations en la matière, les informations initialement obtenues auprès d'un autre État membre ou d'un pays tiers ne devraient être communiquées à Europol que si cet État membre ou ce pays tiers a donné son consentement. Les États membres devraient veiller à ce que le personnel de leur point de contact unique et de leurs services répressifs compétents bénéficie d'une formation et d'un soutien adéquats pour déterminer rapidement et avec précision les informations échangées au titre de la présente directive qui relèvent du mandat d'Europol et lui sont nécessaires pour atteindre ses objectifs.
- (26) Il convient de remédier au problème de la prolifération des canaux de communication utilisés pour la transmission d'informations en matière répressive entre les États membres, car cette prolifération entrave l'échange adéquat et rapide de ces informations et accroît les risques pour la sécurité des données à caractère personnel. L'utilisation de l'application de réseau d'échange sécurisé d'informations (SIENA), gérée et développée par Europol conformément au règlement (UE) 2016/794, devrait, par conséquent, être rendue obligatoire pour toutes les transmissions et communications relevant de la présente directive, y compris pour l'envoi des demandes d'informations aux points de contact uniques et directement aux services répressifs compétents, pour la communication d'informations en réponse à ces demandes ou de la propre initiative des points de contact uniques ou des services répressifs compétents, pour les communications sur les refus des demandes d'informations, pour les éclaircissements et les précisions, ainsi que pour l'envoi de copies des demandes d'informations ou des informations elles-mêmes aux points de contact uniques et à Europol. À cette fin, tous les points de contact uniques et tous les services répressifs compétents susceptibles de participer à des échanges d'informations devraient être directement connectés à SIENA. Afin de permettre aux agents de première ligne, tels que les policiers qui participent à des traques, d'utiliser SIENA, il convient de faire en sorte qu'elle fonctionne également sur des appareils mobiles, s'il y a lieu. À cet égard, il convient de prévoir une brève période de transition afin de permettre le déploiement complet de SIENA, étant donné que cela implique un changement des procédures actuelles dans certains États membres et nécessite une formation du personnel. Afin de tenir compte de la réalité opérationnelle et de ne pas entraver la bonne coopération entre les services répressifs compétents, les États membres devraient pouvoir autoriser leur point de contact unique ou leurs services répressifs compétents à utiliser un autre canal de communication sécurisé dans un nombre limité de situations justifiées. Lorsque les États membres autorisent leur point de contact unique ou leurs services répressifs compétents à utiliser un autre canal de communication en raison de l'urgence de la demande d'informations, ils devraient, dans la mesure du possible et en fonction des besoins opérationnels, revenir à l'utilisation de SIENA une fois l'urgence passée. L'utilisation de SIENA ne devrait pas être obligatoire pour les échanges internes d'informations au sein d'un État membre.
- (27) Afin de simplifier, de faciliter et de mieux gérer les flux d'informations, chaque État membre devrait établir ou désigner un point de contact unique. Les points de contact uniques devraient être compétents pour coordonner et faciliter l'échange d'informations au titre de la présente directive. Chaque État membre devrait notifier à la Commission l'établissement ou la désignation de son point de contact unique, et toute modification à cet égard. La Commission devrait publier ces notifications et leurs éventuelles mises à jour. Les points de contact uniques devraient, en particulier, contribuer à réduire les obstacles aux flux d'informations qui découlent de la fragmentation de la manière dont les services répressifs compétents communiquent entre eux, afin de répondre à la nécessité croissante de lutter conjointement contre la criminalité transfrontière, comme le trafic de stupéfiants, la cybercriminalité, la traite d'êtres humains et le terrorisme. Les points de contact uniques devraient se voir confier un certain nombre de tâches spécifiques minimales et disposer de certaines capacités minimales afin qu'ils soient en mesure de remplir efficacement leurs fonctions de coordination en ce qui concerne l'échange transfrontière d'informations à des fins répressives au titre de la présente directive.

- (28) Les points de contact uniques devraient avoir accès à toutes les informations disponibles dans leur État membre, y compris un accès convivial à toutes les bases de données et plateformes pertinentes de l'Union et internationales, conformément aux modalités précisées dans le droit de l'Union et dans le droit national applicables. Afin de pouvoir satisfaire aux exigences de la présente directive, en particulier celles relatives aux délais, les points de contact uniques devraient être dotés de ressources budgétaires et humaines adéquates, y compris de capacités de traduction appropriées, et fonctionner en permanence. À cet égard, le fait de disposer d'un guichet d'accueil capable de filtrer, de traiter et de canaliser les demandes d'informations entrantes pourrait accroître leur efficacité et leur efficacité. Les points de contact uniques devraient également avoir à leur disposition, à tout moment, des autorités judiciaires compétentes pour accorder les autorisations judiciaires nécessaires. Dans la pratique, cela peut se faire, par exemple, en garantissant la présence physique de ces autorités judiciaires dans les locaux du point de contact unique ou la disponibilité fonctionnelle de ces autorités judiciaires, soit dans les locaux du point de contact unique, soit directement sur appel.
- (29) Pour qu'ils soient en mesure d'exercer efficacement leurs fonctions de coordination au titre de la présente directive, les points de contact uniques devraient être composés de membres du personnel des services répressifs compétents dont la participation est nécessaire à l'échange adéquat et rapide d'informations au titre de la présente directive. Bien qu'il appartienne à chaque État membre de décider précisément de l'organisation et de la composition nécessaires pour satisfaire à cette exigence, les services de police, les services des douanes et d'autres services répressifs compétents responsables de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière, et des points de contact possibles pour les bureaux régionaux et bilatéraux, tels que des fonctionnaires de liaison et des attachés détachés ou affectés dans d'autres États membres et auprès des agences répressives concernées de l'Union, telles qu'Europol, pourraient être représentés au sein des points de contact uniques. Toutefois, dans l'intérêt d'une coordination efficace, au minimum, les points de contact uniques devraient être composés de représentants de l'unité nationale Europol, du bureau SIRENE et du bureau central national Interpol, établis par l'acte juridique de l'Union ou l'accord international applicable et nonobstant le fait que la présente directive ne s'applique pas à l'échange d'informations expressément régi par ces actes juridiques de l'Union.
- (30) Compte tenu des exigences spécifiques de la coopération transfrontière des services répressifs, y compris du traitement d'informations sensibles dans ce contexte, il est essentiel que le personnel des points de contact unique et des services répressifs compétents dispose des connaissances et des compétences nécessaires pour s'acquitter de leurs fonctions au titre de la présente directive de manière licite, efficace et efficace. En particulier, les membres du personnel des points de contact uniques devraient se voir proposer des formations adéquates et régulières, dispensées tant au niveau de l'Union qu'au niveau national, qui correspondent à leurs besoins professionnels et à leurs parcours particuliers et qui facilitent leurs contacts avec les points de contact uniques et les services répressifs compétents d'autres États membres nécessaires pour l'application des règles énoncées dans la présente directive, et ils devraient être encouragés à tirer parti de ces possibilités de formation. À cet égard, il convient d'accorder une attention particulière à la bonne utilisation des outils de traitement des données et des systèmes informatiques, à la transmission des connaissances sur les cadres juridiques nationaux et de l'Union pertinents dans le domaine de la justice et des affaires intérieures, en mettant particulièrement l'accent sur la protection des données à caractère personnel, la coopération en matière répressive et le traitement des informations confidentielles, ainsi qu'aux langues dans lesquelles l'État membre concerné a indiqué que son point de contact unique est en mesure d'échanger des informations, en vue de contribuer à surmonter les barrières linguistiques. Aux fins de ces formations, les États membres devraient également, s'il y a lieu, recourir aux cours et aux outils pertinents proposés par l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL), institué par le règlement (UE) 2015/2219 du Parlement européen et du Conseil⁽¹⁸⁾, envisager la possibilité pour le personnel de passer une semaine à Europol et mettre à profit les offres pertinentes dans le cadre de programmes et de projets financés sur le budget de l'Union, comme le programme d'échange du CEPOL.
- (31) Outre les compétences techniques et les connaissances juridiques, la confiance mutuelle et la compréhension commune sont des conditions préalables à une coopération transfrontière efficace et efficace des services répressifs au titre de la présente directive. Les contacts personnels noués lors d'opérations communes et le partage des compétences acquises facilitent l'instauration d'un climat de confiance et l'émergence d'une culture commune de l'Union en matière répressive. Les États membres devraient également envisager des formations communes et des échanges de personnel axés sur le transfert de connaissances quant aux méthodes de travail, aux approches adoptées lors des enquêtes et aux structures organisationnelles des services répressifs compétents des autres États membres.
- (32) Afin d'accroître la participation aux formations destinées au personnel des points de contact uniques et des services répressifs compétents, les États membres pourraient également envisager des incitations spécifiques pour ce personnel.

⁽¹⁸⁾ Règlement (UE) 2015/2219 du Parlement européen et du Conseil du 25 novembre 2015 sur l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) et remplaçant et abrogeant la décision 2005/681/JAI du Conseil (JO L 319 du 4.12.2015, p. 1).

- (33) Il est nécessaire que les points de contact uniques déploient et exploitent un système électronique unique de gestion des dossiers doté de certaines fonctions et capacités minimales afin de leur permettre d'accomplir chacune des tâches qui leur incombent en vertu de la présente directive de manière efficace et efficiente, notamment en ce qui concerne l'échange d'informations. Le système de gestion des dossiers est un système de gestion des flux permettant aux points de contact uniques de gérer l'échange d'informations. Il est souhaitable que la norme de format universel pour les messages établie par le règlement (UE) 2019/818 du Parlement européen et du Conseil ⁽¹⁹⁾ soit utilisée pour le développement du système de gestion des dossiers.
- (34) Les règles énoncées dans la directive (UE) 2016/680 s'appliquent au traitement des données à caractère personnel dans le système de gestion des dossiers. Le traitement inclut le stockage. Dans un souci de clarté et de protection efficace des données à caractère personnel, les règles énoncées dans ladite directive devraient être précisées dans la présente directive. En particulier, en ce qui concerne l'exigence énoncée dans la directive (UE) 2016/680 selon laquelle les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées, la présente directive devrait préciser que, lorsqu'un point de contact unique reçoit des informations échangées au titre de la présente directive contenant des données à caractère personnel, il ne devrait conserver les données à caractère personnel dans le système de gestion des dossiers que dans la mesure où cela est nécessaire et proportionné à l'accomplissement des tâches qui lui incombent en vertu de la présente directive. Lorsque ce n'est plus le cas, le point de contact unique devrait supprimer irrévocablement les données à caractère personnel du système de gestion des dossiers. Afin de garantir que les données à caractère personnel ne sont conservées que pendant la durée nécessaire et proportionnée, conformément aux règles relatives aux délais de conservation et de réexamen énoncées dans la directive (UE) 2016/680, le point de contact unique devrait réexaminer régulièrement si ces exigences continuent d'être respectées. À cette fin, un premier réexamen devrait avoir lieu au plus tard six mois après la conclusion d'un échange d'informations au titre de la présente directive, c'est-à-dire le moment où la dernière information a été communiquée ou la dernière communication y afférente a été échangée. Les exigences de la présente directive relatives à ce réexamen et à cette suppression ne devraient toutefois pas porter atteinte à la possibilité, pour les autorités nationales compétentes en matière de prévention et de détection des infractions pénales et d'enquêtes en la matière, de conserver les données à caractère personnel dans leurs dossiers nationaux en matière pénale en vertu du droit national, dans le respect du droit de l'Union, en particulier de la directive (UE) 2016/680.
- (35) Afin d'aider les points de contact uniques et les services répressifs compétents pour l'échange d'informations au titre de la présente directive et de promouvoir une culture policière européenne commune entre États membres, les États membres devraient encourager la coopération pratique entre leurs points de contact uniques et leurs services répressifs compétents. En particulier, le Conseil devrait organiser des réunions des responsables des points de contact uniques au moins une fois par an pour qu'ils partagent leurs expériences et leurs bonnes pratiques concernant l'échange d'informations aux fins de la présente directive. D'autres formes de coopération devraient comprendre la rédaction de manuels sur l'échange d'informations en matière répressive, la compilation de fiches d'information nationales sur les informations directement et indirectement accessibles, les points de contact uniques, les services répressifs désignés et les régimes linguistiques, ou d'autres documents sur les procédures communes, la résolution des difficultés liées aux flux de travail, la sensibilisation aux spécificités des cadres juridiques pertinents et l'organisation, s'il y a lieu, de réunions entre les points de contact uniques concernés.
- (36) Afin de permettre le contrôle et l'évaluation nécessaires de l'application de la présente directive, les États membres devraient être tenus de collecter certaines données concernant sa mise en œuvre et de les communiquer chaque année à la Commission. Cette exigence est nécessaire, notamment, pour remédier à l'absence de données comparables quantifiant les échanges transfrontières d'informations pertinents entre les services répressifs compétents et permet également à la Commission de s'acquitter plus aisément de son obligation d'établissement de rapports en ce qui concerne la mise en œuvre de la présente directive. Les données requises à cette fin devraient être générées automatiquement par le système de gestion des dossiers et SIENA.

⁽¹⁹⁾ 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).

- (37) Le caractère transfrontière de la criminalité transnationale et du terrorisme oblige les États membres à compter les uns sur les autres pour prévenir et détecter ces infractions pénales ou mener des enquêtes en la matière. Étant donné que l'objectif de la présente directive, à savoir garantir des flux d'informations adéquats et rapides entre les services répressifs compétents et vers Europol, 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 par l'établissement de règles communes et d'une culture commune en matière d'échange d'informations ainsi que par des outils et des canaux de communication modernes, l'Union peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif.
- (38) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ⁽²⁰⁾ et a rendu un avis le 7 mars 2022.
- (39) La présente directive s'appuie sur les valeurs sur lesquelles l'Union est fondée, énoncées à l'article 2 du traité sur l'Union européenne, notamment l'état de droit, la liberté et la démocratie. Elle respecte également les garanties et droits fondamentaux et observe les principes reconnus par la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), notamment le droit à la liberté et à la sûreté, le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel respectivement prévus par les articles 6, 7 et 8 de la Charte, ainsi que par l'article 16 du traité sur le fonctionnement de l'Union européenne. Tout traitement de données à caractère personnel au titre de la présente directive devrait se limiter à ce qui est absolument nécessaire et proportionné, et être soumis à des conditions claires, à des exigences strictes et à un contrôle effectif des autorités de contrôle nationales établies par la directive (UE) 2016/680 et du Contrôleur européen de la protection des données, le cas échéant conformément à leurs mandats respectifs.
- (40) Conformément aux articles 1^{er} et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application. La présente directive développant 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 la présente directive, s'il la transpose dans son droit interne.
- (41) L'Irlande participe à la présente directive, conformément à l'article 5, paragraphe 1, du protocole n° 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 conformément à l'article 6, paragraphe 2, de la décision 2002/192/CE du Conseil ⁽²¹⁾.
- (42) En ce qui concerne l'Islande et la Norvège, la présente directive constitue 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 ⁽²²⁾, qui relèvent du domaine visé à l'article 1^{er}, point H, de la décision 1999/437/CE du Conseil ⁽²³⁾.
- (43) En ce qui concerne la Suisse, la présente directive constitue 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 ⁽²⁴⁾, qui relèvent du domaine visé à l'article 1^{er}, point H, de la décision 1999/437/CE du Conseil, lue en liaison avec l'article 3 de la décision 2008/149/JAI du Conseil ⁽²⁵⁾.

⁽²⁰⁾ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

⁽²¹⁾ 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).

⁽²²⁾ JO L 176 du 10.7.1999, p. 36.

⁽²³⁾ 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).

⁽²⁴⁾ JO L 53 du 27.2.2008, p. 52.

⁽²⁵⁾ 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).

- (44) En ce qui concerne le Liechtenstein, la présente directive constitue 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 ⁽²⁶⁾, qui relèvent du domaine visé à l'article 1^{er}, point H, de la décision 1999/437/CE du Conseil, lue en liaison avec l'article 3 de la décision 2011/349/UE du Conseil ⁽²⁷⁾,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. La présente directive établit des règles harmonisées relatives à l'échange adéquat et rapide d'informations entre les services répressifs compétents aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière.

En particulier, la présente directive établit des règles sur:

- a) les demandes d'informations soumises aux points de contact uniques établis ou désignés par les États membres, notamment des règles sur la teneur de ces demandes, la communication d'informations en réponse à ces demandes, les langues de travail des points de contact uniques, les délais obligatoires dans lesquels les informations demandées sont communiquées et les motifs pour lesquels ces demandes sont refusées;
- b) la communication par un État membre, de sa propre initiative, d'informations pertinentes aux points de contact uniques ou aux services répressifs compétents d'autres États membres, en particulier les situations dans lesquelles ces informations doivent être communiquées et les modalités de leur communication;
- c) le canal de communication devant être utilisé par défaut pour tous les échanges d'informations au titre de la présente directive et pour les informations qui doivent être communiquées aux points de contact uniques en ce qui concerne les échanges d'informations directement entre les services répressifs compétents;
- d) l'établissement ou la désignation, l'organisation, les tâches, la composition et les capacités du point de contact unique de chaque État membre, y compris des règles sur le déploiement et l'exploitation d'un système électronique unique de gestion des dossiers pour l'accomplissement de ses tâches au titre de la présente directive.

2. La présente directive ne s'applique pas aux échanges d'informations entre les services répressifs compétents aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière, qui sont expressément régis par d'autres actes juridiques de l'Union. Sans préjudice des obligations qui leur incombent en vertu de la présente directive ou d'autres actes juridiques de l'Union, les États membres peuvent adopter ou maintenir des dispositions facilitant davantage l'échange d'informations avec les services répressifs compétents d'autres États membres aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière, y compris au moyen de conventions bilatérales ou multilatérales.

⁽²⁶⁾ JO L 160 du 18.6.2011, p. 21.

⁽²⁷⁾ Décision 2011/349/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 notamment en ce qui concerne la coopération judiciaire en matière pénale et la coopération policière (JO L 160 du 18.6.2011, p. 1).

3. La présente directive n'impose aucune obligation aux États membres:
 - a) d'obtenir des informations par des mesures coercitives;
 - b) de stocker des informations dans le seul but de les communiquer aux services répressifs compétents d'autres États membres;
 - c) de communiquer aux services répressifs compétents d'autres États membres des informations devant être utilisées comme preuves dans une procédure judiciaire.

4. La présente directive n'établit aucun droit d'utiliser les informations communiquées conformément à la présente directive comme preuves dans une procédure judiciaire. L'État membre qui communique les informations peut consentir à leur utilisation comme preuves dans une procédure judiciaire.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

- 1) «service répressif compétent»: tout service de police, de douanes ou autre des États membres compétent en vertu du droit national pour exercer son autorité et prendre des mesures coercitives aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière, ou toute autorité qui participe à des entités conjointes créées entre deux États membres ou plus aux fins de la prévention ou de la détection des infractions pénales ou des enquêtes en la matière, à l'exclusion des agences ou unités traitant particulièrement des questions de sécurité nationale et des fonctionnaires de liaison détachés en vertu de l'article 47 de la convention d'application de l'accord de Schengen;
- 2) «service répressif désigné»: un service répressif compétent autorisé à soumettre des demandes d'informations aux points de contact uniques d'autres États membres conformément à l'article 4, paragraphe 1;
- 3) «infraction pénale grave»: une des infractions suivantes:
 - a) une infraction visée à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil ⁽²⁸⁾;
 - b) une infraction visée à l'article 3, paragraphe 1 ou 2, du règlement (UE) 2016/794;
- 4) «informations»: tout contenu concernant une ou plusieurs personnes physiques ou morales, des faits ou des circonstances qui revêtent un intérêt pour les services répressifs compétents aux fins de l'accomplissement des missions de prévention ou de détection des infractions pénales, ou d'enquête en la matière, qui leur incombent en application du droit national, y compris le renseignement en matière pénale;
- 5) «informations disponibles/dont dispose(nt)»: les informations directement accessibles et les informations indirectement accessibles;
- 6) «informations directement accessibles»: les informations détenues dans une base de données à laquelle le point de contact unique ou un service répressif compétent de l'État membre auquel les informations sont demandées peut accéder directement;
- 7) «informations indirectement accessibles»: les informations qu'un point de contact unique ou un service répressif compétent de l'État membre auquel les informations sont demandées peut obtenir d'autres autorités publiques ou de parties privées établies dans cet État membre, lorsque le droit national le permet et conformément à celui-ci, sans mesures coercitives;
- 8) «données à caractère personnel»: les données à caractère personnel au sens de l'article 3, point 1, de la directive (UE) 2016/680.

⁽²⁸⁾ 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).

*Article 3***Principes relatifs à l'échange d'informations**

Chaque État membre veille, en ce qui concerne tous les échanges d'informations au titre de la présente directive:

- a) à ce que les informations disponibles puissent être communiquées au point de contact unique ou aux services répressifs compétents d'autres États membres (principe de disponibilité);
- b) à ce que les conditions applicables aux demandes d'informations aux points de contact uniques ou aux services répressifs compétents d'autres États membres et celles régissant la communication d'informations à ceux-ci soient équivalentes à celles applicables aux demandes et à la communication d'informations similaires au sein de cet État membre (principe d'accès équivalent);
- c) à protéger les informations communiquées à son point de contact unique ou à ses services répressifs compétents qui sont marquées confidentielles conformément aux exigences énoncées dans son droit national garantissant un niveau de confidentialité similaire à celui du droit national de l'État membre ayant communiqué les informations (principe de confidentialité);
- d) lorsque les informations demandées ont été initialement obtenues auprès d'un autre État membre ou d'un pays tiers, à ce qu'il ne communique ces informations à un autre État membre ou à Europol qu'avec le consentement de l'État membre ou du pays tiers qui a initialement communiqué les informations et conformément aux conditions imposées par ceux-ci à leur utilisation (principe de propriété des données);
- e) à ce que les données à caractère personnel échangées au titre de la présente directive qui s'avèrent inexactes, incomplètes ou plus à jour soient effacées ou rectifiées ou que leur traitement soit limité, selon le cas, et que tout destinataire en soit informé sans tarder (principe de fiabilité des données).

CHAPITRE II

ÉCHANGE D'INFORMATIONS PAR L'INTERMÉDIAIRE DES POINTS DE CONTACT UNIQUES*Article 4***Demandes d'informations aux points de contact uniques**

1. Les États membres veillent à ce que les demandes d'informations que leur point de contact unique et, lorsque leur droit national le prévoit, leurs services répressifs désignés, soumettent au point de contact unique d'un autre État membre respectent les exigences énoncées aux paragraphes 2 à 6.

Les États membres soumettent à la Commission une liste de leurs services répressifs désignés. Les États membres informent la Commission de toute modification apportée à cette liste. La Commission publie en ligne une compilation de ces listes et la tient à jour.

Les États membres veillent à ce que leurs services répressifs désignés, lorsqu'ils soumettent une demande d'informations au point de contact unique d'un autre État membre, envoient en même temps une copie de cette demande d'informations à leur point de contact unique.

2. Les États membres peuvent autoriser leurs services répressifs désignés à ne pas envoyer, au cas par cas, une copie d'une demande d'informations à leur point de contact unique en même temps qu'ils la soumettent au point de contact unique d'un autre État membre conformément au paragraphe 1, lorsque cela compromettrait un ou plusieurs des éléments suivants:

- a) une enquête en cours hautement sensible pour laquelle le traitement de l'information requiert un niveau de confidentialité approprié;
- b) les affaires de terrorisme n'impliquant pas la gestion de situations d'urgence ou de crise;
- c) la sécurité d'une personne.

3. Les États membres veillent à ce que les demandes d'informations ne soient soumises au point de contact unique d'un autre État membre que lorsqu'il existe des raisons objectives de penser que:

- a) les informations demandées sont nécessaires et proportionnées pour réaliser l'objectif mentionné à l'article 1^{er}, paragraphe 1, premier alinéa; et que
- b) cet autre État membre dispose des informations demandées.

4. Les États membres veillent à ce que toute demande d'informations soumise au point de contact unique d'un autre État membre précise si elle revêt un caractère urgent et, le cas échéant, indique les raisons de cette urgence. Ces demandes d'informations sont considérées comme urgentes si, eu égard à l'ensemble des faits et circonstances pertinents de l'espèce, il existe des raisons objectives de penser que les informations demandées remplissent l'un ou plusieurs des critères suivants:

- a) elles sont essentielles à la prévention d'une menace immédiate et grave pour la sécurité publique d'un État membre;
- b) elles sont nécessaires pour prévenir une menace imminente pour la vie ou l'intégrité physique d'une personne;
- c) elles sont nécessaires à l'adoption d'une décision susceptible d'impliquer le maintien de mesures restrictives qui s'apparentent à une privation de liberté;
- d) elles présentent un risque imminent de perdre de leur intérêt si elles ne sont pas communiquées d'urgence et sont considérées comme importantes pour la prévention ou la détection d'infractions pénales, ou les enquêtes en la matière.

5. Les États membres veillent à ce que les demandes d'informations soumises au point de contact unique d'un autre État membre contiennent toutes les données nécessaires pour en permettre le traitement adéquat et rapide conformément à la présente directive, dont au moins les éléments suivants:

- a) une spécification des informations demandées qui soit aussi détaillée que cela est raisonnablement possible dans les circonstances données;
- b) une description de la finalité pour laquelle les informations sont demandées, y compris une description des faits et la mention de l'infraction sous-jacente;
- c) les raisons objectives qui donnent à penser que l'État membre qui a reçu la demande dispose des informations demandées;
- d) une explication du lien entre la finalité de la demande d'informations et toute personne physique ou morale ou toute entité à laquelle les informations se rapportent, le cas échéant;
- e) les raisons pour lesquelles la demande est considérée comme urgente, le cas échéant, conformément au paragraphe 4;
- f) les restrictions quant à l'utilisation des informations contenues dans la demande à des fins autres que celles pour lesquelles elle a été soumise.

6. Les États membres veillent à ce que les demandes d'informations soient soumises au point de contact unique d'un autre État membre dans l'une des langues figurant sur la liste établie par cet autre État membre conformément à l'article 11.

Article 5

Communication d'informations en réponse à des demandes soumises aux points de contact uniques

1. Les États membres veillent à ce que leur point de contact unique communique les informations demandées conformément à l'article 4 dès que possible et, en tout état de cause, dans les délais suivants, selon le cas:

- a) huit heures pour les demandes urgentes portant sur des informations directement accessibles;
- b) trois jours civils pour les demandes urgentes portant sur des informations indirectement accessibles;
- c) sept jours civils pour toutes les autres demandes.

Les délais prévus au premier alinéa commencent à courir au moment de la réception de la demande d'informations.

2. Lorsque, selon son droit national, conformément à l'article 9, un État membre ne peut communiquer les informations demandées qu'après l'obtention d'une autorisation judiciaire, cet État membre peut déroger aux délais énoncés au paragraphe 1 du présent article dans la mesure où cela est nécessaire pour obtenir cette autorisation. En pareils cas, les États membres veillent à ce que leur point de contact unique s'acquitte des deux obligations suivantes:

- a) informer immédiatement le point de contact unique ou, le cas échéant, le service répressif désigné de l'État membre demandeur du retard attendu, en précisant la durée et les motifs dudit retard;
- b) tenir le point de contact unique ou, le cas échéant, le service répressif désigné de l'État membre demandeur ultérieurement informé et communiquer les informations demandées dès que possible après obtention de l'autorisation judiciaire.

3. Les États membres veillent à ce que leur point de contact unique communique les informations demandées conformément à l'article 4 au point de contact unique ou, le cas échéant, au service répressif désigné de l'État membre demandeur, dans la langue dans laquelle la demande d'informations a été soumise conformément à l'article 4, paragraphe 6.

Les États membres veillent à ce que leur point de contact unique envoie une copie des informations demandées au point de contact unique de l'État membre demandeur en même temps qu'il communique les informations demandées au service répressif désigné de cet État membre.

Les États membres peuvent autoriser leur point de contact unique à ne pas envoyer, en même temps qu'il communique les informations aux services répressifs désignés d'un autre État membre conformément au présent article, une copie de ces informations au point de contact unique de cet autre État membre lorsque cela compromettrait un ou plusieurs des éléments suivants:

- a) une enquête en cours hautement sensible pour laquelle le traitement de l'information requiert un niveau de confidentialité approprié;
- b) les affaires de terrorisme n'impliquant pas la gestion de situations d'urgence ou de crise;
- c) la sécurité d'une personne.

Article 6

Refus de demandes d'informations

1. Les États membres veillent à ce que leur point de contact unique ne refuse de communiquer les informations demandées conformément à l'article 4 que dans la mesure où l'un des motifs suivants s'applique:

- a) le point de contact unique et les services répressifs compétents de l'État membre qui a reçu la demande ne disposent pas des informations demandées;
- b) la demande d'informations ne satisfait pas aux exigences énoncées à l'article 4;
- c) l'autorisation judiciaire exigée en vertu du droit national de l'État membre qui a reçu la demande conformément à l'article 9 a été refusée;
- d) les informations demandées constituent des données à caractère personnel autres que celles relevant des catégories de données à caractère personnel visées à l'article 10, point b);
- e) les informations demandées se sont révélées inexactes, incomplètes ou ne sont plus à jour et ne peuvent être communiquées conformément à l'article 7, paragraphe 2, de la directive (UE) 2016/680;
- f) il existe des raisons objectives de penser que la communication des informations demandées:
 - i) serait contraire ou porterait atteinte aux intérêts essentiels de la sécurité nationale de l'État membre qui a reçu la demande;
 - ii) compromettrait le bon déroulement d'une enquête en cours en matière pénale ou la sécurité d'une personne physique;
 - iii) porterait indûment atteinte aux intérêts importants protégés d'une personne morale;

- g) la demande concerne:
- i) une infraction pénale punissable d'une peine d'emprisonnement maximale d'un an ou moins en vertu du droit de l'État membre qui a reçu la demande; ou
 - ii) une affaire qui ne constitue pas une infraction pénale en vertu du droit de l'État membre qui a reçu la demande;
- h) les informations demandées ont été initialement obtenues d'un autre État membre ou d'un pays tiers, et l'État membre ou le pays tiers en question n'a pas consenti à la communication des informations.

Les États membres font preuve de diligence raisonnable pour évaluer si la demande d'informations soumise à leur point de contact unique est conforme aux exigences énoncées à l'article 4, notamment en ce qui concerne l'existence d'une violation manifeste des droits fondamentaux.

Tout refus de demande d'informations ne concerne que la partie des informations demandées à laquelle se rapportent les motifs énoncés au premier alinéa et est, le cas échéant, sans préjudice de l'obligation de communiquer les autres parties des informations conformément à la présente directive.

2. Les États membres veillent à ce que leur point de contact unique informe le point de contact unique ou, le cas échéant, le service répressif désigné de l'État membre demandeur du refus de la demande d'informations, en précisant les motifs de ce refus, dans les délais prévus à l'article 5, paragraphe 1.

3. S'il y a lieu, les États membres veillent à ce que leur point de contact unique sollicite immédiatement auprès du point de contact unique ou, le cas échéant, du service répressif désigné de l'État membre demandeur, les éclaircissements ou précisions nécessaires au traitement d'une demande d'informations qui, à défaut, devrait être refusée.

Les délais indiqués à l'article 5, paragraphe 1, sont suspendus à partir du moment où le point de contact unique ou, le cas échéant, le service répressif désigné de l'État membre demandeur reçoit la demande d'éclaircissements ou de précisions, jusqu'au moment où les éclaircissements ou précisions demandés sont apportés.

4. Les refus de demandes d'informations, les motifs de tels refus, les demandes d'éclaircissements ou de précisions et les éclaircissements ou précisions visés au paragraphe 3 du présent article ainsi que toute autre communication relative à une demande d'informations soumise au point de contact unique d'un autre État membre, sont communiqués dans la langue dans laquelle cette demande a été soumise conformément à l'article 4, paragraphe 6.

CHAPITRE III

AUTRES ÉCHANGES D'INFORMATIONS

Article 7

Communication d'informations sur propre initiative

1. Les États membres peuvent communiquer, de leur propre initiative, par l'intermédiaire de leur point de contact unique ou de leurs services répressifs compétents, les informations dont ils disposent aux points de contact uniques ou aux services répressifs compétents d'autres États membres lorsqu'il existe des raisons objectives de penser que ces informations pourraient présenter un intérêt pour ces autres États membres aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière.

2. Les États membres veillent à ce que leur point de contact unique ou leurs services répressifs compétents communiquent, de leur propre initiative, les informations dont ils disposent au point de contact unique ou aux services répressifs compétents d'autres États membres lorsqu'il existe des raisons objectives de penser que ces informations pourraient présenter un intérêt pour ces autres États membres aux fins de la prévention ou de la détection des infractions pénales graves, ou des enquêtes en la matière. Toutefois, une telle obligation n'existe pas dès lors que les motifs visés à l'article 6, paragraphe 1, point c) ou f), s'appliquent à ces informations.

3. Les États membres veillent à ce que, lorsque leur point de contact unique ou leurs services répressifs compétents communiquent des informations de leur propre initiative au point de contact unique d'un autre État membre, conformément au paragraphe 1 ou 2, ils le fassent dans l'une des langues figurant sur la liste établie par cet autre État membre conformément à l'article 11.

Les États membres veillent à ce que, lorsque leur point de contact unique communique des informations de sa propre initiative au service répressif compétent d'un autre État membre, il envoie en même temps une copie de ces informations au point de contact unique de cet autre État membre.

Les États membres veillent à ce que, lorsque leurs services répressifs compétents communiquent de leur propre initiative des informations à un autre État membre, ils envoient en même temps une copie de ces informations au point de contact unique de leur État membre et, le cas échéant, au point de contact unique de cet autre État membre.

4. Les États membres peuvent autoriser leurs services répressifs compétents à ne pas envoyer, en même temps qu'ils communiquent des informations au point de contact unique ou aux services répressifs compétents d'un autre État membre conformément au présent article, une copie de ces informations au point de contact unique de leur État membre ou au point de contact unique de cet autre État membre, lorsque cela compromettrait un ou plusieurs des éléments suivants:

- a) une enquête en cours hautement sensible pour laquelle le traitement de l'information requiert un niveau de confidentialité approprié;
- b) les affaires de terrorisme n'impliquant pas la gestion de situations d'urgence ou de crise;
- c) la sécurité d'une personne.

Article 8

Échange d'informations à la suite de demandes soumises directement aux services répressifs compétents

1. Lorsque leur point de contact unique soumet une demande d'informations directement à un service répressif compétent d'un autre État membre, les États membres veillent à ce qu'il envoie en même temps une copie de cette demande au point de contact unique de cet autre État membre. Les États membres veillent à ce que, lorsqu'un de leurs services répressifs compétents communique des informations en réponse à une telle demande, il envoie en même temps une copie de ces informations au point de contact unique de son État membre.

2. Les États membres veillent à ce que, lorsqu'un de leurs services répressifs compétents soumet une demande d'informations ou communique des informations en réponse à une telle demande directement à un service répressif compétent d'un autre État membre, il envoie en même temps une copie de cette demande ou de ces informations au point de contact unique de son État membre et au point de contact unique de cet autre État membre.

3. Les États membres peuvent autoriser leur point de contact unique ou leurs services répressifs compétents à ne pas envoyer de copies des demandes ou des informations visées au paragraphe 1 ou 2 lorsque cela compromettrait un ou plusieurs des éléments suivants:

- a) une enquête en cours hautement sensible pour laquelle le traitement de l'information requiert un niveau de confidentialité approprié;
- b) les affaires de terrorisme n'impliquant pas la gestion de situations d'urgence ou de crise;
- c) la sécurité d'une personne.

CHAPITRE IV

RÈGLES SUPPLÉMENTAIRES RELATIVES À LA COMMUNICATION D'INFORMATIONS AU TITRE DES CHAPITRES II ET III*Article 9***Autorisation judiciaire**

1. Un État membre n'exige pas d'autorisation judiciaire pour la communication d'informations au point de contact unique ou aux services répressifs compétents d'autres États membres au titre du chapitre II ou III, lorsque son droit national n'exige pas une telle autorisation judiciaire pour une communication d'informations similaires au sein de cet État membre.
2. Lorsque leur droit national exige une autorisation judiciaire pour la communication d'informations au point de contact unique ou aux services répressifs compétents d'autres États membres au titre du chapitre II ou III, les États membres veillent à ce que leur point de contact unique ou leurs services répressifs compétents prennent immédiatement toutes les mesures nécessaires, conformément à leur droit national, pour obtenir cette autorisation judiciaire dès que possible.
3. Les demandes d'autorisation judiciaire visées au paragraphe 2 font l'objet d'une appréciation et d'une décision conformément au droit national de l'État membre de l'autorité judiciaire compétente.

*Article 10***Règles supplémentaires relatives aux informations constituant des données à caractère personnel**

Lorsque leur point de contact unique ou leurs services répressifs compétents communiquent au titre du chapitre II ou III des informations qui constituent des données à caractère personnel, les États membres veillent à ce que:

- a) les données à caractère personnel soient exactes, complètes et à jour, conformément à l'article 7, paragraphe 2, de la directive (UE) 2016/680;
- b) les catégories de données à caractère personnel communiquées par catégorie de personnes concernées restent limitées à celles énumérées à l'annexe II, section B, du règlement (UE) 2016/794 et soient nécessaires et proportionnées aux fins de la demande;
- c) leur point de contact unique ou leurs services répressifs compétents communiquent aussi, en même temps et dans la mesure du possible, les éléments nécessaires permettant au point de contact unique ou au service répressif compétent de l'autre État membre d'apprécier le degré d'exactitude, d'exhaustivité et de fiabilité des données à caractère personnel, ainsi que la mesure dans laquelle ces données sont à jour.

*Article 11***Liste des langues**

1. Les États membres établissent et tiennent à jour une liste comportant une ou plusieurs des langues dans lesquelles leur point de contact unique est en mesure d'échanger des informations. Cette liste comprend l'anglais.
2. Les États membres fournissent la liste visée au paragraphe 1, ainsi que ses éventuelles mises à jour, à la Commission. La Commission publie en ligne une compilation de ces listes et tient celle-ci à jour.

*Article 12***Communication d'informations à Europol**

1. Les États membres veillent à ce que, lorsque leur point de contact unique ou leurs services répressifs compétents adressent des demandes d'informations, communiquent des informations en réponse à ces demandes ou transmettent des informations de leur propre initiative au titre du chapitre II ou III de la présente directive, le personnel de leur point de contact unique ou de leurs services répressifs compétents évalue également, au cas par cas et sous réserve de l'article 7, paragraphe 7, du règlement (UE) 2016/794, s'il est nécessaire d'envoyer à Europol une copie de la demande d'informations ou des informations communiquées, dans la mesure où les informations sur lesquelles porte la communication concernent des infractions pénales relevant des objectifs d'Europol énoncés à l'article 3 du règlement (UE) 2016/794.

2. Les États membres veillent à ce que, lorsqu'une copie d'une demande d'informations ou une copie des informations est envoyée à Europol en vertu du paragraphe 1 du présent article, les finalités du traitement des informations et toute restriction éventuelle à ce traitement en vertu de l'article 19 du règlement (UE) 2016/794 soient dûment communiquées à Europol. Les États membres veillent à ce que les informations initialement obtenues d'un autre État membre ou d'un pays tiers ne soient transmises à Europol en vertu du paragraphe 1 du présent article que si cet autre État membre ou ce pays tiers a donné son consentement.

Article 13

Canal de communication sécurisé

1. Les États membres veillent à ce que leur point de contact unique ou leurs services répressifs compétents utilisent l'application de réseau d'échange sécurisé d'informations d'Europol (SIENA) pour adresser des demandes d'informations, communiquer des informations en réponse à ces demandes ou transmettre des informations de leur propre initiative au titre du chapitre II ou III ou de l'article 12.

2. Les États membres peuvent autoriser leur point de contact unique ou leurs services répressifs compétents à ne pas utiliser SIENA pour adresser des demandes d'informations, communiquer des informations en réponse à ces demandes ou transmettre des informations de leur propre initiative au titre du chapitre II ou III ou de l'article 12 dans un ou plusieurs des cas suivants:

- a) l'échange d'informations nécessite le concours de pays tiers ou d'organisations internationales ou il existe des raisons objectives de penser qu'un tel concours sera nécessaire à un stade ultérieur, y compris par le canal de communication d'Interpol;
- b) l'urgence de la demande d'informations nécessite l'utilisation temporaire d'un autre canal de communication;
- c) un incident technique ou opérationnel inattendu empêche leur point de contact unique ou leur autorité répressive compétente d'utiliser SIENA pour échanger les informations.

3. Les États membres veillent à ce que leur point de contact unique et tous leurs services répressifs compétents susceptibles de participer à l'échange d'informations au titre de la présente directive soient directement connectés à SIENA, y compris, s'il y a lieu, via des appareils mobiles.

CHAPITRE V

POINT DE CONTACT UNIQUE POUR L'ÉCHANGE D'INFORMATIONS ENTRE ÉTATS MEMBRES

Article 14

Établissement ou désignation et tâches et capacités des points de contact uniques

1. Chaque État membre établit ou désigne un point de contact unique. Le point de contact unique est l'entité centrale chargée de coordonner et de faciliter l'échange d'informations au titre de la présente directive.

2. Les États membres veillent à ce que leur point de contact unique dispose du pouvoir d'action et des moyens nécessaires pour accomplir au moins l'ensemble des tâches suivantes:

- a) recevoir et évaluer les demandes d'informations soumises conformément à l'article 4 dans les langues notifiées conformément à l'article 11, paragraphe 2;
- b) transmettre les demandes d'informations aux services répressifs compétents et, si nécessaire, coordonner entre ces derniers le traitement de ces demandes et la communication d'informations en réponse à ces demandes;
- c) coordonner l'analyse et structurer les informations en vue de les communiquer aux points de contact uniques et, le cas échéant, aux services répressifs compétents d'autres États membres;

- d) communiquer, sur demande ou de sa propre initiative, des informations à d'autres États membres, conformément aux articles 5 et 7;
 - e) refuser de communiquer des informations conformément à l'article 6 et, si nécessaire, demander des éclaircissements ou des précisions conformément à l'article 6, paragraphe 3;
 - f) adresser des demandes d'informations aux points de contact uniques d'autres États membres conformément à l'article 4 et, s'il y a lieu, fournir des éclaircissements ou des précisions conformément à l'article 6, paragraphe 3.
3. Les États membres veillent à ce que:
- a) leur point de contact unique:
 - i) ait accès à toutes les informations dont disposent leurs services répressifs compétents, dans la mesure où cela est nécessaire à l'exécution des tâches qui lui incombent en vertu de la présente directive;
 - ii) accomplisse ses tâches 24 heures sur 24 et sept jours sur sept;
 - iii) soit doté du personnel qualifié, des outils opérationnels appropriés, des ressources techniques et financières, des infrastructures et des capacités, y compris en matière de traduction, nécessaires à l'accomplissement de ses tâches de manière adéquate, efficace et rapide conformément à la présente directive, y compris, selon le cas, dans les délais fixés à l'article 5, paragraphe 1;
 - b) les autorités judiciaires compétentes pour accorder les autorisations judiciaires requises en droit national conformément à l'article 9 soient joignables par le point de contact unique 24 heures sur 24 et sept jours sur sept.
4. Dans le mois qui suit l'établissement ou la désignation de leur point de contact unique, les États membres en font notification à la Commission. Ils informent la Commission de tout changement concernant leur point de contact unique.

La Commission publie ces notifications, et leurs éventuelles mises à jour, au *Journal officiel de l'Union européenne*.

Article 15

Organisation, composition et formation

1. Les États membres déterminent l'organisation et la composition de leur point de contact unique de manière que ce dernier puisse s'acquitter des tâches qui lui incombent en vertu de la présente directive de manière efficiente et efficace.
2. Les États membres veillent à ce que leur point de contact unique soit composé de membres du personnel de leurs services répressifs compétents dont la participation est nécessaire à l'échange adéquat et rapide d'informations au titre de la présente directive, dont au moins les structures suivantes, dans la mesure où l'État membre concerné est tenu par le droit ou l'accord international applicable d'établir ou de désigner ces unités ou bureaux:
 - a) l'unité nationale Europol instituée par l'article 7 du règlement (UE) 2016/794;
 - b) le bureau SIRENE institué par l'article 7, paragraphe 2, du règlement (UE) 2018/1862;
 - c) le bureau central national Interpol institué par l'article 32 du statut de l'Organisation internationale de police criminelle – Interpol.
3. Les États membres veillent à ce que le personnel de leur point de contact unique soit suffisamment qualifié pour remplir les fonctions qui lui incombent en vertu de la présente directive. À cette fin, les États membres donnent au personnel de leur point de contact unique l'accès à une formation adéquate et régulière, notamment dans les domaines suivants:
 - a) l'utilisation des outils de traitement des données utilisés par le point de contact unique, en particulier SIENA et le système de gestion des dossiers;
 - b) l'application du droit de l'Union et du droit national se rapportant aux activités du point de contact unique au titre de la présente directive, notamment en ce qui concerne la protection des données à caractère personnel, y compris la directive (UE) 2016/680, la coopération transfrontière entre les services répressifs, y compris la présente directive et le règlement (UE) 2016/794, et le traitement des informations confidentielles;

- c) l'utilisation des langues figurant sur la liste établie par l'État membre concerné conformément à l'article 11.

Article 16

Système de gestion des dossiers

1. Les États membres veillent à ce que leur point de contact unique déploie et exploite un système électronique unique de gestion des dossiers en tant que répertoire lui permettant d'accomplir les tâches qui lui incombent en vertu de la présente directive. Le système de gestion des dossiers est doté au moins de l'ensemble des fonctions et capacités suivantes:

- a) enregistrement des demandes d'informations entrantes et sortantes visées aux articles 5 et 8, ainsi que de toute autre communication relative à ces demandes avec les points de contact uniques et, le cas échéant, les services répressifs compétents d'autres États membres, y compris les informations sur les refus de demandes d'informations ainsi que les demandes et communications d'éclaircissements ou de précisions prévues à l'article 6, paragraphes 2 et 3, respectivement;
- b) enregistrement des communications entre le point de contact unique et les services répressifs compétents, en application de l'article 14, paragraphe 2, point b);
- c) enregistrement des informations communiquées au point de contact unique et, le cas échéant, aux services répressifs compétents d'autres États membres, conformément aux articles 5, 7 et 8;
- d) recoupement des demandes d'informations entrantes, visées aux articles 5 et 8, avec les informations dont dispose le point de contact unique, y compris les informations communiquées conformément à l'article 5, paragraphe 3, deuxième alinéa, et à l'article 7, paragraphe 3, deuxième alinéa, et avec les autres informations pertinentes enregistrées dans le système de gestion des dossiers;
- e) suivi adéquat et rapide des demandes d'informations entrantes visées à l'article 4, notamment en vue de respecter les délais de communication des informations demandées fixés à l'article 5;
- f) interopérabilité avec l'application SIENA, afin notamment que les communications entrantes qui transitent par cette application puissent être directement enregistrées dans le système de gestion des dossiers et que les communications sortantes qui transitent par cette application puissent être directement envoyées à partir dudit système;
- g) production de statistiques sur les échanges d'informations au titre de la présente directive à des fins d'évaluation et de suivi, notamment aux fins de l'article 18;
- h) journalisation des accès et des autres opérations de traitement pour ce qui est des informations contenues dans le système de gestion des dossiers, à des fins de responsabilité et de cybersécurité, conformément à l'article 25 de la directive (UE) 2016/680.

2. Les États membres veillent à ce que tous les risques en matière de cybersécurité liés au système de gestion des dossiers, notamment en ce qui concerne son architecture, sa gouvernance et son contrôle, soient gérés et traités de manière prudente et efficace et que des garanties adéquates contre les accès non autorisés et les abus soient prévues.

3. Les États membres veillent à ce que le système de gestion des dossiers ne contienne des données à caractère personnel que pour la durée nécessaire et proportionnée à l'exécution, par le point de contact unique, des tâches qui lui sont assignées en vertu de la présente directive, puis à ce que les données à caractère personnel qu'il contient soient irrévocablement supprimées.

4. Les États membres veillent à ce que leur point de contact unique examine, pour la première fois au plus tard six mois après la conclusion d'un échange d'informations, puis régulièrement, le respect du paragraphe 3.

Article 17

Coopération entre les points de contact uniques

1. Les États membres favorisent une coopération concrète entre leurs points de contact uniques et les services répressifs compétents aux fins de la présente directive.

2. Les États membres veillent à ce que les responsables des points de contact uniques se réunissent au moins une fois par an afin d'évaluer la qualité de la coopération entre leurs services, de discuter des mesures techniques ou organisationnelles nécessaires en cas de difficultés et de clarifier les procédures si nécessaire.

CHAPITRE VI

DISPOSITIONS FINALES

Article 18

Statistiques

1. Au plus tard le 1^{er} mars de chaque année, chaque État membre fournit à la Commission des statistiques sur les échanges d'informations qui ont eu lieu au cours de l'année civile précédente avec les autres États membres au titre de la présente directive.

2. Chaque État membre veille à ce que les statistiques visées au paragraphe 1 portent au minimum sur:

- a) le nombre de demandes d'informations soumises par leur point de contact unique et, s'il y a lieu, par leurs services répressifs compétents;
- b) le nombre de demandes d'informations qui ont été reçues et auxquelles il a été répondu par leur point de contact unique et par leurs services répressifs compétents, ventilé selon le caractère urgent ou non de ces demandes et par État membre demandeur;
- c) le nombre de demandes d'informations refusées en vertu de l'article 6, ventilé par État membre demandeur et par motif de refus;
- d) le nombre de cas dans lesquels il a été dérogé aux délais prévus à l'article 5, paragraphe 1, parce qu'il était nécessaire d'obtenir une autorisation judiciaire conformément à l'article 5, paragraphe 2, ventilé par État membre ayant soumis les demandes d'informations concernées.

3. La Commission compile les statistiques minimales fournies par les États membres en vertu du paragraphe 2 et les met à la disposition du Parlement européen et du Conseil.

Article 19

Établissement de rapports

1. Au plus tard le 12 juin 2026, puis tous les cinq ans après le 12 juin 2027, la Commission soumet au Parlement européen et au Conseil un rapport évaluant la mise en œuvre de la présente directive et contenant des informations détaillées sur sa mise en œuvre par chaque État membre. Lors de l'établissement de ce rapport, la Commission accorde une attention particulière à l'efficacité avec laquelle les services répressifs compétents ont échangé des informations, aux motifs pour lesquels les demandes d'informations ont été refusées, notamment lorsque les demandes ne relèvent pas des objectifs de la présente directive, et au respect des dispositions relatives à la protection des données et à la communication d'informations à Europol.

2. Au plus tard le 12 juin 2027, puis tous les cinq ans, la Commission soumet au Parlement européen et au Conseil un rapport évaluant l'efficacité de la présente directive, en particulier son incidence sur la coopération des services répressifs, les obligations prévues à l'article 14, paragraphe 3, point a) iii), et la protection des données à caractère personnel. La Commission tient compte des informations communiquées par les États membres et de toute autre information pertinente liée à la transposition et à la mise en œuvre de la présente directive, y compris, le cas échéant, aux obstacles pratiques qui entravent sa mise en œuvre effective. Sur la base de cette évaluation, la Commission décide des actions de suivi appropriées, y compris, le cas échéant, d'une proposition législative.

*Article 20***Modification de la convention d'application de l'accord de Schengen**

À compter du 12 décembre 2024, les parties des articles 39 et 46 de la convention d'application de l'accord de Schengen qui n'ont pas été remplacées par la décision-cadre 2006/960/JAI sont remplacées par la présente directive dans la mesure où ces articles concernent l'échange d'informations relevant du champ d'application de la présente directive.

*Article 21***Abrogation**

La décision-cadre 2006/960/JAI est abrogée à partir du 12 décembre 2024.

Les références faites à la décision-cadre abrogée s'entendent comme faites à la présente directive et sont à lire selon le tableau de correspondance figurant à l'annexe.

*Article 22***Transposition**

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 12 décembre 2024. Ils en informent immédiatement la Commission.

Par dérogation au premier alinéa, les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à l'article 13 au plus tard le 12 juin 2027. Ils en informent immédiatement la Commission.

Lorsque les États membres adoptent les dispositions visées aux premier et second alinéas, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

*Article 23***Entrée en vigueur**

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

*Article 24***Destinataires**

Les États membres sont destinataires de la présente directive conformément aux traités.

Fait à Strasbourg, le 10 mai 2023.

Par le Parlement européen
La présidente
R. METSOLA

Par le Conseil
La présidente
J. ROSWALL

ANNEXE

TABLEAU DE CORRESPONDANCE

Décision-cadre 2006/960/JAI du Conseil	Présente directive
Article 1 ^{er}	Article 1 ^{er}
Article 2	Article 2
Article 3	Articles 3 et 9
Article 4	Article 5
Article 5	Article 4
Article 6	Articles 11, 12 et 13
Article 7	Articles 7 et 8
Article 8	Article 10
Article 9	Article 3
Article 10	Article 6
Article 11	Article 21
Article 12	Article 19
Article 13	Article 22