Journal officiel
de l'Union européenne

FR
Série L

2025/2447

5.12.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2447 DE LA COMMISSION

du 4 décembre 2025

portant modalités d'application du règlement (UE) 2018/1727 du Parlement européen et du Conseil en ce qui concerne les spécifications, mesures et autres exigences techniques relatives à l'établissement et à l'utilisation du système informatique décentralisé aux fins d'un traitement et d'une communication sécurisés des informations

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil [1], et notamment son article 22 *bis*, paragraphe 3, et son article 22 *ter*, paragraphe 1, points a), b), c) et d),

considérant ce qui suit:

(1) Le règlement (UE) 2018/1727 fixe le cadre de la nouvelle infrastructure numérique interne d'Eurojust et de l'établissement d'un système décentralisé de communication numérique sécurisée entre les autorités nationales compétentes des États membres et Eurojust.

(2) La communication numérique sécurisée doit s'effectuer au moyen du système informatique décentralisé. Afin de mettre en place le système informatique décentralisé, il y a lieu d'établir des spécifications techniques définissant les méthodes et protocoles de communication, les mesures techniques garantissant des normes minimales de sécurité de l'information et la sécurité en général, ainsi que des objectifs minimaux en matière de disponibilité pour la mise en œuvre de ce système.

(3) Conformément à l'article 22 *bis*, paragraphe 1, du règlement (UE) 2018/1727, le système informatique décentralisé doit comprendre les systèmes informatiques des États membres et d'Eurojust, ainsi que des points d'accès e-CODEX interopérables, par l'intermédiaire desquels ces systèmes informatiques sont interconnectés. Les spécifications et autres exigences techniques du système informatique décentralisé énoncées dans le présent règlement devraient tenir compte de ce cadre.

(4) Les points d'accès du système informatique décentralisé devraient se fonder sur les points d'accès e-CODEX autorisés tels que définis à l'article 3, paragraphe 3, du règlement (UE) 2022/850 du Parlement européen et du Conseil [2].

(5) Le système informatique décentralisé est établi au sein d'un système informatique décentralisé plus large basé sur l'e-CODEX, appelé JUstice Digital EXchange system (JUDEX). Il est par conséquent nécessaire de garantir un échange efficace des informations concernant les développements horizontaux.

(6) Conformément à l'article 22 *bis*, paragraphe 4, du règlement (UE) 2018/1727, les États membres et Eurojust peuvent choisir d'utiliser le logiciel de mise en œuvre de référence développé par la Commission comme système dorsal en lieu et place d'un système informatique national. Afin de garantir l'interopérabilité, tant les systèmes informatiques nationaux que le logiciel de mise en œuvre de référence devraient être soumis aux mêmes spécifications et exigences techniques.

(7) Les données relatives aux infractions terroristes et aux formes graves de criminalité organisée devraient être transmises de manière structurée, afin d'améliorer la qualité et la pertinence des informations, et de faire en sorte que les informations puissent être intégrées plus efficacement dans le système de gestion des dossiers d'Eurojust et mieux recoupées avec les informations déjà conservées dans ledit système. En ce qui concerne les données dactyloscopiques et les photographies susceptibles d'être transmises à Eurojust à des fins d'identification de personnes faisant l'objet de procédures pénales liées à des infractions terroristes, il conviendrait de définir le format et les normes techniques de transmission.

[1] JO L 295 du 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

[2] Règlement (UE) 2022/850 du Parlement européen et du Conseil du 30 mai 2022 relatif à un système informatisé pour l'échange électronique transfrontière de données dans le domaine de la coopération judiciaire en matière civile et pénale (système e-CODEX), et modifiant le règlement (UE) 2018/1726 (JO L 150 du 1.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust facilite et soutient l'émission et l'exécution des demandes de coopération judiciaire dans ce domaine, notamment les demandes et les décisions qui se fondent sur des instruments donnant effet au principe de reconnaissance mutuelle. Les autorités nationales compétentes devraient avoir la possibilité de demander à Eurojust, par l'intermédiaire du système informatique décentralisé, d'apporter son assistance et d'assurer une coordination.

(9) Dans un souci d'efficacité et de cohérence, il importe que les spécifications techniques à établir en vertu du règlement (UE) 2018/1727 soient compatibles avec les spécifications techniques établies en vertu des règlements (UE) 2023/2844 ([3]), (UE) 2023/1543 ([4]) et (UE) 2024/3011 ([5]) du Parlement européen et du Conseil, ainsi qu'avec les futures mesures de numérisation ayant trait au mandat d'Eurojust visant à soutenir les autorités nationales compétentes.

(10) Toute autre communication entre Eurojust et les autorités nationales compétentes, telle que la communication d'informations concernant les résultats du traitement des informations, notamment sur l'existence de liens avec des affaires figurant déjà dans le système de gestion des dossiers, conformément à l'article 22 du règlement (UE) 2018/1727, lorsqu'Eurojust agit de sa propre initiative, ou la communication d'informations transmises à Eurojust afin de préserver, d'analyser et de conserver les éléments de preuve relatifs aux génocides, aux crimes contre l'humanité, aux crimes de guerre et aux infractions pénales connexes, conformément à l'article 4, paragraphe 1, point j), dudit règlement, devrait également être rendue possible par le système informatique décentralisé.

(11) Pour faire en sorte que le présent règlement prenne en considération les besoins opérationnels d'Eurojust, celle-ci a été consultée, conformément à l'article 22 *bis*, paragraphe 3, du règlement (UE) 2018/1727.

(12) Conformément à l'article 4 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande a notifié, par courrier du 9 septembre 2019, son intention d'accepter le règlement (UE) 2018/1727 et d'être liée par celui-ci. La décision (UE) 2019/2006 de la Commission ([6]) a confirmé cette participation. Le règlement (UE) 2023/2131 ([7]) a modifié le règlement (UE) 2018/1727 de manière à permettre la mise en place de canaux de communication numérique sécurisés entre Eurojust et les autorités nationales compétentes; il constitue la base juridique du présent règlement. N'ayant pas fait part de son intention de participer à l'adoption et à l'application du règlement (UE) 2023/2131 et n'ayant pas notifié son intention d'accepter ledit règlement et d'être liée par celui-ci, l'Irlande, conformément aux articles 1er et 2, et à l'article 4 *bis*, paragraphe 1, du protocole n° 21, n'est pas liée par le règlement (UE) 2023/2131 ni soumise à son application. L'Irlande ne participe donc pas à l'adoption du présent règlement.

(13) Conformément aux articles 1er 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 n'a pas participé à l'adoption du règlement (UE) 2018/1727. Le Danemark n'est donc pas lié par le présent règlement ni soumis à son application.

([3]) Règlement (UE) 2023/2844 du Parlement européen et du Conseil du 13 décembre 2023 relatif à la numérisation de la coopération judiciaire et de l'accès à la justice dans les affaires transfrontières en matière civile, commerciale et pénale, et modifiant certains actes dans le domaine de la coopération judiciaire (JO L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Règlement (UE) 2024/3011 du Parlement européen et du Conseil du 27 novembre 2024 relatif au transfert des procédures en matière pénale (JO L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Décision (UE) 2019/2006 de la Commission du 29 novembre 2019 concernant la participation de l'Irlande au règlement (UE) 2018/1727 du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) (JO L 310 du 2.12.2019, p. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Règlement (UE) 2023/2131 du Parlement européen et du Conseil du 4 octobre 2023 modifiant le règlement (UE) 2018/1727 du Parlement européen et du Conseil et la décision 2005/671/JAI du Conseil en ce qui concerne l'échange d'informations numériques dans les affaires de terrorisme (JO L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) 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 ([8]) et a rendu un avis le 21 octobre 2025.

(15) Les mesures prévues dans le présent règlement sont conformes à l'avis du comité institué par l'article 22 *quater* du règlement (UE) 2018/1727,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Spécifications techniques du système informatique décentralisé

Les spécifications, mesures et objectifs techniques du système informatique décentralisé visés à l'article 22 *ter*, paragraphe 1, points a), b), c) et d), du règlement (UE) 2018/1727 sont ceux indiqués à l'annexe I du présent règlement.

Article 2

Normes de procédure numériques

Les normes de procédure numériques applicables à la communication électronique par l'intermédiaire du système informatique décentralisé visées à l'article 22 *bis*, paragraphe 3, du règlement (UE) 2018/1727 sont celles indiquées à l'annexe II du présent règlement.

Article 3

Spécifications techniques pour la transmission de données dactyloscopiques et de photographies

Les spécifications techniques et le format de transmission d'empreintes digitales et de photographies visés à l'article 22 *bis*, paragraphe 3, du règlement (UE) 2018/1727 sont celles indiquées à l'annexe III du présent règlement.

Article 4

Entrée en vigueur

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

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

Fait à Bruxelles, le 4 décembre 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

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

ANNEXE I

SPÉCIFICATIONS, MESURES ET OBJECTIFS TECHNIQUES DU SYSTÈME INFORMATIQUE DÉCENTRALISÉ

1. **Introduction et champ d'application**

La présente annexe énonce les spécifications, mesures et objectifs techniques du système informatique décentralisé pour l'échange d'informations au titre du règlement (UE) 2018/1727.

Le caractère décentralisé du système informatique permet un échange de données direct et sécurisé entre les autorités nationales compétentes et Eurojust.

2. **Définitions**

Aux fins de la présente annexe, on entend par:

2.1. «HyperText Transfer Protocol Secure» ou «HTTPS» (protocole de transfert hypertexte sécurisé): les canaux de communication cryptée et de connexion sécurisée;

2.2. «non-répudiation de l'origine»: les mesures apportant la preuve de l'intégrité et la preuve de l'origine des données grâce à des méthodes telles que la certification numérique, l'infrastructure à clé publique ainsi que les signatures et cachets électroniques;

2.3. «non-répudiation de la réception»: les mesures apportant à l'émetteur la preuve de la réception des données par le destinataire prévu des données grâce à des méthodes telles que la certification numérique, l'infrastructure à clé publique ainsi que les signatures et cachets électroniques;

2.4. «SOAP» (Simple Object Access Protocol): selon les normes du World Wide Web Consortium, une spécification de protocole de messagerie pour l'échange d'informations structurées dans la mise en œuvre de services web dans les réseaux informatiques;

2.5. «REST» (Representational State Transfer): un style d'architecture permettant de concevoir des applications en réseau, reposant sur un modèle de communication client-serveur sans état et utilisant des méthodes standards pour effectuer des opérations sur des ressources, qui sont généralement représentées dans des formats structurés;

2.6. «service web»: un logiciel destiné à assurer une interaction interopérable machine-machine sur un réseau et qui dispose d'une interface décrite sous un format pouvant être traité par machine;

2.7. «échange de données»: l'échange de messages et de documents par l'intermédiaire du système informatique décentralisé;

2.8. «système e-CODEX»: le système e-CODEX tel qu'il est défini à l'article 3, point 1, du règlement (UE) 2022/850;

2.9. «vocabulaire de base e-Justice de l'Union»: le vocabulaire de base e-Justice de l'Union tel que défini au point 4 de l'annexe du règlement (UE) 2022/850;

2.10. «ebMS»: le service de messagerie ebXML, un protocole de messagerie développé par OASIS qui permet un échange sécurisé, fiable et interopérable de documents commerciaux sur support électronique utilisant SOAP. Il favorise l'intégration interentreprises dans divers systèmes;

2.11. «AS4»: la déclaration d'applicabilité 4, une norme OASIS qui définit le profil ebMS 3.0 et simplifie la messagerie interentreprises sécurisée et interopérable en utilisant des normes ouvertes telles que SOAP et WS-Security;

2.12. «durée maximale d'interruption admissible»: le délai maximal acceptable pour rétablir le service après un incident;

2.13. «perte de données maximale admissible»: le volume maximal acceptable de perte de données en cas de défaillance.

3. **Méthodes de communication par voie électronique**

3.1. Aux fins de l'échange de messages et de documents, le système informatique décentralisé utilise des méthodes de communication fondées sur des services, telles que les services web ou d'autres composants et solutions logicielles réutilisables.

3.2. En particulier, le système informatique décentralisé nécessitera une communication par l'intermédiaire des points d'accès e-CODEX, tels que visés à l'article 5, paragraphe 2, du règlement (UE) 2022/850. Par conséquent, pour garantir un échange transfrontière de données efficace et interopérable, le système informatique décentralisé facilite la communication par l'intermédiaire du système e-CODEX.

4. **Protocoles de communication**

4.1. Le système informatique décentralisé utilise des protocoles internet sécurisés pour:

a) la communication au sein du système informatique décentralisé entre les autorités compétentes et Eurojust;

b) la communication avec la base de données des autorités compétentes/cours et tribunaux telle que mentionnée au point 7.1.

4.2. Aux fins de la définition et de la transmission de données et de métadonnées structurées, les composants du système informatique décentralisé sont basés sur des normes et des protocoles sectoriels complets et largement acceptés, tels que SOAP et REST.

4.3. Pour les protocoles de transport et de messagerie, le système informatique décentralisé repose sur des protocoles normalisés sécurisés tels que:

a) le profil AS4 pour l'échange transfrontière de données, garantissant une messagerie sécurisée et fiable avec chiffrement et non-répudiation;

b) les API HTTPS/RESTful pour la communication prenant en charge les formats JSON et XML;

c) SOAP pour les interactions de haute fiabilité, intégrant WS-Security pour l'authentification et le chiffrement.

4.4. Aux fins d'un échange de données fluide et interopérable, les protocoles de communication utilisés par le système informatique décentralisé sont conformes aux normes d'interopérabilité applicables.

4.5. Le cas échéant, les schémas XML utilisent les normes ou vocabulaires pertinents, qui sont nécessaires à la validation correcte des éléments et types définis dans le schéma. Ces normes et vocabulaires peuvent inclure:

a) le vocabulaire de base e-Justice de l'Union;

b) des types de données non qualifiés;

c) une liste de codes pour les codes linguistiques de l'Union européenne.

4.6. En ce qui concerne les protocoles de sécurité et d'authentification, le système informatique décentralisé repose sur des protocoles normalisés tels que:

a) TLS (sécurité de la couche de transport) pour la communication cryptée et authentifiée sur les réseaux, qui prend en charge l'authentification mutuelle au moyen de certificats numériques X.509;

b) OAuth/OpenID Connect (OIDC) pour une authentification et une autorisation sécurisées;

c) ICP (infrastructure à clé publique) et signatures numériques pour l'échange sécurisé de clés et la vérification de l'intégrité des messages, au moyen de certificats numériques (X.509) délivrés par des autorités de certification reconnues.

5. **Objectifs en matière de sécurité de l'information et mesures techniques pertinentes**

5.1. En ce qui concerne l'échange d'informations au moyen du système informatique décentralisé, les mesures techniques permettant d'assurer le respect des normes minimales de sécurité informatique sont notamment les suivantes:

a) mesures visant à garantir la confidentialité des informations, y compris par le recours à des canaux de communication sécurisés;

b) mesures visant à garantir l'intégrité des données au repos et en transit;

c) mesures visant à garantir la non-répudiation de l'origine de l'émetteur des informations au sein du système informatique décentralisé et la non-répudiation de la réception des informations;

d) mesures visant à garantir la journalisation des événements liés à la sécurité conformément aux recommandations internationales reconnues en matière de normes de sécurité informatique ([1]);

e) mesures visant à garantir l'authentification et l'autorisation des utilisateurs et mesures visant à vérifier l'identité des systèmes connectés au système informatique décentralisé.

5.2. Les composants du système informatique décentralisé garantissent une communication et une transmission de données sécurisées, en utilisant le chiffrement, l'infrastructure à clé publique avec des certificats numériques d'authentification et l'échange sécurisé de clés, ainsi que des protocoles de messagerie sécurisée tels qu'AS4 (ebMS), les API RESTful et SOAP, afin de préserver la confidentialité et l'intégrité des messages.

5.3. En cas de recours au protocole TLS dans le contexte du système informatique décentralisé, la dernière version stable du protocole est utilisée ou, à défaut, une version ne présentant pas de failles de sécurité connues. Seules les longueurs de clé garantissant un niveau adéquat de sécurité cryptographique sont autorisées, et les suites cryptographiques dont on sait qu'elles sont peu sûres ou obsolètes ne sont pas utilisées.

5.4. Dans la mesure du possible, les certificats numériques ICP utilisés aux fins de l'exploitation du système informatique décentralisé sont délivrés par des autorités de certification reconnues comme prestataires de services de confiance qualifiés au sens du règlement (UE) n° 910/2014 du Parlement européen et du Conseil ([2]). Des mesures sont mises en œuvre pour garantir que ces certificats sont utilisés uniquement aux fins prévues, au niveau de confiance requis et conformément aux exigences applicables du règlement (UE) n° 910/2014.

5.5. Les composants du système informatique décentralisé sont développés conformément au principe de protection des données dès la conception et par défaut, et des mesures administratives, organisationnelles et techniques appropriées sont mises en œuvre pour garantir un niveau élevé de cybersécurité.

5.6. La Commission conçoit, développe et maintient le logiciel de mise en œuvre de référence conformément aux exigences et principes en matière de protection des données énoncés dans le règlement (UE) 2018/1725. Le logiciel de mise en œuvre de référence fourni par la Commission permet aux États membres de se conformer aux obligations qui leur incombent en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil ([3]) et de la directive (UE) 2016/680, selon le cas.

([1]) Sans préjudice de la journalisation à des fins de sécurité, les mécanismes de journalisation utilisés par les composants du système informatique décentralisé permettent, s'il y a lieu, de garantir le respect des exigences énoncées à l'article 88 du règlement (UE) 2018/1725 et, le cas échéant, à l'article 25 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Les États membres qui utilisent un système dorsal national différent du logiciel de mise en œuvre de référence mettent en œuvre les mesures nécessaires pour s'assurer que leur système dorsal national est conforme aux exigences du règlement (UE) 2016/679 et de la directive (UE) 2016/680, selon le cas.

5.8. Eurojust met en œuvre les mesures nécessaires pour faire en sorte que son système dorsal, ou l'exemplaire du logiciel de mise en œuvre de référence qu'elle déploie, soit conforme aux exigences des règlements (UE) 2018/1725 et (UE) 2018/1727.

5.9. Les États membres et Eurojust mettent en place des mécanismes solides de détection des menaces et de réaction aux incidents afin de garantir l'identification, l'atténuation et le rétablissement en temps utile à la suite des incidents de sécurité, conformément à leurs politiques pertinentes, pour les systèmes informatiques faisant partie du système informatique décentralisé qui relèvent de leur responsabilité.

6. **Objectifs minimaux en matière de disponibilité**

6.1. Eurojust et les États membres veillent à ce que les composants du système informatique décentralisé relevant de leur responsabilité soient disponibles 24 heures sur 24 et 7 jours sur 7, avec un taux de disponibilité technique cible d'au moins 98 % sur une base annuelle, à l'exclusion de la maintenance programmée.

6.2. La Commission veille à ce que la base de données des cours et tribunaux soit disponible 24 heures sur 24 et 7 jours sur 7, avec un taux de disponibilité technique cible de plus de 99 % sur une base annuelle, à l'exclusion de la maintenance programmée.

6.3. Dans la mesure du possible, pendant les jours ouvrables, les opérations de maintenance doivent être planifiées entre 20 h 00 et 7 h 00 HEC.

6.4. Les États membres informent la Commission, Eurojust et les autres États membres des activités de maintenance selon les modalités suivantes:

a) 5 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner jusqu'à 4 heures d'indisponibilité;

b) 10 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner entre 4 et 12 heures d'indisponibilité;

c) 30 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner plus de 12 heures d'indisponibilité.

6.5. Si les États membres disposent de fenêtres de maintenance régulières fixes, ils informent la Commission, Eurojust et les autres États membres de l'heure et du ou des jours où ces fenêtres régulières fixes sont prévues. Par dérogation aux obligations énoncées dans la première phrase, si des composants du système informatique décentralisé relevant de la responsabilité des États membres deviennent indisponibles au cours d'une telle fenêtre fixe régulière, les États membres peuvent choisir de ne pas en informer la Commission à chaque fois.

6.6. En cas de défaillance technique imprévue d'un composant du système informatique décentralisé relevant de la responsabilité des États membres, ceux-ci informent sans délai la Commission et les autres États membres de cette défaillance et, s'il est connu, du délai de rétablissement prévu.

6.7. Eurojust informe la Commission et les États membres des activités de maintenance selon les modalités suivantes:

a) 5 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner jusqu'à 4 heures d'indisponibilité;

b) 10 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner entre 4 et 12 heures d'indisponibilité;

c) 30 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner plus de 12 heures d'indisponibilité.

6.8. Si Eurojust dispose de fenêtres de maintenance régulières fixes, elle informe la Commission et les États membres de l'heure et du ou des jours où ces fenêtres régulières fixes sont prévues. Par dérogation aux obligations énoncées dans la première phrase, si des composants du système informatique décentralisé relevant de la responsabilité d'Eurojust deviennent indisponibles au cours d'une telle fenêtre fixe régulière, Eurojust peut choisir de ne pas en informer la Commission à chaque fois.

6.9. En cas de défaillance technique imprévue d'un composant du système informatique décentralisé relevant de la responsabilité d'Eurojust, celle-ci informe sans délai la Commission et les États membres de cette défaillance et, s'il est connu, du délai de rétablissement prévu.

6.10. En cas de défaillance technique inattendue de la base de données des autorités compétentes/cours et tribunaux, la Commission informe sans délai Eurojust et les États membres de cette indisponibilité et, s'il est connu, du délai de rétablissement prévu.

6.11. En cas de perturbation du service, les États membres et Eurojust font en sorte que le service soit rapidement rétabli et que la perte de données soit minimale, conformément à la durée maximale d'interruption admissible et à la perte de données maximale admissible.

6.12. Les États membres et Eurojust mettent en œuvre les mesures appropriées pour atteindre les objectifs de disponibilité décrits ci-dessus et établissent des procédures pour réagir efficacement aux incidents.

7. **Base de données des autorités compétentes/cours et tribunaux (CDB)**

7.1. Conformément à l'article 22 *bis* du règlement (UE) 2018/1727, le système informatique décentralisé permet la communication électronique entre les autorités nationales compétentes et Eurojust. Eu égard aux obligations d'échange d'informations entre les autorités nationales compétentes et Eurojust prévues aux articles 21, 21 *bis* et 22, mais également au rôle d'Eurojust consistant à faciliter et à soutenir l'émission et l'exécution de toute demande d'entraide judiciaire ou de reconnaissance mutuelle en application de l'article 8, paragraphe 1, du règlement (UE) 2018/1727, les autorités compétentes concernées doivent être clairement identifiables lorsqu'elles utilisent le système informatique décentralisé. Par conséquent, il est essentiel de créer une source authentique comportant des informations sur lesdites autorités aux fins du système informatique décentralisé.

7.2. La CDB comporte les informations suivantes sous forme structurée:

a) aux fins de l'article 8, paragraphes 1, 3 et 4, et des articles 21, 21 *bis* et 22 du règlement (UE) 2018/1727, des informations sur les autorités nationales compétentes, y compris les correspondants nationaux tels que prévus à l'article 20 dudit règlement, ainsi que les membres nationaux dont il est question à l'article 7 ([4]) du même règlement;

b) le cas échéant, des informations nécessaires pour déterminer les champs géographiques ou matériels relevant de la compétence des autorités compétentes, ou d'autres critères pertinents nécessaires pour établir leur compétence;

c) des informations nécessaires à l'acheminement correct des messages techniques au sein du système informatique décentralisé.

7.3. La Commission est responsable du développement, de la maintenance, du fonctionnement et du soutien de la CDB.

7.4. La CDB permet aux États membres et à Eurojust de mettre à jour les informations y figurant, et aux autorités nationales compétentes et aux membres nationaux participant au système informatique décentralisé d'accéder à ces informations et de les extraire au moyen de programmes.

7.5. L'accès à la CDB est possible via un protocole de communication commun, que les autorités compétentes connectées au système informatique centralisé utilisent un système dorsal national ou un exemplaire du logiciel de mise en œuvre de référence.

7.6. Les États membres veillent à ce que les informations relatives à leurs autorités compétentes figurant dans la CDB, telles qu'énumérées au point 7.2, soient complètes, exactes et tenues à jour.

([4]) Cela s'entend sans préjudice de toute délégation de pouvoirs du membre national au profit de son adjoint, d'autres membres du personnel du bureau national ou de membres du personnel autorisés d'Eurojust.

ANNEXE II

NORMES DE PROCÉDURE NUMÉRIQUES

L'article 3, point 9, du règlement (UE) 2022/850 définit les normes de procédure numériques comme étant les spécifications techniques relatives aux modèles de processus opérationnel et aux schémas de données qui énoncent la structure électronique des données échangées par l'intermédiaire du système e-CODEX.

La présente annexe expose les spécifications techniques relatives aux modèles de processus opérationnel et les spécifications techniques relatives aux schémas de données.

1. **Spécifications techniques relatives aux modèles de processus opérationnel au titre du règlement (UE) 2018/1727**

Les spécifications techniques relatives aux modèles de processus opérationnel sont énoncées aux points 1.1 à 1.5. Elles définissent les principaux aspects nécessaires pour permettre la communication électronique aux fins du règlement (UE) 2018/1727 par l'intermédiaire du système informatique décentralisé.

Le système informatique décentralisé ne permet l'échange d'informations qu'entre les autorités nationales compétentes d'un État membre et le membre national dudit État membre.

1.1. *Échange d'informations en rapport avec le registre judiciaire antiterroriste européen (CTR) – article 21* bis *du règlement (UE) 2018/1727*

1.1.1. Modèle pour la transmission de données CTR:

L'autorité nationale compétente transmet au membre national les données à faire figurer dans le CTR concernant les procédures en matière de terrorisme.

1.1.2. Modèle pour la réception de données CTR:

Le membre national réceptionne les données CTR.

1.1.3. Modèle de demande de consentement:

Le membre national demande le consentement de son autorité nationale compétente.

1.1.4. Modèle pour la réception d'une demande de consentement:

L'autorité nationale compétente réceptionne la demande de consentement.

1.1.5. Modèle pour l'envoi d'une réponse à une demande de consentement:

L'autorité nationale compétente envoie une réponse à la demande de consentement.

1.1.6. Modèle pour la réception d'une réponse à une demande de consentement:

Le membre national réceptionne la réponse à la demande de consentement.

1.1.7. Modèle pour la transmission d'informations sur un lien:

Le membre national informe l'autorité nationale compétente du lien avec une autre affaire.

1.1.8. Modèle pour la mise à jour de données CTR:

L'autorité nationale compétente transmet à son membre national respectif les données qui nécessitent une mise à jour ou une suppression.

1.1.9. Modèle pour la réception de données CTR mises à jour:

Le membre national réceptionne les données CTR qui nécessitent une mise à jour ou une suppression.

1.2. *Échange d'informations en rapport avec les formes graves de criminalité – article 21 du règlement (UE) 2018/1727*

1.2.1. Modèle pour la transmission de données sur les formes graves de criminalité transfrontière:

L'autorité nationale compétente transmet à Eurojust des données sur les formes graves de criminalité transfrontière.

1.2.2. Modèle pour la réception de données sur les formes graves de criminalité transfrontière:

Le membre national réceptionne les données relatives aux formes graves de criminalité transfrontière.

1.2.3. Modèle de demande de consentement:

Le membre national demande le consentement de son autorité nationale compétente.

1.2.4. Modèle pour la réception d'une demande de consentement:

L'autorité nationale compétente réceptionne la demande de consentement.

1.2.5. Modèle pour l'envoi d'une réponse à une demande de consentement:

L'autorité nationale compétente envoie une réponse à la demande de consentement.

1.2.6. Modèle pour la réception d'une réponse à une demande de consentement:

Le membre national réceptionne la réponse à la demande de consentement.

1.2.7. Modèle pour la transmission d'informations sur un lien:

Le membre national informe l'autorité nationale compétente du lien avec une autre affaire.

1.2.8. Modèle pour la mise à jour de données sur les formes graves de criminalité transfrontière:

L'autorité nationale compétente transmet à son membre national respectif les données qui nécessitent une mise à jour ou une suppression.

1.2.9. Modèle pour la réception de données mises à jour sur les formes graves de criminalité transfrontière:

Le membre national réceptionne les données relatives à des formes graves de criminalité transfrontière qui nécessitent une mise à jour ou une suppression.

1.3. *Échange d'informations générales*

1.3.1. Modèle pour l'envoi d'informations:

Le membre national envoie des informations à l'autorité nationale compétente ou inversement.

1.3.2. Modèle pour la réception d'informations:

L'autorité nationale compétente ou le membre national réceptionne les informations.

1.3.3. Modèle pour la réponse aux informations:

L'autorité nationale compétente répond aux informations reçues du membre national ou inversement.

1.3.4. Modèle pour la réception d'une réponse:

Le membre national réceptionne la réponse de l'autorité nationale compétente.

1.3.5. Modèle pour l'envoi d'informations:

L'autorité nationale compétente envoie des informations au membre national.

1.3.6. Modèle pour la réception d'informations:

Le membre national réceptionne les informations.

1.3.7. Modèle pour la réponse aux informations:

Le membre national répond aux informations reçues de l'autorité nationale compétente.

1.3.8. Modèle pour la réception d'une réponse:

L'autorité nationale compétente réceptionne la réponse du membre national.

1.4. *Rôle de facilitation et de soutien — article 8, paragraphe 1, du règlement (UE) 2018/1727*

Remarque: Lorsque les modèles de facilitation et de soutien décrits au point 1.5 impliquent l'échange de formulaires réglementaires établis par des actes juridiques de l'Union dans le domaine de la coopération judiciaire en matière pénale, les modèles utilisent, si disponibles, les représentations de données structurées et les schémas XML pertinents élaborés en rapport avec ces actes, par exemple ceux établis aux fins de la mise en œuvre du règlement (UE) 2023/2844 ou d'autres instruments pertinents.

1.5. *Modèle de demande de facilitation ou de soutien*

1.5.1. Modèle pour la transmission d'une demande de facilitation ou de soutien:

L'autorité nationale compétente transmet une demande de facilitation ou une demande de soutien à son membre national respectif.

1.5.2. Modèle pour la réception d'une demande de facilitation ou de soutien:

Le membre national réceptionne la demande de facilitation ou de soutien et la transmet au membre national de l'État membre requis en dehors de JUDEX.

1.5.3. Modèle pour le transfert d'une demande de facilitation ou de soutien à l'autorité nationale compétente:

Le membre national de l'État membre requis envoie la demande à son autorité nationale compétente respective.

1.5.4. Modèle pour la réception d'une demande de facilitation ou de soutien:

L'autorité nationale compétente réceptionne la demande de facilitation ou de soutien.

1.5.5. Modèle pour l'envoi d'une réponse à une demande de facilitation ou de soutien:

L'autorité nationale compétente envoie au membre national de l'État membre requis une réponse ou des informations faisant suite à la demande.

1.5.6. Modèle pour la réception d'une réponse à une demande de facilitation ou de soutien:

Le membre national réceptionne la réponse ou les informations fournies par l'autorité compétente nationale à la suite de la demande de facilitation ou de soutien et la/les communique au membre national de l'État membre requérant en dehors de JUDEX.

1.5.7. Modèle pour la réponse à une demande de facilitation ou de soutien:

Le membre national de l'État membre requérant répond aux informations fournies par l'autorité nationale compétente en rapport avec la demande de facilitation ou de soutien, ou partage ces informations.

1.5.8. Modèle pour la réception d'une réponse:

L'autorité nationale compétente réceptionne la réponse ou les informations concernant la demande de facilitation ou de soutien.

2. **Spécifications techniques relatives aux schémas de données**

Les spécifications techniques destinées à servir de base à l'élaboration de définitions de schéma XML (XSD) aux fins de la numérisation du règlement (UE) 2018/1727 sont énoncées aux points 2.1 et 2.2 de la présente annexe. Ces spécifications définissent les éléments clés et toute autre information utile afin de fournir une description complète pour les besoins de la création desdits schémas.

La description se veut générique afin que les XSD créés puissent être modifiés et étendus sans qu'il soit nécessaire d'apporter des modifications substantielles à ces spécifications.

Ces spécifications s'appliquent à la présentation réglementaire des schémas établie à l'annexe du règlement (UE) 2018/1727, ainsi qu'à tout message prédéfini ou à tout message à contenu libre utilisés dans les échanges effectués au titre dudit règlement.

2.1. *Considérations générales*

Pour tous les schémas à fournir, les dispositions suivantes s'appliquent:

2.1.1. Versions

Un attribut de version doit être inclus pour faciliter la gestion des versions du schéma et permettre la mise à jour de celui-ci dans les versions ultérieures conformément aux exigences opérationnelles. L'attribut de version indique si la nouvelle version est rétrocompatible lors de l'introduction de nouvelles fonctionnalités ou d'améliorations.

2.1.2. Déclaration de schéma et métadonnées

— Le cas échéant, le schéma utilise les normes ou vocabulaires pertinents, tels qu'exigés par e-CODEX pour garantir l'interopérabilité, qui sont nécessaires à la validation correcte des éléments et types définis dans le schéma en question. Ces normes ou vocabulaires peuvent inclure:

  — le vocabulaire de base e-Justice de l'Union;

  — des types de données non qualifiés;

  — une liste de codes pour les codes linguistiques de l'Union européenne.

— En outre, le cas échéant, le schéma peut intégrer des normes ETSI pertinentes pour utiliser leurs définitions.

2.1.3. Annotations et documentation

— **Annotations**: chaque élément du schéma est généralement accompagné d'annotations. Les annotations fournissent des informations lisibles par l'homme au sujet de l'élément, en définissant souvent la finalité ou l'utilisation de celui-ci de manière claire et concise.

2.1.4. Utilisation et adaptabilité

Le schéma obéit aux règles énoncées aux points a) à d):

a) **Structure modulaire**: chaque section est conçue pour remplir une fonctionnalité spécifique et peut être réutilisée ou adaptée de manière indépendante. Cela facilite l'adaptation du schéma à des cas d'utilisation divers.

b) **Extensibilité**: le schéma est conçu de manière à prendre en charge l'incorporation d'éléments ou d'attributs nouveaux si des informations supplémentaires s'avèrent nécessaires par la suite. Ce résultat est obtenu à l'aide d'éléments et de séquences facultatifs, pouvant être complétés sans casser les implémentations existantes.

c) **Structure adaptable**: le schéma est conçu de manière à permettre l'ajout ou la modification d'éléments ou de types de données, selon les besoins. La structure du schéma s'adapte aux changements dans les exigences sans nécessiter de remaniements majeurs.

d) **Éléments facultatifs**: des éléments du schéma peuvent être désignés comme facultatifs, c'est-à-dire qu'ils peuvent être inclus ou omis selon les circonstances particulières.

Le schéma est conçu de manière à prendre en charge la collecte de données structurées pour répondre à des demandes spécifiques.

2.1.5. Modifications

La conception du schéma se caractérise par sa flexibilité, sa modularité et sa facilité d'adaptation. Les types complexes et les éléments facultatifs sont intégrés dans la conception de sorte que celle-ci permette de gérer des scénarios divers tout en restant facile à modifier et à compléter.

2.2. *Échange de données structurées*

Les données structurées mentionnées aux points 2.2.1 et 2.2.2 doivent être fournies conformément à l'article 22 *bis*, paragraphe 3, du règlement (UE) 2018/1727. Le schéma permet également de désigner les ensembles de données devant être supprimés lors des mises à jour futures.

2.2.1. Données du registre judiciaire antiterroriste européen

Les spécifications techniques suivantes du schéma de données établissent un cadre structuré pour la création du schéma au format XML.

a) Section de premier niveau

Cette section de premier niveau correspond aux informations énumérées à l'annexe III du règlement (UE) 2018/1727, concernant les informations à faire figurer dans le registre judiciaire européen antiterroriste (CTR).

b) Structure du message

La structure des données CTR se compose d'une séquence d'éléments et comprend au minimum les éléments suivants:

i) informations pour l'identification des personnes physiques:

— le nom de famille;

— le ou les prénoms;

— les pseudonymes éventuels;

— la date de naissance;

— le lieu de naissance (ville et pays);

— la ou les nationalités;

— le document d'identité (type et numéro du document);

— le sexe;

— le lieu de résidence;

ii) informations pour l'identification des personnes morales:

— la dénomination commerciale;

— la forme juridique;

— le lieu du siège social;

iii) informations pour l'identification des personnes physiques et morales:

— les numéros de téléphone;

— les adresses électroniques;

— les informations sur les comptes détenus auprès de banques ou d'autres institutions financières;

— l'état d'avancement des procédures;

iv) informations relatives à l'infraction:

— les informations concernant les personnes morales impliquées dans la préparation ou la commission d'une infraction terroriste;

— la qualification juridique de l'infraction en vertu du droit national;

— la forme d'infraction grave applicable figurant sur la liste visée à l'annexe I;

— toute affiliation à un groupe terroriste;

— le type de terrorisme, par exemple djihadisme, séparatisme, terrorisme de gauche ou terrorisme de droite;

— le résumé de l'affaire;

v) informations relatives aux procédures nationales:

— l'état d'avancement de ces procédures;

— le Parquet compétent;

— le numéro de l'affaire;

— la date d'ouverture des poursuites judiciaires officielles;

— les liens avec d'autres affaires pertinentes;

vi) champ réservé aux informations complémentaires (contenu libre);

vii) code d'autorisation préalable.

2.2.2. Données transmises en application de l'article 21 du règlement (UE) 2018/1727

a) Article 21, paragraphe 4, du règlement (UE) 2018/1727, prévoyant la création d'équipes communes d'enquête («ECE»)

i) Section de premier niveau
Cette section de premier niveau correspond aux informations visées à l'article 21, paragraphe 4, du règlement (UE) 2018/1727, concernant la création d'ECE.

ii) Structure du message
La structure des données se compose d'une séquence d'éléments et comprend au minimum les éléments suivants:

— Autorité judiciaire nationale menant la procédure pénale

— Numéro de référence national de la procédure pénale

— État d'avancement de la procédure pénale

— Infractions pénales faisant l'objet d'une enquête

— Autres pays concernés par l'affaire

— Ce dossier bénéficie-t-il déjà du soutien d'Eurojust?

— Si oui, numéro de dossier Eurojust?

— Si non, s'agit-il d'une demande de soutien?

— Ce dossier bénéficie-t-il du soutien d'Europol?

— Si oui, task force opérationnelle et/ou application de réseau d'échange sécurisé d'informations («SIENA»)?

— Accord relatif à l'ECE:

— Pays participants

— Parties à l'ECE (autorités nationales chargées des enquêtes)

— Numéro de référence national de la procédure pénale visée par l'ECE

— Date de signature

— Durée

— Infractions pénales faisant l'objet d'une enquête

— Résumé succinct de l'affaire

— Principaux suspects dans le cadre de la procédure pénale visée par l'ECE (nom, prénom, date et lieu de naissance et éventuellement d'autres catégories de données pertinentes et nécessaires mentionnées à l'annexe II)

— Résultats des travaux des ECE:

— Difficultés/retards dans:

— la mise en place de l'ECE

— l'obtention/le partage d'éléments de preuve au sein de l'ECE

— l'adoption/la mise en œuvre d'une stratégie commune en matière de poursuites

— Recevabilité/irrecevabilité/appréciation des éléments de preuve de l'ECE dans le cadre de la procédure nationale

— Issue de la procédure judiciaire (poursuites fructueuses/infructueuses et condamnations/acquittements)

iii) Code d'autorisation préalable

b) Article 21, paragraphe 5, du règlement (UE) 2018/1727, affaires graves et complexes

i) Section de premier niveau

Cette section de premier niveau correspond aux informations visées à l'article 21, paragraphe 5, du règlement Eurojust, c'est-à-dire aux affaires graves et complexes.

ii) Structure du message

La structure des données se compose d'une séquence d'éléments et comprend au minimum les éléments suivants:

— Autorité judiciaire nationale menant la procédure pénale

— Numéro de référence national de la procédure pénale

— État d'avancement de la procédure pénale

— Infractions pénales faisant l'objet d'une enquête

— Autres pays concernés par l'affaire

— Ce dossier bénéficie-t-il déjà du soutien d'Eurojust?

— Si oui, numéro de dossier Eurojust?

— Si non, s'agit-il d'une demande de soutien?

— Ce dossier bénéficie-t-il du soutien d'Europol?

— Si oui, task force opérationnelle et/ou SIENA?

— Forme de criminalité grave applicable

— Implication d'un réseau de criminalité organisée

— Type mafieux

— Réseau transnational de criminalité organisée

— Répercussions au niveau de l'UE

— Principaux suspects dans le cadre de la procédure pénale (nom, prénom, date et lieu de naissance et éventuellement d'autres catégories de données pertinentes et nécessaires mentionnées à l'annexe II)

— Résumé succinct de l'affaire

— Autres pays concernés

— Pays avec lesquels une coopération a déjà été engagée

— Autorités compétentes intervenant dans un autre pays

— Instruments de coopération judiciaire utilisés

— Nombre de demandes envoyées/reçues

— Existence d'enquêtes liées

— Pays avec lesquels la coopération doit être activée/pays potentiellement touchés

— Type de coopération nécessaire (par exemple: extradition, collecte de preuves, autre forme de coopération)

— Existence d'enquêtes liées

iii) Code d'autorisation préalable

c) Article 21, paragraphe 6, point a), du règlement (UE) 2018/1727, conflits de compétence

i) Section de premier niveau

Cette section de premier niveau correspond aux informations visées à l'article 21, paragraphe 6, point a), du règlement (UE) 2018/1727, c'est-à-dire aux conflits de compétence.

ii) Structure du message

La structure des données se compose d'une séquence d'éléments et comprend au minimum les éléments suivants:

— Autorité judiciaire nationale menant la procédure pénale

— Numéro de référence national de la procédure pénale

— État d'avancement de la procédure pénale (par exemple: enquête, poursuites, procès).

— Infractions pénales faisant l'objet d'une enquête

— Autres pays concernés par l'affaire

— Ce dossier bénéficie-t-il déjà du soutien d'Eurojust?

— Si oui, numéro de dossier Eurojust?

— Si non, s'agit-il d'une demande de soutien?

— Ce dossier bénéficie-t-il du soutien d'Europol?

— Si oui, task force opérationnelle et/ou SIENA?

— Autres pays concernés

— Autorités nationales compétentes de l'autre pays, si elles sont connues

— Numéro de référence national de la procédure pénale engagée dans un autre pays

— Stade de la procédure dans l'autre pays, s'il est connu

— Conflit positif ou négatif

— Conflit réel ou potentiel

— Activités de coordination déjà entreprises (par exemple, consultations au titre de la décision-cadre 2009/948/JAI du Conseil [1])

— Résumé succinct de l'affaire

— Principaux suspects communs (nom, prénom, date et lieu de naissance et éventuellement d'autres catégories de données pertinentes et nécessaires mentionnées à l'annexe II)

iii) Code d'autorisation préalable

d) Article 21, paragraphe 6, point b), livraisons contrôlées

i) Section de premier niveau

Cette section de premier niveau correspond aux informations visées à l'article 21, paragraphe 6, point b), du règlement (UE) 2018/1727: livraisons contrôlées

ii) Structure du message

La structure des données se compose d'une séquence d'éléments et comprend au minimum les éléments suivants:

— Autorité judiciaire nationale menant la procédure pénale

— Numéro de référence national de la procédure pénale

— État d'avancement de la procédure pénale (par exemple: enquête, poursuites, procès).

— Infractions pénales faisant l'objet d'une enquête

— Autres pays concernés par l'affaire

— Ce dossier bénéficie-t-il déjà du soutien d'Eurojust?

— Si oui, numéro de dossier Eurojust?

— Si non, s'agit-il d'une demande de soutien?

— Ce dossier bénéficie-t-il du soutien d'Europol?

— Si oui, task force opérationnelle et/ou SIENA?

— Autres pays concernés

— Pays d'origine/de transit/de destination

— Autorités nationales compétentes dans d'autres pays

— Existence d'enquêtes liées dans d'autres pays

[1] Décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales (JO L 328 du 15.12.2009, p. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Type de marchandises livrées (par exemple, stupéfiants avec indication de leur nature/argent/armes/cigarettes/autres)

— État d'avancement de la livraison contrôlée (par exemple, planifiée, en cours, achevée)

— Résultat de la livraison contrôlée, si déjà exécutée

— Instrument de coopération judiciaire utilisé

— Principaux suspects communs (nom, prénom, date et lieu de naissance et éventuellement d'autres catégories de données pertinentes et nécessaires mentionnées à l'annexe II)

iii) Code d'autorisation préalable

e) Article 21, paragraphe 6, point c), du règlement (UE) 2018/1727, problèmes récurrents avec les instruments de coopération judiciaire

i) Section de premier niveau

Cette section de premier niveau correspond aux informations visées à l'article 21, paragraphe 6, point c), du règlement (UE) 2018/1727: problèmes récurrents avec les instruments de coopération judiciaire.

ii) Structure du message

La structure des données se compose d'une séquence d'éléments et comprend au minimum les éléments suivants:

— Autorité judiciaire nationale menant la procédure pénale

— Numéro de référence national de la procédure pénale

— État d'avancement de la procédure pénale (par exemple: enquête, poursuites, procès).

— Infractions pénales faisant l'objet d'une enquête

— Autres pays concernés par l'affaire

— Ce dossier bénéficie-t-il déjà du soutien d'Eurojust?

— Si oui, numéro de dossier Eurojust?

— Si non, s'agit-il d'une demande de soutien?

— Ce dossier bénéficie-t-il du soutien d'Europol?

— Si oui, task force opérationnelle et/ou SIENA?

— Autres pays concernés

— Autorités nationales compétentes, si elles sont connues

— Agissant en qualité d'autorité d'émission ou d'exécution

— Instrument de coopération judiciaire mobilisé (par exemple MAE, DEE, gel et confiscation)

— Demande spécifique concernée (par exemple quelle mesure d'enquête, quel type de gel, MAE à des fins d'exécution d'une peine ou de poursuites)

— Refus ou difficultés récurrentes

— En cas de refus, quel motif spécifique est invoqué?

— Description succincte du problème

— Autres autorités nationales rencontrant le même problème, le cas échéant

iii) Code d'autorisation préalable

2.3. *Codes d'autorisation préalable*

Lorsqu'elles partagent des données avec Eurojust via JUDEX, les autorités nationales fournissent, au moyen de codes d'autorisation préalable, des indications sur le traitement ultérieur des données, l'accès à celles-ci et leur transfert à la suite de la mise en évidence d'un lien. Les codes d'autorisation préalable indiquent si, et dans quelle mesure, les informations en rapport avec le lien peuvent être partagées avec d'autres autorités nationales compétentes, d'autres agences et organes de l'Union, des pays tiers ou des organisations internationales.

2.4. *Messages prédéfinis*

Les messages prédéfinis sont des représentations d'échanges qui sont institués par le règlement (UE) 2018/1727 mais pour lesquels l'acte juridique ne prévoit aucune forme particulière. Leurs types et leur nombre sont déterminés dans le cadre de l'analyse opérationnelle et technique.

Les définitions de schéma XML (XSD) pour les messages prédéfinis sont conçues de manière à en garantir la cohérence, la structure et la conformité avec les besoins opérationnels.

Ces schémas obéissent aux règles suivantes:

a) la section de premier niveau du schéma est nommée d'après le type de message spécifique qui est défini;

b) les champs obligatoires pour le type de message spécifique sont ajoutés et définis à l'intérieur de cette structure, de manière à garantir une représentation adéquate des éléments de données.

2.5. *Messages à contenu libre*

Les messages à contenu libre sont des représentations d'échanges permettant l'insertion de contenus non structurés ou partiellement structurés, conciliant une certaine souplesse avec le respect des exigences réglementaires et opérationnelles. Les XSD pour les messages à contenu libre sont conçues de manière à en garantir la cohérence et le formatage adéquat.

Ces schémas obéissent aux règles suivantes:

a) la section de premier niveau du schéma est nommée d'après le type de message à contenu libre spécifique qui est défini;

b) le schéma définit la structure nécessaire au message à contenu libre tout en permettant un ordonnancement adéquat des éléments, en fonction des besoins;

c) les champs obligatoires pour le type de message à contenu libre spécifique sont ajoutés et définis à l'intérieur de cette structure, de manière à garantir une représentation adéquate des éléments de données.

ANNEXE III

SPÉCIFICATIONS TECHNIQUES DES EMPREINTES DIGITALES ET DES PHOTOGRAPHIES

Les messages échangés par l'intermédiaire du système informatique décentralisé peuvent être accompagnés de pièces jointes, y compris de fichiers au format du National Institute of Standards and Technology (institut national américain des normes et des technologies, ci-après «NIST») contenant des empreintes digitales et des photographies, conformément aux spécifications techniques énoncées aux points 1 et 2.

1. **Empreintes digitales**

Les empreintes digitales qui peuvent être partagées avec Eurojust aux fins d'une identification fiable des personnes faisant l'objet de procédures pénales liées à des infractions terroristes remplissent les conditions suivantes:

a) les empreintes digitales sont fournies dans un fichier contenant des images numériques d'empreintes digitales (le fichier dactyloscopique NIST) et sont saisies conformément à la norme ANSI/NIST-ITL 1-2011 Update 2015 (ou une version plus récente);

b) le fichier dactyloscopique NIST comprend jusqu'à dix empreintes digitales individuelles: roulées et/ou à plat;

c) toutes les empreintes digitales sont étiquetées;

d) les empreintes digitales sont saisies au moyen de dispositifs de scannage en direct ou d'encre sur papier, à condition que les empreintes digitales saisies au moyen d'encre sur papier aient été scannées avec la résolution requise et avec la même qualité;

e) le fichier dactyloscopique NIST permet l'inclusion d'informations complémentaires telles que les conditions d'enregistrement des empreintes digitales et la méthode utilisée pour obtenir des images d'empreintes digitales individuelles;

f) les empreintes digitales ont une résolution nominale de 500 ou 1 000 ppi [1] (avec un écart acceptable de +/– 10 ppi) avec 256 niveaux de gris;

g) l'algorithme de compression des empreintes digitales à utiliser est conforme aux recommandations du NIST. Les données dactyloscopiques d'une résolution de 500 ppi sont comprimées au moyen de l'algorithme WSQ (ISO/IEC 19794-5:2005). Les données dactyloscopiques d'une résolution de 1 000 ppi sont comprimées selon la norme de compression d'images JPEG 2000 (ISO/IEC 15444-1) et son système de codage. Le taux de compression cible est de 15:1.

2. **Photographies**

Les photographies qui peuvent être partagées avec Eurojust aux fins d'une identification fiable des personnes faisant l'objet de procédures pénales liées à des infractions terroristes remplissent les conditions suivantes:

a) une seule image faciale est fournie dans chaque fichier photographique (le fichier photographique NIST) et est saisie conformément à la norme ANSI/NIST-ITL 1-2011 Update 2015, ou à toute version plus récente disponible;

b) les photographies sont soit en niveaux de gris, soit en couleur, soit dans le proche infrarouge;

c) la qualité des photographies est basée sur les exigences fixées pour les images par la norme ISO/IEC 19794-5:2011 Frontal image type, ou toute version plus récente disponible;

d) le fichier photographique NIST permet d'inclure des informations complémentaires, notamment la date à laquelle l'image a été prise;

[1] Pixels par pouce (en anglais: «pixels per inch»).

e) les photographies en mode portrait ont une résolution de 600 pixels par 800 pixels au minimum et de 1 200 pixels par 1 600 pixels au maximum;

f) le visage doit occuper, à l'intérieur de la photographie, un espace suffisant pour qu'il y ait, au minimum, 120 pixels entre les centres de chaque œil;

g) l'algorithme de compression des photographies à utiliser est conforme aux recommandations du NIST. Les photographies ne sont comprimées qu'une seule fois selon la norme de compression d'images et le système de codage JPG (ISO/IEC 10918) ou JPEG 2000 (ISO/IEC 15444), le taux de compression maximal autorisé étant de 20:1.