

ISSN 2432-6089

# 法と情報雑誌

The Law and Information Magazine

第9巻第1号（通巻第55号・2024年1月）

法と情報研究会 編

（第1分冊）

## 本号目次

[資料]

夏井高人	規則(EU) 2022/850 [参考訳]	1～57 頁
夏井高人	委員会決定(EU) 2023/2099 [参考訳]	58～62 頁
夏井高人	指令(EU) 2023/977 [参考訳]	63～132 頁



## 規則(EU) 2022/850

### [参考訳]

2023 年 12 月 22 日  
明治大学法学部教授  
夏井 高人

REGULATION (EU) 2022/850 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (OJ L 150, 1.6.2022, p. 1-19)のテキスト(英語版)に基づいて和訳を試みた。

原文のテキストを入手できるサイトの URL は、下記のとおりである。

<http://data.europa.eu/eli/reg/2022/850/oj>  
[2023 年 11 月 30 日確認]

規則(EU) 2022/850 に関しては、その立法提案の段階で全文訳出を試み、e-CODEX 規則案(COM/2020/712 final)の参考訳(法と情報雑誌 6 巻 5 号 233~319 頁所収)として既に公表した。

規則(EU) 2022/850 の立法趣旨や立法提案に至る経緯等に関しては、この e-CODEX 規則案の中で詳細に述べられている。

e-CODEX 規則案の参考訳の中には誤記や誤訳等が含まれているため、その後、更に検討を加え、再考すべき点は再考した。

この規則(EU) 2022/850 の参考訳は、そのような e-CODEX 規則案の参考訳の見直しのための検討作業を経た上で作成されたものである。

それゆえ、原文が e-CODEX 規則案の提案時と規則としての採択後とではほぼ同一の内容になっている場合であっても、e-CODEX 規則案の参考訳とこの規則(EU) 2022/850 の参考訳との間で異なる訳出となっている箇所がある。

この規則(EU) 2022/850 の参考訳は、あくまでも原文を読む際の参考として提供しているものであり、個人的な見解としての法解釈の結果を「日本語以外の言語で書かれた文書の日本語による翻訳文」というスタイルを用いて表現した文書の一種である。

— 解 説 —

### 1. 規則(EU) 2022/850 について

規則(EU) 2022/850 は、2022 年 5 月 30 日に採択された。

規則(EU) 2022/850 は、2022 年 6 月 21 日に発効した。

規則(EU) 2022/850 の第 18 条は、eu-LISA に関する基本的な法令である規則(EU) 2018/1726 (OJ L 295, 21.11.2018, p. 99-137)の一部改正条項となっている。規則(EU) 2018/1726 の該当する条項は、規則(EU) 2022/850 の発効によって改正された。

## 1. 1 e-CODEX システムについて

e-CODEX システムは、民事及び刑事の法務上の協力の分野におけるデータの国境を越える電子的な交換のためのコンピュータ化されたシステム (computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters)の略称である。

e-CODEX システムは、eu-LISA によって管理される。eu-LISA の組織及び権限は、規則(EU) 2018/1726 (OJ L 295, 21.11.2018, p. 99-137)によって定められている。規則(EU) 2022/850 によって eu-LISA が e-CODEX システムを管理することになった。そのため、規則(EU) 2022/850 の中には eu-LISA の権限を拡張して e-CODEX システムを所管できるようにするための規則(EU) 2018/1726 の一部改正条項が含まれている。

e-CODEX システムは、民事及び刑事の法務上の協力 (judicial cooperation in civil and criminal matters)を支えるための電子的な情報通信システムの一つである。この民事及び刑事の法務上の協力とは、複数の国の裁判所または検察庁の間における協力のことを指し、警察・検察の分野における協力を主たる内容としている。それゆえ、この場合における「judicial」は、「司法」ではなく「法務」である。

e-CODEX システムを用いて送受信される文書は、多種類に及ぶと推定される。eu-LISA の所管事項との関係もあるが、将来、e-CODEX システムを介して交換される電子的な文書の種類が増加する可能性は十分にある。

現在の状態を前提とした上で、e-CODEX システムを用いて送受信される文書の中には、刑事手続上の証拠収集等の目的のために裁判所または検察庁等の法務当局から発令される命令書の類が含まれる。

この関連において特に重要な EU の法令としては、刑事手続における電子証拠の提出命令及び保全命令等を定める規則(EU) 2023/1543 (OJ L 191, 28.7.2023, p. 118-180)、刑事手続における電子証拠の収集の際にその手続に関与するサービスプロバイダの指定等を定める指令(EU) 2023/1544 (OJ L 191, 28.7.2023, p. 181-190)、犯罪捜査と関連する情報交換に関する指令(EU) 2023/977 (OJ L 134, 22.5.2023, p. 1-24)、欧州捜査令状を定める指令 2014/41/EU (OJ L 130, 1.5.2014, p.1-36)をあげることができる。

e-CODEX システムは、情報交換のための手段に過ぎないので、このシステムを用いて実際に交

換される情報がどのようなものなのかを正確に理解することが重要である。

## 1.2 e-CODEX システムの利用と関連するインシデント通知について

規則(EU) 2022/850 の第 11 条第 4 項は、構成国内にある被接続システム (connected systems) の許可された e-CODEX アクセスポイント (authorised e-CODEX access points) 等と関連するインシデントの通知を定め、同条第 5 項は、eu-LISA によって発見された脆弱性及びインシデントの連絡を定めている。後者の脆弱性及びインシデントは、e-CODEX アクセスポイントと関連するインシデントに限定されないと解される。

これらのインシデントの通知及び連絡は、eu-LISA を中心的な管理主体とするセキュリティ管理の体系内における内部的なインシデント情報のエスカレーションとインシデント対応を定めるものと考えられる。

ところで、e-CODEX システムは、複数の構成国の被接続システムと結び付けられた欧州連合全域にわたって連携する情報ネットワークシステムの一つであるので、インシデントの通知及びインシデント対応に関しては、規則(EU) 2022/850 に定める事柄と併行して、NIS2 指令に定めるインシデント通知、インシデント対応及び回復力の確保の体系が存在するので、それら相互の関係が検討されなければならない。

許可された e-CODEX アクセスポイントの中で構成国の行政機関である被接続システムの許可された e-CODEX アクセスポイントに関しては、NIS2 指令に定める各構成国の単一連絡部局を通じて、インシデント情報が ENISA 及びその他の関連部署にエスカレーションされることになると考えられる。

これに対し、構成国内にある行政機関ではない被接続システムの許可された e-CODEX アクセスポイントに関しては、NIS2 指令に定める CSIRT を通じてエスカレーションが行われることになるのかどうか、必ずしも明確ではなく、少なくとも、規則(EU) 2022/850 及び NIS2 指令のいずれにおいても、このことと関連して直接的に定める条項はない。

インシデントの通知及びインシデント対応に関する eu-LISA の権限と ENISA の権限との間の関係の細部に関しても、必ずしも明確であるとは言えない(規則(EU) 2018/1726 の第 37 条及び第 38 条参照)。

例えば SIS のような、eu-LISA が所管する EU の別の大規模 IT システム上で発見されたインシデントが e-CODEX の安全な運用にも影響を与える危険性がある場合の対処は、eu-LISA の長官の裁量に任されていると理解するしかない(規則(EU) 2018/1861 の第 45 条参照)。

この点に関し、eu-LISA が所管する EU の大規模 IT システムと関連する EU の法令に定める関連条項全体を総合的に検討した法学上の研究成果はまだ存在しないようである。

それゆえ、これらの諸点に関し、更に詳細な検討が尽されなければならない。

### 1. 3 規則(EU) 2022/850 の原文中にある誤記等の問題

規則(EU) 2022/850 の原文(英語版)には明らかな誤りが見られる。不完全な文なのではないかと疑われる箇所も存在する。

それらが訂正されるべき誤記等に該当すると欧州委員会が判断する場合、所定の手続を経て EU 官報上で公表されるその正誤表(corrigendum)によっていずれ訂正されることになるかと予想されるが、Eur-lex 上で 2023 年 12 月 5 日の時点において確認できた範囲内では、規則(EU)2022/850 の原文(英語版)に適用される正誤表は公表されていない。

そのため、この参考訳においては、誤記等のある箇所に関し、適宜意識し、または、意識的に原文のままに訳出することにしたが、特に留意すべき点に関しては、「参考訳作成において留意した事項」の項で個別に指摘することにした。

なお、アイルランドに関し、前文(49)では、アイルランドが規則(EU) 2022/850 の採択手続に参加せず、それゆえに同規則がアイルランドを拘束することはない旨が述べられているけれども、その後、アイルランドから欧州委員会に対する通知によってアイルランドが同規則を受諾し、同規則によって拘束される意思をもつことが確認されたため、委員会決定(EU) 2023/2099 (OJL 241, 29.9.2023, p. 144-144)によって、必要な法的対応が行われた。

## 2. 参考訳作成における基本方針

この参考訳においては、規則(EU) 2022/850 の前文(recital)、条文(articles)及び別紙(Annex)の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし、原文を表示することが無意味な部分(特に脚注内)に関しては、原文または訳文の表示を省略した。

この参考訳は、あくまでも規則(EU) 2022/850 の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は、現時点における研究成果を反映するものである。将来、更に研究を深めた結果として修正すべき部分を発見したときは、その時点において、改訂版等を作成すべきかどうかを検討する。

参考訳の訳出に際しては原則として直訳とすることとしたが、直訳のままでは日本語にかなりにくい箇所に関しては、やむを得ず意訳とした。

この参考訳に訳注はない。参考訳中にある脚注は、全て原注である。訳注等による個別の説明がなければ当該箇所の訳出の理由がわかりにくいと想定される箇所に関しては、必要に応じて、「参考訳作成において留意した事項」の中で説明を加えることとした。

読みやすさを重視し、条文中の号(point)の表記を一部省略した。例えば、「point(a)」は「第(a)号」であるが、「第」と「号」を省略し、「(a)」と表記することにした。

この参考訳は、Eur-lex のデータ二次利用条件を遵守して作成した。

### 3. 参考訳作成において留意した事項

この参考訳は規則(EU) 2022/850 の注釈書ではないので、それらの箇所を全てを指摘することは避け、必要に応じて合理的に解釈した上で訳文を作成することにした。

ここでは、特に説明を加えないと誤訳ではないかと誤解される危険性がある箇所を中心に、この参考訳作成において留意した事項を摘記する。

\*\*\*

規則(EU) 2022/850 の前文(12)の第 1 文の中にある「for cross-border exchanges」との箇所は、「for cross-border exchanges of data」の誤記と思われる。

この参考訳においては、合理的に解釈した上で訳出することにした。

規則(EU) 2022/850 の前文(19)の第 1 文の中にある「can be used in cross-border civil and criminal matters」との箇所は、不完全な文であり、「can be used for cross-border judicial corporation in civil and criminal matters」というような文が正しいのではないかと疑われる。

ただし、この参考訳においては、原文のまま訳出することにした。

規則(EU) 2022/850 の前文(25)の第 8 文の中にある「bear the responsibility for any damage resulting from the operation」との箇所は、「bear the liability for any damage resulting from the operation」の誤記ではないかと思われる。

規則(EU) 2022/850 の第 9 条 3 項の「responsibility for any damage」も同様である。

ただし、この参考訳においては、原文のまま合理的に解して訳出することにした。

規則(EU) 2022/850 の前文(35)の中にある「the Commission should provide relevant information」との箇所は、「the Commission should provide eu-LISA with relevant information」の誤記または省略表現ではないかと考えられる。

この参考訳においては、合理的に解釈して訳出することにした。

規則(EU) 2022/850 の前文(37)の第 1 文は不完全な文であり、第 13 条第 3 項と同一の文とすべきものではないかという疑いがある。

ただし、この参考訳においては、原文のまま合理的に解して訳出することにした。

規則(EU) 2022/850 の第 18 条第 2 号の脚注(\*1)の末尾の「(OJ L 150, 31.5.2022, p. 1).;」との箇所は、明白に、「(OJ L 150, 31.5.2022, p. 1).;」の誤記である。

この参考訳においては、そのように解した上で、訳出することにした。

規則(EU) 2022/850 の第 18 条第 5 号(a)の脚注(\*2)の末尾の「(OJ L 312, 7.12.2018, p. 14).」との箇所は、明白に、「(OJ L 312, 7.12.2018, p. 14).」の誤記である。



この参考訳においては、そのように解した上で、訳出することにした。

規則(EU)2022/850 の第 18 条第 5 号(a)の脚注(\*3)の末尾の「(OJL312, 7.12.2018, p. 56).;」との箇所は、明白に、「(OJL312, 7.12.2018, p. 56).;」の誤記である。

この参考訳においては、そのように解した上で、訳出することにした。

#### 4. 関連参考訳

e-CODEX 規則案 (COM/2020/712 final) の参考訳は、法と情報雑誌 6 巻 5 号 233～319 頁にある。  
委員会決定 (EU) 2023/2099 の参考訳は、法と情報雑誌 9 巻 1 号 58～62 頁にある。

指令 2014/41/EU の参考訳は、法と情報雑誌 3 巻 7 号 199～245 頁にある。

eu-LISA 規則 (EU) 2018/1726 の参考訳は、法と情報雑誌 4 巻 3 号 138～188 頁にある。  
ETIAS 規則 (EU) 2018/1240 の参考訳は、法と情報雑誌 4 巻 3 号 42～137 頁にある。入国／出国システム (EES) 規則 (EU) 2017/2226 の参考訳は、法と情報雑誌 3 巻 3 号 201～300 頁にある。  
ECRIS-TCN 規則 (EU) 2019/816 の参考訳は、法と情報雑誌 4 巻 6 号 176～208 頁にある。相互運用性規則 (EU) 2019/817 の参考訳は、法と情報雑誌 4 巻 8 号 79～157 頁にある。相互運用性規則 (EU) 2019/818 の参考訳は、法と情報雑誌 4 巻 8 号 158～231 頁にある。VIS 規則 (EC) No 767/2008 の参考訳は、法と情報雑誌 2 巻 5 号 1～48 頁にある。規則 (EU) 2018/1861 の参考訳は、法と情報雑誌 4 巻 4 号 89～146 頁にある。規則 (EU) 2018/1862 の参考訳は、法と情報雑誌 4 巻 6 号 1～70 頁にある。規則 (EU) 2016/399 (シェンゲンボーダーコード) の参考訳は、法と情報雑誌 2 巻 7 号 1～82 頁にある。

規則 (EU) 2016/679 (一般データ保護規則) の参考訳・再訂版は、法と情報雑誌 3 巻 5 号 1～114 頁にある。規則 (EU) 2018/1725 の参考訳は、法と情報雑誌 4 巻 1 号 1～81 頁にある。指令 2002/58/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 158～187 頁にある。指令 (EU) 2016/680 の参考訳は、法と情報雑誌 2 巻 1 号 41～140 頁にある。

電子識別規則 (EU) No 910/2014 の参考訳は、法と情報雑誌 2 巻 10 号 147～196 頁にある。

規則 (EU) No 182/2011 の参考訳は、法と情報雑誌 3 巻 5 号 168～179 頁にある。

この参考訳の校正等に関し、唐亀侑久氏 (株式会社ラック) の助力を得た。

\*\*\*

**民事及び刑事の法務上の協力の分野におけるデータの国境を越える  
電子的な交換のためのコンピュータ化されたシステム(e-CODEX システム)に関する  
並びに規則(EU) 2018/1726 を改正する  
欧州議会及び理事会の 2022 年 5 月 30 日の規則(EU) 2022/850**

REGULATION (EU) 2022/850 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726

(EEA に適用される正文)

(Text with EEA relevance)

欧州議会及び欧州連合の理事会は、  
欧州連合の機能に関する条約、とりわけ、同条約の第 81 条第 2 項及び第 82 条第 1 項に鑑み、  
欧州委員会からの提案に鑑み、  
立法案を国内議会に送付した後、  
欧州経済社会委員会の意見書に鑑み<sup>1</sup>、  
通常の立法手続に従って審議し<sup>2</sup>、

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,  
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 81(2) and Article 82(1) thereof,  
Having regard to the proposal from the European Commission,  
After transmission of the draft legislative act to the national parliaments,  
Having regard to the opinion of the European Economic and Social Committee <sup>(1)</sup>,  
Acting in accordance with the ordinary legislative procedure <sup>(2)</sup>,

Whereas:

- (1) 市民及び企業の法務への実効的なアクセスを確保すること、並びに、商事を含め民事における及び刑事における構成国間の法務上の協力を容易にすることは、欧州連合の機能に関する条約 (TFEU) の第 3 部第 V 款に掲げられた欧州連合の自由、保安及び法務の領域の主たる目的の中にある。

---

<sup>1</sup> OJ C 286, 16.7.2021, p. 82.

<sup>2</sup> 欧州議会の 2022 年 3 月 24 日付け意見書(官報未搭載)及び理事会の 2022 年 4 月 12 日付け決定。 Position of the European Parliament of 24 March 2022 (not yet published in the Official Journal) and decision of the Council of 12 April 2022.

Ensuring the effective access of citizens and businesses to justice and facilitating judicial cooperation in civil, including commercial, and criminal matters between the Member States are among the main objectives of the Union's area of freedom, security and justice enshrined in Part three, Title V of the Treaty on the Functioning of the European Union (TFEU).

- (2) 形式的で費用のかかる法律上の手続、手続の長期の遅延、及び、裁判所制度を利用することの高額な費用のような多数の理由のゆえに、法務制度にアクセスすることは、時として困難なことである。

It is sometimes difficult to access justice systems for a number of reasons such as formalistic and expensive legal procedures, long procedural delays and high costs of using court systems.

- (3) そこで、デジタルの方法で法務制度が効率的に協力できることを確保するための適切な経路が開発されることが重要である。それゆえ、個人データの保護の権利を常に尊重しつつ、迅速で、直接で、相互運用性があり、持続性があり、信頼できかつ安全な、国境を越える事件関連データの電子的な交換をできるようにする情報技術システムを欧州連合レベルで構築することが不可欠である。そのようなシステムは、市民及び企業が、国内法または欧州連合法によって定められているときは、法務当局またはそれ以外の職務権限のある機関との間で、デジタルの方式で文書及び証拠を交換できるようにすることによって、法務へのアクセス及び透明性を向上させることに貢献すべきである。その制度は、欧州連合内の市民の信頼、及び、構成国の法務当局とそれ以外の職務権限のある機関との間の相互信頼を増加させるべきである。

It is thus important that appropriate channels are developed to ensure that justice systems can efficiently cooperate in a digital way. Therefore, it is essential to establish, at Union level, an information technology system that allows for the swift, direct, interoperable, sustainable, reliable and secure cross-border electronic exchange of case-related data, while always respecting the right to protection of personal data. Such a system should contribute to improving access to justice and transparency by enabling citizens and businesses to exchange documents and evidence in digital form with judicial or other competent authorities, when provided for by national or Union law. That system should increase citizens' trust in the Union and mutual trust between Member States' judicial and other competent authorities.

- (4) 民事及び刑事の手続のデジタル化は、とりわけ、法務へのアクセスを容易にすることによって、欧州連合内における法の支配と基本的な権利の保障を強化することを狙いとして推進されるべきである。

Digitalisation of proceedings in civil and criminal matters should be encouraged with the aim of strengthening the rule of law and fundamental rights guarantees in the Union, particularly by facilitating access to justice.

- (5) この規則は、民事及び刑事の法務上の協力の分野におけるデータの国境を越える電子的な交

換に関係するものである。民事及び刑事における法務上の協力、並びに、法務当局またはそれ以外の職務権限のある機関それぞれの職務権限は、欧州連合の法行為及び欧州連合の司法裁判所の判例法に従って理解されるべきである。

This Regulation concerns the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters. Judicial cooperation in civil and criminal matters and the respective competences of judicial or other competent authorities should be understood in accordance with Union legal acts and the case law of the Court of Justice of the European Union.

- (6) 構成国内に設けられた既存のバックエンドシステムを置き換え、または、高額な費用で修正することのないツールが、事件と関連するデータの国境を越える電子的な交換のために開発されてきた。オンラインデータ交換を介する e-法務通信 (e-CODEX) システムは、今日までに開発されたそのような主たるツールである。

Tools which have not replaced or required costly modifications to the existing back-end systems established in the Member States have previously been developed for the cross-border electronic exchange of case-related data. The e-Justice Communication via Online Data Exchange (e-CODEX) system is the main such tool developed to date.

- (7) e-CODEX システムは、民事及び刑事の法務上の協力の分野におけるデータの国境を越える電子的な交換を容易にするために特別に設計されたツールである。刑事及び民事の手続のデジタル化の増加という文脈において、e-CODEX システムの狙いは、職務権限のある機関間の国境を越える通信の効率性を向上させること、及び、市民と企業の法務へのアクセスを容易にすることにある。欧州議会及び理事会の規則(EU) 2018/1726<sup>3</sup>によって設けられた自由、保安及び法務の領域における大規模 IT システムの業務運営管理のための欧州連合局 (eu-LISA) に対する e-CODEX システムの移管までの間、e-CODEX システムは、欧州連合の計画から資金拠出を受けた構成国及び組織のコンソーシアム(「e-CODEX システム運営管理法主体」)によって運営管理される。

The e-CODEX system is a tool specifically designed to facilitate the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters. In the context of increased digitalisation of proceedings in civil and criminal matters, the aim of the e-CODEX system is to improve the efficiency of cross-border communication between competent authorities and to facilitate citizens'

---

<sup>3</sup> 自由、保安及び法務の領域における大規模 IT システムの業務運営管理のための欧州連合局 (eu-LISA) に関する、並びに、規則(EC) No 1987/2006 及び理事会決定 2007/533/JHA を改正し、規則(EU) No 1077/2011 を廃止する欧州議会及び理事会の 2018 年 11 月 14 日の規則(EU) 2018/1726 (OJ L 295, 21.11.2018, p. 99).

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

and businesses' access to justice. Until the handover of the e-CODEX system to the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), established by Regulation (EU) 2018/1726 of the European Parliament and of the Council<sup>(3)</sup>, the e-CODEX system will be managed by a consortium of Member States and organisations with funding from Union programmes (the 'entity managing the e-CODEX system').

- (8) e-CODEX システムは、法務当局のような職務権限のある国内機関またはそれ以外の組織の IT システムを接続する、法務部門のための相互運用性のあるソリューションを提供する。それゆえ、e-CODEX システムは、民事及び刑事の法務上の協力の分野における国内 IT システム間の相互運用性があり、安全かつ分散型の通信ネットワークにとって好ましいソリューションとして認識されるべきである。

The e-CODEX system provides an interoperable solution for the justice sector to connect the IT systems of the competent national authorities, such as the judiciary, or other organisations. The e-CODEX system should therefore be viewed as the preferred solution for an interoperable, secure and decentralised communication network between national IT systems in the area of judicial cooperation in civil and criminal matters.

- (9) この規則の目的のために、データの電子的な交換は、構造化されまたは構造化されないデータ、ファイルまたはメタデータの形態による文または音響、視覚または視聴覚の記録のような、e-CODEX システムによって電子的な形態で送信され得る全てのコンテンツを含む。

For the purposes of this Regulation, the electronic exchange of data includes any content transmissible in electronic form by means of the e-CODEX system, such as text or sound, visual or audiovisual recordings, in the form of either structured or unstructured data, files or metadata.

- (10) この規則は、e-CODEX システムの義務的な利用を定めない。それと同時に、この規則に定めるいかなる条項も、構成国が利用案件実証実験を開発すること及び維持することを妨げてはならない。

This Regulation does not provide for the mandatory use of the e-CODEX system. At the same time, nothing in this Regulation should prevent Member States from developing and maintaining pilot use cases.

- (11) e-CODEX システムは、2 つのソフトウェア要素によって構成されている:すなわち、別のゲートウェイとの間のメッセージの交換のためのゲートウェイ、そして、国内 IT システム間のメッセージの交換と関連する多数の機能を提供するコネクタである。現在、ゲートウェイは、「eDelivery」として知られ、欧州委員会によって維持管理されている欧州接続機能の汎用構成要素を基盤として構築されており、他方で、コネクタの運営管理は、e-CODEX システム運営管理法主体によって遂行されている。コネクタは、セキュリティライブラリ及び配達証明を介する電子署名の検証のような機

能を提供する。加えて、e-CODEX システム運営管理法主体は、同法主体が e-CODEX システムを実証実験した個別の民事手続及び刑事手続において使用されるデジタル書式のためのデータスキームを開発した。

The e-CODEX system consists of two software elements: a gateway for the exchange of messages with other gateways; and a connector, which provides a number of functionalities related to the exchange of messages between national IT systems. Currently, the gateway is based on a building block of the Connecting Europe Facility maintained by the Commission known as 'eDelivery', while the management of the connector is carried out by the entity managing the e-CODEX system. The connector provides functions such as verification of electronic signatures via a security library and proof of delivery. In addition, the entity managing the e-CODEX system has developed data schemas for digital forms to be used in the specific civil and criminal procedures for which it has piloted the e-CODEX system.

- (12) 欧州連合内の法務上の協力の分野における国境を越えるデータの交換のための e-CODEX システムの重要性に鑑み、e-CODEX システムは、e-CODEX システムの稼働及び開発と関連する規定を定める欧州連合の持続性のある法的枠組みによって構築されるべきである。そのような法的枠組みは、欧州連合基本権憲章に定める基本的な権利、特に同憲章の第VI款に掲げる権利、とりわけ、実効的な救済及び公平な裁判の権利に関する第 47 条に定める権利の保護を確保すべきである。そのような法的枠組みは、それらの基本的な権利の保護のために不可欠な手続上の権利の保護を、いかなる方法によっても損ねてはならない。そのような法的枠組みは、e-CODEX システムの技術上の持続性と防護を保証するため、e-CODEX システムの構成要素も明確に定め、かつ、枠組み設定すべきである。e-CODEX システムは、e-CODEX アクセスポイントの IT 構成要素を定めるべきであり、その e-CODEX アクセスポイントは、識別された別のゲートウェイとの間の安全な通信の目的のためのゲートウェイ及びメッセージの交換を支援する目的のためのコネクタによって構成されるべきである。e-CODEX システムは、民事及び刑事の法務上の協力の分野において採択された欧州連合の法行為によって定められた法律上の手続のための e-CODEX アクセスポイントの利用を支援し、e-CODEX アクセスポイント間の情報の交換をできるようにするためのデジタル手順標準も含めるべきである。

Given the importance of the e-CODEX system for cross-border exchanges in the area of judicial cooperation in the Union, the e-CODEX system should be established by means of a sustainable Union legal framework that provides for rules regarding its functioning and development. Such a legal framework should ensure the protection of fundamental rights as provided for in the Charter of Fundamental Rights of the European Union, especially those enshrined in Title VI thereof, and in particular in Article 47 on the right to an effective remedy and to a fair trial. It should in no way undermine the protection of procedural rights which are essential for the protection of those fundamental rights. It should also clearly set out and frame the components of the e-CODEX system in order to guarantee its technical sustainability and security. The e-CODEX system should establish the IT components of an e-CODEX access point, which should consist of a gateway for the purposes of secure communication with other identified gateways and a connector for the purpose of supporting the exchange of messages. The

e-CODEX system should also include digital procedural standards to support the use of e-CODEX access points for legal procedures provided for by Union legal acts adopted in the area of judicial cooperation in civil and criminal matters and to enable the exchange of information between the e-CODEX access points.

- (13) 相互運用性のレイヤの一つとしてのセマンティックな相互運用性が、複数の関係者間における標準化され、かつ、意味のあるやりとりの準備を整えるというこの規則の目的を達成するために寄与する要素であるべきであるということに鑑み、長期にわたり、かつ、利用案件を横断して、データの一貫性及びデータの品質を確保するために使用される、二次利用可能な意味論上の用語及び定義のための資産である EU の e 法務コア語彙に対し、特別の配慮が与えられるべきである。

Given that semantic interoperability, as one of the layers of interoperability, should be a contributing factor to achieving this Regulation's objective of setting up a standardised and meaningful interaction between two or more parties, particular consideration should be given to the EU e-Justice Core Vocabulary, which is an asset for reusable semantical terms and definitions used to ensure data consistency and data quality over time and across use cases.

- (14) 法務当局の独立性の原則を尊重しつつ、e-CODEX システム及びその統治の長期的な持続性を確保することが必要であることから、適切な e-CODEX システム運営管理法主体が指定されるべきである。当該法主体内における e-CODEX システムの統治の過程において、法務当局の独立性が確保されるべきである。

Since it is necessary to ensure the long-term sustainability of the e-CODEX system and its governance, while respecting the principle of the independence of the judiciary, an appropriate entity for the management of the e-CODEX system should be designated. The independence of the judiciary, in the context of the governance of the e-CODEX system within that entity, should be ensured.

- (15) 部局の統治の構造が、部局の運営会議、計画運営会議及び諮問グループに参加することにより、e-CODEX システムの業務運営管理に構成国が関与することを許容し得るので、e-CODEX システムの業務運営管理のために最も適切な法主体は、部局である。eu-LISA は、大規模 IT システムの業務運営管理と関連する経験をもっている。それゆえ、eu-LISA は、e-CODEX システムの業務運営管理を委託されるべきである。eu-LISA の運営会議の職責を修正することにより、そして、e-CODEX 諮問グループを設置することにより、eu-LISA の現行の統治構造を補正することも必要である。それゆえ、規則(EU) 2018/1726 は、しかるべく改正されるべきである。ジェンダーバランスを考慮に入れた上で、個別の e-CODEX 計画運営会議も設置されるべきである。e-CODEX 計画運営会議は、デジタル手順標準、新機能及びソフトウェアの新バージョンの開発に関するものを含め、活動の優先順序に関し、eu-LISA の運営会議に対して助言すべきである。

The most appropriate entity for the management of the e-CODEX system is an agency, since its governance structure would allow Member States to be involved in the management of the e-CODEX system by participating in the agency's management board, programme management board and advisory



group. eu-LISA has relevant experience in managing large-scale IT systems. eu-LISA should therefore be entrusted with the management of the e-CODEX system. It is also necessary to adjust the existing governance structure of eu-LISA by adapting the responsibilities of its Management Board and by establishing an e-CODEX Advisory Group. Regulation (EU) 2018/1726 should therefore be amended accordingly. A specific e-CODEX Programme Management Board should also be established, taking into account gender balance. The e-CODEX Programme Management Board should advise eu-LISA's Management Board on the prioritisation of activities, including on developing digital procedural standards, new features and new software versions.

- (16) 規則(EU) 2018/1726 の第 19 条に従い、eu-LISA の運営会議の権能は、就中、自由、保安及び法務の領域における大規模 IT システムに影響を与える eu-LISA の全ての判断及び活動が、法務当局の独立性の原則を尊重することを確保するためのものである。eu-LISA の統治構造及び資金の仕組みは、更に、同原則の尊重を保障する。職業法律専門家、それ以外の専門家及び関連する利害関係者が、e-CODEX 諮問グループ及び e-CODEX 計画運営会議を通じて、e-CODEX システムの統治に関与することも重要である。職業法律専門家、それ以外の専門家及び関連する利害関係者の関与と関連する手立て及び条件の詳細は、当該の者らが、実効的に参加し、かつ、端的に言えば、それらの者のフィードバックが適正に考慮されることを確保することによって、実効的に意見聴取できるようにすべきである。

In accordance with Article 19 of Regulation (EU) 2018/1726, the functions of eu-LISA's Management Board are, inter alia, to ensure that all of eu-LISA's decisions and actions which affect large-scale IT systems in the area of freedom, security and justice respect the principle of independence of the judiciary. eu-LISA's governance structure and financing scheme further guarantee that that principle is respected. It is also important to involve the legal professions, other experts and relevant stakeholders in the governance of the e-CODEX system through the e-CODEX Advisory Group and the e-CODEX Programme Management Board. The detailed arrangements and conditions as regards the involvement of the legal professions, other experts and relevant stakeholders should allow them to participate effectively and be consulted effectively, namely by ensuring their feedback is duly considered.

- (17) eu-LISA の優先事項である入国/出国システム(EES)、欧州旅行情報及び許可システム(ETIAS)、第三国国民及び無国籍者に関する前科情報を保有する構成国の識別に関する集中化されたシステム(ECRIS-TCN)、改良されたシェンゲン情報システム(SIS)、Visa 情報システム(VIS)及び Eurodac の開発及び運営管理の職務、並びに、EU の情報システム間の相互運用性の枠組みを構築する戦略的な職務に鑑み、eu-LISA は、2023 年 7 月 1 日から 2023 年 12 月 31 日までの間に e-CODEX システムの職責を受継すべきである。

Given eu-LISA's priority tasks of developing and managing the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN), the revised Schengen Information System (SIS), the Visa Information System (VIS) and Eurodac,

as well as the strategic task of establishing a framework for interoperability between EU information systems, eu-LISA should take over the responsibility for the e-CODEX system between 1 July 2023 and 31 December 2023.

- (18) e-CODEX 連絡担当者は、この規則に基づく技術上の支援を要請し、それを受ける資格をもつべきであり、構成国間における e-CODEX システムの運用を支援すべきである。eu-LISA によって遂行される活動のサービスレベルの要求事項は、構成国または欧州委員会によって許可された e-CODEX アクセスポイントの数に比例し、かつ、許可された e-CODEX アクセスポイントが適用するデジタル手順標準の数と比例する構成国内及び欧州委員会内の e-CODEX 連絡担当者の数という事柄に対処すべきである。

e-CODEX correspondents should be entitled to request and receive technical support under this Regulation and should support the operation of the e-CODEX system among Member States. The service level requirements for the activities to be carried out by eu-LISA should address the matter of the number of e-CODEX correspondents in Member States and in the Commission, in proportion to the number of the e-CODEX access points authorised by the Member States or by the Commission and to the number of the digital procedural standards which they apply.

- (19) e-CODEX システムは、国境を越える民事及び刑事において使用され得る。そのような利用が e-CODEX システムの利用を阻害しない限り、国内法または欧州連合法に基づく法務上の協力の外にある別の目的のために e-CODEX システム及び e-CODEX システムの構成要素を利用できるべきである。この規則は、対応するデジタル手順標準に従い、許可された e-CODEX アクセスポイントを介して被接続システム間における国境を越えるデータの交換に対してのみ適用される。

The e-CODEX system can be used in cross-border civil and criminal matters. It should be possible to use the e-CODEX system and the components of the e-CODEX system for other purposes outside of the scope of judicial cooperation under national or Union law as long as such use does not impair the use of the e-CODEX system. This Regulation only applies to the cross-border exchange of data between connected systems via authorised e-CODEX access points, in accordance with the corresponding digital procedural standards.

- (20) ゲートウェイの運営管理は、現在のところ、eDelivery 内で、部門横断ベースで、欧州委員会によって提供されているので、ゲートウェイの運営管理を除き、eu-LISA は、e-CODEX システムの構成要素に関する職責を負うべきである。eu-LISA は、e-CODEX システム運営管理法主体から、コネクタ及びデジタル手順標準の業務運営管理の全ての職責を受継すべきである。ゲートウェイとコネクタが e-CODEX システムの統合された構成要素であることに鑑み、eu-LISA は、コネクタが、最新版のゲートウェイと互換性をもつことを確保すべきである。その目的のために、欧州委員会 は、eu-LISA が e-CODEX システムの職責を受継する前に実施される準備作業に、及び、この規則の発効時点から、eDelivery の関連統治組織に eu-LISA を包摂すべきである。

eu-LISA should be responsible for the components of the e-CODEX system, except for the management of the gateway, since it is currently provided by the Commission on a cross-sectoral basis within eDelivery. eu-LISA should take over full responsibility for the management of the connector and the digital procedural standards from the entity managing the e-CODEX system. Given that the gateway and the connector are integral components of the e-CODEX system, eu-LISA should ensure that the connector is compatible with the latest version of the gateway. To that end, the Commission should include eu-LISA in the preparatory work undertaken before eu-LISA takes over responsibility for the e-CODEX system and in the relevant governance body of eDelivery as from the entry into force of this Regulation.

- (21) この規則の実装のための統一的な条件を確保するため、実装権限は、欧州委員会に対して与えられるべきである。それらの権限は、欧州議会及び理事会の規則(EU) No 182/2011<sup>4</sup>に従って実行されるべきである。当該枠組みの中で採択された実装行為は:防護に関するもの及び完全性と真正性の検証の手法に関するものを含め、e-CODEX システムの構成要素を支えるミニマムの技術仕様と技術標準;eu-LISA によって遂行される活動のためのサービスレベルの要求事項、及び、許可された e-CODEX アクセスポイントの数に比例し、かつ、e-CODEX アクセスポイントが適用するデジタル手順標準の数に比例する許可された e-CODEX アクセスポイントに対応する e-CODEX 連絡担当者の数を含め、当該活動のために必要なその他の技術仕様;並びに、e-CODEX システムの移管及び受継のための個別の覚書を定めるべきである。実装行為は、民事及び刑事の法務上の協力の分野の手続における e-CODEX システムの利用を支えるデジタル手順標準も定め得るべきである。

In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council<sup>(4)</sup>. The implementing acts adopted in that framework should establish: the minimum technical specifications and standards, including for security and methods for integrity and authenticity verification, underpinning the components of the e-CODEX system; the service level requirements for the activities carried out by eu-LISA and other necessary technical specifications for those activities, including the number of e-CODEX correspondents for the authorised e-CODEX access points, in proportion to the number of authorised e-CODEX access points and to the number of digital procedural standards which they apply; and the specific arrangements for the handover and takeover of the e-CODEX system. Implementing acts should also be able to establish digital procedural standards to support the use of the e-CODEX system in the procedures in the area of judicial cooperation in civil and criminal matters.

---

<sup>4</sup> 欧州委員会の実装権限の行使の構成国による管理のための仕組みに関する規定及び一般原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011 (OJ L 55, 28.2.2011, p. 13).

Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

- (22) コネクタは、欧州議会及び理事会の規則(EU) No 910/2014<sup>5)</sup>に定める全てのタイプの電子シール及び電子署名に技術的に対応できるべきである。欧州委員会によって定められるミニマムの技術仕様及び技術標準は、コネクタと関連するセキュリティ運用基準を含めるべきである。コネクタの稼働に関するセキュリティ上の要求事項は、情報セキュリティの技術標準、そして、欧州議会及び理事会の規則(EU) No 910/2014、規則(EU) No 2016/679<sup>6)</sup>及び規則(EU) 2018/1725<sup>7)</sup>並びに欧州議会及び理事会の指令(EU) 2016/680<sup>8)</sup>のような欧州連合の現行の法行為を考慮すべきである。

The connector should be able to technically support all types of electronic seals and electronic signatures as provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council<sup>5)</sup>. The minimum technical specifications and standards established by the Commission should include security operating standards regarding the connector. The security requirements for the functioning of the connector should take into account standards for information security and existing Union legal acts, such as Regulations (EU) No 910/2014, (EU) No 2016/679<sup>6)</sup> and (EU) 2018/1725<sup>7)</sup> of the European Parliament and of the Council and Directive (EU) 2016/680 of the European Parliament and of the Council<sup>8)</sup>.

---

<sup>5)</sup> 域内市場における電子的なやりとりのための電子識別及び信頼サービスに関する、及び、指令 1999/93/EC を廃止する欧州議会及び理事会の 2014 年 7 月 23 日の規則(EU) No 910/2014 (OJ L 257, 28.8.2014, p. 73).

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

<sup>6)</sup> 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679 (一般データ保護規則) (OJ L 119, 4.5.2016, p. 1).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

<sup>7)</sup> 欧州連合の機関、組織、事務局及び部局による個人データの処理と関連する自然人の保護に関する並びにそのデータの支障のない移動に関する、並びに、規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39).

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

<sup>8)</sup> 犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行の目的のために職務権限のある機関による個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/680 (OJ L 119, 4.5.2016, p. 89).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

- (23) e-CODEX システムの運営管理と関係する eu-LISA の個別の職責が定められるべきである。

The specific responsibilities of eu-LISA in relation to the management of the e-CODEX system should be laid down.

- (24) eu-LISA の職務は、それが必要なときは、e-CODEX システムへの新機能の追加を含めるべきである。そのような新機能の一つは、個々の許可された e-CODEX アクセスポイントを介して送受信された技術メッセージの数に関する関連統計データを検索できるようにするコネクタ内の機能であるべきである。

The tasks of eu-LISA should include the addition of new features to the e-CODEX system, if needed. One such new feature should be a feature in the connector allowing for the retrieval of relevant statistical data regarding the number of technical messages sent and received through each authorised e-CODEX access point.

- (25) 国内レベルにおいて、構成国は、行政機関に対し、または、民間会社及び法律実務家を代表する組織のような法人に対し、e-CODEX アクセスポイントを運営管理することを許可できるべきである。構成国は、そのような許可された e-CODEX アクセスポイントのリストを維持管理し、かつ、関連する手続の過程において e-CODEX アクセスポイントが相互にやりとりできるようにするため、eu-LISA に対し、そのリストを通知すべきである。国内レベルにおいて許可された e-CODEX アクセスポイントを運営管理する法主体は、規則(EU) 2016/679 に定めるデータ保護の要件及び基本原則を遵守すべきである。欧州連合レベルにおいて、欧州委員会は、欧州連合の機関、組織、事務局または部局に対し、e-CODEX アクセスポイントを運営管理することを許可できるべきである。欧州委員会は、そのような許可された e-CODEX アクセスポイントのリストを維持管理し、かつ、関連する手続の過程において e-CODEX アクセスポイントが相互にやりとりできるようにするため、eu-LISA に対し、そのリストを通知すべきである。欧州連合レベルにおいて許可された e-CODEX アクセスポイントを運営管理する法主体は、規則(EU)2018/1725 に定めるデータ保護の要件及び基本原則を遵守すべきである。e-CODEX システムの業務運営管理を eu-LISA が確保すべきものとしつつ、かつ、e-CODEX システムの分散型の性質に鑑み、許可された e-CODEX アクセスポイントの設置及び運営の職責は、専ら、関連する e-CODEX アクセスポイントを運営管理する法主体にあるべきである。許可された e-CODEX アクセスポイントを運営管理する法主体は、適用可能な法律に従い、当該許可された e-CODEX アクセスポイントの運営管理から生ずる損害に対する責任を負うべきである。構成国及び欧州委員会は、許可された e-CODEX アクセスポイントを運営管理する法主体が、e-CODEX システムが適正かつ信頼できる態様で機能することを保証するために必要となる技術上の機器及び人的資源をもつことを検証すべきである。当該法主体が、必要な技術上の機器及び人的資源をもたない場合、当該法主体の許可された e-CODEX アクセスポイントは、e-CODEX アクセスポイントの許可を失うべきである。

At national level, it should be possible for Member States to authorise public authorities or legal persons, such as private companies and organisations representing legal practitioners, to operate e-CODEX access points. The Member States should maintain a list of such authorised e-CODEX access points and notify

them to eu-LISA in order to enable them to interact with one another in the context of the relevant procedures. Entities operating authorised e-CODEX access points at national level are to comply with the data protection requirements and principles laid down in Regulation (EU) 2016/679. At Union level, it should be possible for the Commission to authorise Union institutions, bodies, offices or agencies to operate e-CODEX access points. The Commission should maintain a list of such authorised e-CODEX access points and notify them to eu-LISA in order to enable them to interact with one another in the context of the relevant procedures. Entities operating authorised e-CODEX access points at Union level are to comply with the data protection requirements and principles laid down in Regulation (EU) 2018/1725. While eu-LISA should ensure the management of the e-CODEX system, and having regard to the decentralised nature of the e-CODEX system, the responsibility for setting up and operating the authorised e-CODEX access points should lie exclusively with the entities operating the relevant authorised e-CODEX access points. An entity operating an authorised e-CODEX access point should bear the responsibility for any damage resulting from the operation of that authorised e-CODEX access point, in accordance with the applicable law. The Member States and the Commission should verify that entities operating authorised e-CODEX access points have the necessary technical equipment and human resources in order to guarantee that the e-CODEX system functions properly and in a reliable manner. Where those entities do not have the necessary technical equipment and human resources, their authorised e-CODEX access point should lose its authorisation.

- (26) 構成国は、とりわけ、行政機関ではない法主体によって e-CODEX アクセスポイントが運営管理される場合においては、当該構成国が職責を負う許可された e-CODEX アクセスポイントを監督すべきである。構成国は、適切なデータ防護措置が設けられることを確保すべきである。

Member States should supervise the authorised e-CODEX access points for which they are responsible, in particular when they are operated by entities that are not public authorities. Member States should ensure that adequate data security measures are in place.

- (27) 構成国は、Web サイト及びソーシャルメディアプラットフォームを含め、大規模な通信経路のセットによって、一般公衆に対し、e-CODEX システムに関して情報提供すべきである。

Member States should inform the general public about the e-CODEX system by means of a set of large-scale communication channels, including websites and social media platforms.

- (28) 当該構成国が許可した個々の e-CODEX アクセスポイントが適用する資格をもつデジタル手順標準を決定するのは各構成国であるが、各構成国は、それだけではなく、この規則に基づく実装行為によって採択されたデジタル手順標準が当該構成国の領土において適用されることも確保すべきである。

While it is for each Member State to determine the digital procedural standards which each e-CODEX access point it has authorised is entitled to apply, each Member State should nevertheless ensure that all

the digital procedural standards adopted by means of implementing acts under this Regulation apply in their territory.

- (29) 欧州連合内の民事及び刑事の法務上の協力の分野におけるデータの国境を越える電子的な交換をできるようにする道具の影響を監視するための仕組みが設けられるべきである。それゆえ、許可された e-CODEX アクセスポイントを運営管理する法主体は、e-CODEX システムの利用に関する包括的なデータを自動的に収集し、維持管理できるべきである。それは、関連データの収集における構成国の仕事を緩和し、相互の説明責任と透明性を確保するものであるべきであるだけでなく、民事及び刑事の法務上の協力の分野において採択された欧州連合の法行為の欧州委員会による事後的な監視を大きく容易にするものでもあるべきである。収集された情報は、集約されたデータのみを包含すべきであり、かつ、個人データを構成してはならない。

A mechanism should be put in place to monitor the impact of instruments that enable the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters in the Union. The entities operating authorised e-CODEX access points should therefore be able to systematically collect and maintain comprehensive data on the use of the e-CODEX system. That should not only alleviate the work of the Member States in collecting the relevant data and ensure mutual accountability and transparency, but also significantly facilitate the ex-post monitoring by the Commission of the Union legal acts adopted in the area of judicial cooperation in civil and criminal matters. The information collected should only encompass aggregated data and should not constitute personal data.

- (30) ゲートウェイの目的のための場合を含め、e-CODEX システムと関係して e-CODEX 連絡担当者に対する技術上の支援を提供する場合、eu-LISA は、単一連絡先として行動すべきである。

When providing technical support to e-CODEX correspondents in relation to the e-CODEX system, eu-LISA should act as a single point of contact, including for the purposes of the gateway.

- (31) eu-LISA は、その職務を遂行する際、高いレベルのセキュリティを維持すべきである。ソフトウェアの更なる技術的進化またはアップグレードの開発に従事する際、eu-LISA は、規則(EU) 2018/1725 に従い、バイデザインのセキュリティの原則並びにバイデザイン及びバイデフォルトのデータ保護の原則を実装すべきである。許可された e-CODEX アクセスポイントを運営管理する法主体は、当該法主体の e-CODEX アクセスポイントを介して送信されるデータの防護及び保護に関する職責を負うべきである。

eu-LISA should maintain a high level of security when carrying out its tasks. When undertaking further technical evolutions of software or developing upgrades, eu-LISA should implement the principles of security by design and data protection by design and by default, in accordance with Regulation (EU) 2018/1725. An entity operating an authorised e-CODEX access point should bear the responsibility for the security and protection of the data transmitted via its authorised e-CODEX access point.

- (32) 欧州連合の利益において交換される機密情報の保護に関する理事会内会合における欧州連合の構成国間の合意<sup>9</sup>の第 2 条に定義する機密情報は、同合意、それ以外の欧州連合の法行為及び国内法に定める関連条件が満たされない限り、e-CODEX システムを介して送信されてはならない。

Classified information, as defined in Article 2 of the Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union<sup>(9)</sup>, should not be transmitted via the e-CODEX system, unless the relevant conditions provided for in that Agreement, in other Union legal acts and in national law are fulfilled.

- (33) eu-LISA が e-CODEX システムの受継を適切に準備できるようにするため、e-CODEX システム運営管理法主体は、2022 年 12 月 31 日までに、この規則により欧州委員会によって採択される実装行為に従い、無事な移管過程及び同過程の無事な完了のための基準を含め、e-CODEX システムの移管のための詳細な手立てを定める移管文書を提出すべきである。その移管文書は、ゲートウェイ、コネクタ及びデジタル手順標準並びに関連支援ソフトウェア製品、文書及びそれ以外の資産を含め、e-CODEX システムの構成要素を包摂すべきである。欧州委員会は、この規則により採択された実装行為及び移管文書を eu-LISA が遵守することを確保するため、移管及び受継の過程を監視すべきである。欧州委員会が、e-CODEX システム運営管理法主体及び eu-LISA の意見聴取を経た上で、その過程が無事に完了したことを宣言した後に限り、その受継が起きるべきである。移管文書の提出の後、eu-LISA への e-CODEX システムの無事な移管までの間、e-CODEX システム運営管理法主体は、e-CODEX システムに対して変更を行ってはならず、または、e-CODEX システムの保守管理を遂行する目的のため以外の場合に、新たなソフトウェアリリースを配布してはならない。

In order to allow eu-LISA to prepare adequately for the takeover of the e-CODEX system, the entity managing the e-CODEX system should submit by 31 December 2022 a handover document setting out the detailed arrangements for the transfer of the e-CODEX system, including the criteria for a successful handover process and for the successful completion of that process, in accordance with implementing acts adopted by the Commission pursuant to this Regulation. The handover document should cover the components of the e-CODEX system, including the gateway, the connector and the digital procedural standards, as well as the relevant supporting software products, documentation and other assets. The Commission should monitor the handover and takeover process in order to ensure that it complies with the implementing acts adopted pursuant to this Regulation and the handover document. The takeover should only take place once the Commission has declared that the process has been successfully completed, after consulting the entity managing the e-CODEX system and eu-LISA. After submitting the handover document and until the successful handover of the e-CODEX system to eu-LISA, the entity managing the e-CODEX system should not make changes to the e-CODEX system or deliver any new

---

<sup>9</sup> OJ C 202, 8.7.2011, p. 13.



software release other than for the purpose of carrying out corrective maintenance of the e-CODEX system.

- (34) eu-LISA への e-CODEX システム移管の一部として、この規則の下にある eu-LISA の職責を eu-LISA が遂行できるようにするため、e-CODEX システムと関連する知的財産権または利用権並びに関連支援ソフトウェア製品、文書及びそれ以外の資産が eu-LISA に対して移転されることを確保されるべきである。ただし、e-CODEX システムの主要なソフトウェア構成要素に関しては、当該ソフトウェア構成要素がオープンソースであり、欧州連合公共使用許諾 (EUPL) の適用があるので、契約による移転を要しない。

As part of the handover of the e-CODEX system to eu-LISA, it should be ensured that any intellectual property rights or usage rights relating to the e-CODEX system and the relevant supporting software products, documentation and other assets are transferred to eu-LISA so as to enable it to carry out its responsibilities under this Regulation. However, for the main software components of the e-CODEX system, a contractual transfer is not needed because those software components are open source and covered by the European Union Public Licence.

- (35) e-CODEX システムを欧州委員会が定期的に評価できるようにするため、eu-LISA は、欧州委員会に対し、2 年毎に、e-CODEX システムの技術的進化及び技術の稼働に関し、報告すべきである。その報告書にフィードするため、構成国は、eu-LISA に対し、当該構成国の領土内にある被接続システム毎の許可された e-CODEX アクセスポイントと関係する関連情報を提供すべきであり、また、欧州委員会は、eu-LISA に対し、欧州連合の機関、組織、事務局及び部局によって運営管理されている許可された e-CODEX アクセスポイントと関係する関連情報を提供すべきである。

In order for the Commission to be able to evaluate the e-CODEX system on a regular basis, eu-LISA should report to the Commission every two years on the technical evolution and the technical functioning of the e-CODEX system. In order to feed into that report, Member States should provide eu-LISA with the relevant information concerning the authorised e-CODEX access points for the connected systems in their territory, and the Commission should provide relevant information concerning the authorised e-CODEX access points operated by Union institutions, bodies, offices and agencies.

- (36) e-CODEX 諮問グループは、eu-LISA に対し、とりわけ、経験とベストプラクティスの交換を促進することにより、e-CODEX システムと関連する必要な専門知識を提供すべきである。構成国の発意により開始されたデジタル手順標準を含め、新たなデジタル手順標準の開発に e-CODEX 諮問グループが参加できるべきである。

The e-CODEX Advisory Group should provide eu-LISA with the necessary expertise related to the e-CODEX system, in particular by promoting the exchange of experiences and best practices. It should be possible for the e-CODEX Advisory Group to be involved in the development of new digital procedural standards, including those launched at the initiative of Member States.

- (37) e-CODEX 計画運営会議の構成員及び同構成員の代替要員は、再任され得るべきである。e-CODEX 計画運営会議への異なる構成国の代表に対し、適正な配慮が与えられるべきであり、それが可能である限り、経時的には全ての構成国が e-CODEX 計画運営会議において代表されることを確保するため、それが促進されるべきである。

The term of office of the members of the e-CODEX Programme Management Board and their alternates should be renewable. Due consideration should be given to the representation of different Member States on the e-CODEX Programme Management Board, which is to be promoted whenever possible so as to ensure that all Member States are represented on the e-CODEX Programme Management Board over time.

- (38) e-CODEX 計画運営会議の義務を遂行する際、e-CODEX 計画運営会議は、e-CODEX システムと関連して eu-LISA によって講じられた全ての措置が、例えば、インフラ、データ管理及びデータ分離に関する措置のような技術上の措置、または、鍵となる要員及びそれ以外の人的資源に関する措置のような組織的な措置が法務当局の独立性の原則に適うものであることを確保すべきである。

When carrying out its duties, the e-CODEX Programme Management Board should ensure that all measures taken by eu-LISA regarding the e-CODEX system, either technical, for example measures concerning infrastructure, data management and data separation, or organisational, for example measures concerning key personnel and other human resources, are in accordance with the principle of the independence of the judiciary.

- (39) 欧州議会及び理事会が e-CODEX システムの移転の完了を評価できるようにし、かつ、e-CODEX システムが一般的にどのように良好に稼働しているかを評価できるようにするため、欧州委員会は、e-CODEX システムの全体的な評価書を定期的に作成すべきである。欧州委員会は、e-CODEX システムに関する職責を eu-LISA が受継した 3 年後にそのような最初の評価書を準備し、かつ、その後は 4 年毎に準備すべきである。

In order to enable the European Parliament and the Council to assess the success of the transfer of the e-CODEX system and how well the e-CODEX system functions in general, the Commission should regularly produce overall evaluations of the e-CODEX system. The Commission should prepare the first such evaluation three years after eu-LISA takes over responsibility for the e-CODEX system and every four years thereafter.

- (40) この規則に定める eu-LISA の新たな職務を適切に遂行できるようにすることを確保するため、十分な資源が eu-LISA に対して提供されるべきである。この規則に従って e-CODEX システムの運営管理のために割当てられるべきその資源は、別の目的のために使用してはならない。

Sufficient resources should be provided to eu-LISA in order to ensure that it is able to adequately carry

out its new tasks as set out in this Regulation. The resources committed to the operation of the e-CODEX system in accordance with this Regulation should not be used for any other purpose.

- (41) この規則に定める職務の遂行において負担する費用に関しては、この規則のいかなる条項も、構成国が、e-CODEX システムの国内レベルの実装のための欧州連合の資金計画からの資金提供を申請することを妨げてはならない。

As regards the costs incurred in the performance of tasks laid down by this Regulation, nothing in this Regulation should prevent Member States from applying for funding from Union financing programmes for the implementation of the e-CODEX system at national level.

- (42) 国内法によって許容されている限り、この規則のいかなる条項も、eu-LISA に対する情報の、とりわけ、この規則に定める通知の、自動化された方法による提出を妨げてはならない。

Insofar as permitted by national law, nothing in this Regulation prevents the submission of information to eu-LISA in an automated way, in particular the notifications provided for in this Regulation.

- (43) この規則は、個人データの処理のための特別の法的根拠を提供していない。この規則に基づく個人データの処理は、適用可能なデータ保護の規定に従うべきである。欧州議会及び理事会の規則(EU) 2016/679 並びに指令 2002/58/EC<sup>10</sup>及び指令(EU) 2016/680 は、この規則に従って構成国の領土内に設けられている許可された e-CODEX アクセスポイントを運営管理する法主体によって遂行される個人データの処理に適用される。

This Regulation does not provide any specific legal basis for the processing of personal data. Any processing of personal data under this Regulation should be in accordance with the applicable data protection rules. Regulation (EU) 2016/679 and Directives 2002/58/EC<sup>(10)</sup> and (EU) 2016/680 of the European Parliament and the Council apply to the processing of personal data carried out by entities operating authorised e-CODEX access points which are established within the territory of the Member States in accordance with this Regulation.

- (44) 規則(EU) 2018/1725 は、この規則に基づいて欧州連合の機関、組織、事務局及び部局によって遂行される個人データの処理に適用される。

Regulation (EU) 2018/1725 applies to the processing of personal data carried out by Union institutions,

---

<sup>10</sup> 電子通信部門における個人データ処理及びプライバシー保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC (プライバシー及び電子通信に関する指令) (OJ L 201, 31.7.2002, p. 37).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

bodies, offices and agencies under this Regulation.

- (45) 国際公法によって規律される国際機関もしくは同機関の下部組織、または、それ以外の関連法主体もしくは組織であって、複数の国家間の協定によって設置され、もしくは、複数の国家間の協定を基礎とするものが、e-CODEX システムの業務運営管理が eu-LISA に対して委託された後において、関連する利害関係者として e-CODEX システムに参加できるべきである。その目的のために、そして、e-CODEX システムの実効的で、標準化され、かつ、安全な運用管理を確保するため、eu-LISA が、規則(EU) 2018/1726 により、当該機関、組織及び法主体との間で作業覚書を締結できるべきである。

It should be possible for international organisations or their subordinate bodies, governed by public international law, or other relevant entities or bodies, which are set up by, or on the basis of, an agreement between two or more countries, to participate in the e-CODEX system as relevant stakeholders after its operational management has been entrusted to eu-LISA. To that end, and in order to ensure the effective, standardised and secure operation of the e-CODEX system, it should be possible for eu-LISA to conclude working arrangements with those organisations, bodies and entities pursuant to Regulation (EU) 2018/1726.

- (46) この規則の目的、すなわち、欧州連合レベルで e-CODEX システムを設置し、システムの運営管理を eu-LISA に委託することは、構成国によっては十分に達成され得ず、その活動の規模及び影響のゆえに、欧州連合レベルでより良く達成され得るので、欧州連合は、欧州連合条約 (TEU) の第 5 条に定める補完性の原則に従い、措置を採択できる。同条に定める比例性の原則に従い、この規則は、当該目的を達成するために必要なところを超えることがない。

Since the objectives of this Regulation, namely the establishment of the e-CODEX system at Union level and the entrusting of the system's management to eu-LISA, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

- (47) 欧州委員会は、第三国の e-CODEX システムへの参加を許容することの実現可能性を検討すべきであり、かつ、それが必要なときは、そのような参加をできるものとし、かつ、その目的のための規定及び手順を定める立法提案書を提示すべきである。

The Commission should study the feasibility of allowing third countries to participate in the e-CODEX system and, if necessary, present a legislative proposal to allow for such participation and to lay down rules and protocols to that end.

- (48) TEU 及び TFEU に附属するデンマークの地位に関する議定書第 22 号の第 1 条及び第 2 条に

従い、デンマークは、この規則の採択に参加しておらず、この規則によって拘束されることがなく、または、この規則の適用に服さない。

In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

- (49) TEU 及び TFEU に附属する自由、保安及び法務の領域に関する英国及びアイルランドの地位に関する議定書第 21 号の第 1 条及び第 2 条及び第 4 条 a 第 1 項に従い、かつ、同議定書の第 4 条を妨げることなく、アイルランドは、この規則の採択に参加しておらず、この規則によって拘束されることがなく、または、この規則の適用に服さない。

In accordance with Articles 1 and 2 and Article 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

- (50) eu-LISA の本拠地は、エストニアのタリンに定められた。eu-LISA の特別の性格及び特性を考慮し、エストニアのタリンにおいて e-CODEX システムを開発し、業務運営上の管理をすることが適切であると判断された。

eu-LISA's seat was established in Tallinn, Estonia. In view of its specific nature and characteristics, it was considered appropriate to develop and operationally manage the e-CODEX system in Tallinn, Estonia.

- (51) 欧州データ保護監督官は、規則(EU)2018/1725 の第 42 条第 1 項に従って意見聴取を受け、2021 年 1 月 26 日にその意見を伝達した、

The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 26 January 2021,

以上のおりであるので、この規則を採択する:

**HAVE ADOPTED THIS REGULATION:**

## 第 1 章 総則的な規定

### Chapter 1 General Provisions

#### 第 1 条 対象事項

##### Article 1 Subject matter

1. この規則は、e-CODEX システムの法的枠組みを設ける。

This Regulation establishes the legal framework for the e-CODEX system.

2. この規則は、以下の事項に関する規定を定める:
  - (a) e-CODEX システムの定義、構成要素、機能及び運営管理;
  - (b) 自由、保安及び法務の領域における大規模 IT システムの業務運営管理のための欧州連合局 (eu-LISA) の e-CODEX システムと関連する職責;
  - (c) 欧州委員会、構成国及び許可された e-CODEX アクセスポイントを運営管理する法主体の職責;
  - (d) e-CODEX システムの保安に関する法的枠組み。

This Regulation lays down rules on the following:

- (a) the definition, composition, functions and management of the e-CODEX system;
- (b) the responsibilities of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) regarding the e-CODEX system;
- (c) the responsibilities of the Commission, Member States and the entities operating authorised e-CODEX access points;
- (d) the legal framework for the security of the e-CODEX system.

#### 第 2 条 適用範囲

##### Article 2 Scope

この規則は、民事及び刑事の法務上の協力の分野において採択された欧州連合の法行為に従った e-CODEX システムによる同分野におけるデータの国境を越える電子的な交換に対して適用される。

This Regulation applies to the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters by means of the e-CODEX system in accordance with the Union legal acts adopted in that area.

### 第3条 定義

#### Article 3 Definitions

この規則の目的のために、以下の定義が適用される:

- (1) 「e-CODEX システム」(オンラインデータ交換を介する e-法務通信システム)とは、民事及び刑事の法務上の協力の領域において、迅速、安全かつ信頼できる態様で、データの電子的な交換を容易にする目的のための国境を越える通信であって、電子的な形態により伝送可能なコンテンツを含む通信のための、分散型で相互運用性のあるシステムのことを意味し;
- (2) 「e-CODEX アクセスポイント」とは、ハードウェアインフラ上にインストールされたソフトウェアパッケージであって、安全かつ信頼できる態様で、他の e-CODEX アクセスポイントに対して情報を送信し、及び、他の e-CODEX アクセスポイントから情報を受信することができるもののことを意味し;
- (3) 「許可された e-CODEX アクセスポイント」とは、第 6 条第 4 項または第 8 条第 1 項に従って欧州委員会または構成国によって許可され、かつ、eu-LISA に対して通知された e-CODEX アクセスポイントであって、少なくとも 1 つのデジタル手順標準を適用するもののことを意味し;
- (4) 「許可された e-CODEX アクセスポイントを運営管理する法主体」とは、国内行政機関もしくは国内法の下で許可された法人または欧州連合の機関、組織、事務局もしくは部局であって、許可された e-CODEX アクセスポイントを運営管理しているもののことを意味し;
- (5) 「e-CODEX 連絡担当者」とは、構成国または欧州委員会によって指定された自然人であって、第 7 条第 3 項に従って e-CODEX システムの全ての構成要素に関して eu-LISA から第 7 条第 1 項(f)に示す技術上の支援を要請することができ、また、その支援を受けることができる者のことを意味し;
- (6) 「被接続システム」とは、他のそのような IT システムとの間におけるデータの交換の目的のために e-CODEX アクセスポイントと接続されている IT システムのことを意味し;
- (7) 「中央検査プラットフォーム」とは、専ら検査のために利用される e-CODEX システムの構成要素であって、当該法主体の許可された e-CODEX アクセスポイントが正しく運営管理されているか否か、及び、当該法主体の許可された e-CODEX アクセスポイントと結びつけられている被接続システム内のデジタル手順標準が正しく使用されているかどうかを検査するために、許可された e-CODEX アクセスポイントを運営管理する法主体によって利用され得る機能のセットを提供するもののことを意味し;
- (8) 「業務プロセスモデル」とは、複数の通信当事者間の標準化され、かつ、意味のあるやりとりを達成するための、関連するデータモデルに沿って関連付けられ、構造化された複数の活動または職務の概念モデル、並びに、その流れの中で遂行されなければならない活動または職務の流れの図及び文による表現のことを意味し;
- (9) 「デジタル手順標準」とは、EU の e 法務コア語彙を基盤とする e-CODEX システムを介するデータ交換の電子的な構造を定める業務プロセスモデル及びデータスキームのための技術仕様のことを意味する。

For the purposes of this Regulation, the following definitions apply:

- (1) ‘e-CODEX system’ (e-Justice Communication via Online Data Exchange system) means a decentralised and interoperable system for cross-border communication for the purpose of facilitating the electronic exchange of data, which includes any content transmissible in electronic form, in a swift, secure and reliable manner in the area of judicial cooperation in civil and criminal matters;
- (2) ‘e-CODEX access point’ means the software packages installed on hardware infrastructure which are able to transmit information to and receive information from other e-CODEX access points in a secure and reliable manner;
- (3) ‘authorised e-CODEX access point’ means an e-CODEX access point which has been authorised by the Commission or a Member State and notified to eu-LISA in accordance with Article 6(4) or Article 8(1) and which applies at least one digital procedural standard;
- (4) ‘entity operating an authorised e-CODEX access point’ means a national public authority or legal person authorised under national law or a Union institution, body, office or agency which operates an authorised e-CODEX access point;
- (5) ‘e-CODEX correspondent’ means a natural person, designated by a Member State or the Commission, who can request and receive technical support as referred to in Article 7(1), point (f), from eu-LISA concerning all the components of the e-CODEX system in accordance with Article 7(3);
- (6) ‘connected system’ means an IT system which is connected to an e-CODEX access point for the purpose of exchanging data with other such IT systems;
- (7) ‘central testing platform’ means a component of the e-CODEX system, used exclusively for testing, which provides a set of functions which can be used by entities operating authorised e-CODEX access points to verify whether their authorised e-CODEX access points are correctly operating and whether the digital procedural standards in the connected systems associated with those authorised e-CODEX access points are correctly being used;
- (8) ‘business process model’ means a graphical and textual representation of a conceptual model of several related, structured activities or tasks, along with the relevant data models, and the sequence in which the activities or tasks have to be performed in order to achieve a standardised and meaningful interaction between two or more parties;
- (9) ‘digital procedural standard’ means the technical specifications for business process models and data schemas which set out the electronic structure of the data exchanged through the e-CODEX system based on the EU e-Justice Core Vocabulary.

#### 第 4 条 非差別及び基本的な権利の尊重

##### Article 4 Non-discrimination and respect for fundamental rights

e-CODEX システムを介するデータの電子的な交換によって影響を受ける全ての者の基本的な権利及び自由, とりわけ, 法務への実効的なアクセスの権利, 公正な裁判の権利, 非差別の原則, 個



人データの保護の権利及びプライバシーの権利は、欧州連合法に従って全面的に尊重される。

The fundamental rights and freedoms of all persons affected by the electronic exchange of data through the e-CODEX system, in particular the right to effective access to justice, the right to a fair trial, the principle of non-discrimination, the right to the protection of personal data and the right to privacy, shall be fully respected in accordance with Union law.

## 第 2 章 e-CODEX システムと関係する構成要素, 機能及び職責

### Chapter 2 Composition, Functions and Responsibilities in relation to the e-CODEX system

#### 第 5 条 e-CODEX システムの構成要素

##### Article 5 Composition of the e-CODEX system

1. e-CODEX システムは, 以下によって構成される:
  - (a) e-CODEX アクセスポイント;
  - (b) デジタル手順標準;及び
  - (c) 別紙に列挙する支援ソフトウェア製品, 文書及びそれ以外の資産。

The e-CODEX system shall be composed of:

- (a) an e-CODEX access point;
- (b) digital procedural standards; and
- (c) the supporting software products, documentation and other assets listed in the Annex.

2. e-CODEX アクセスポイントは, 以下によって構成される:
  - (a) 同一の共通プロトコルセットを用いている別のゲートウェイとの間の電気通信ネットワーク上において, 安全な情報の交換をできるようにする, 共通プロトコルセットを基礎とするソフトウェアで構成されるゲートウェイ;
  - (b) 以下のことをできるようにするオープンプロトコルの共通のセットを基礎とするソフトウェアで構成され, 被接続システムを(a)に示すゲートウェイと結びつけ得るようにするコネクタ:
    - (i) メッセージの構造化, 履歴記録及びリンク付け;
    - (ii) メッセージの完全性及び真正性の検証;
    - (iii) 交換されたメッセージの受信の時刻と結びつけられた証拠の生成。

e-CODEX access points shall be composed of:

- (a) a gateway consisting of software, based on a common set of protocols, enabling the secure exchange of information over a telecommunications network with other gateways using the same common set of protocols;
- (b) a connector, making it possible to link connected systems to the gateway referred to in point (a), consisting of software, based on a common set of open protocols, enabling the following:
  - (i) the structuring, logging and linking of messages;
  - (ii) the verification of the integrity and authenticity of messages;
  - (iii) the creation of time-linked evidence of receipt for exchanged messages.

## 第 6 条 欧州委員会の職責

### Article 6 Responsibilities of the Commission

1. 2022 年 12 月 31 日までに、欧州委員会は、実装行為により、以下の事項を定める:
  - (a) 防護に関するもの及び完全性と真正性の検証の手法に関するものを含め、第 5 条に示す e-CODEX システムの構成要素を支えるミニマムの技術仕様と技術標準;
  - (b) 第 7 条に示す eu-LISA によって遂行される活動のためのサービスレベルの要求事項、及び、e-CODEX 連絡担当者の数を含め、当該活動のために必要なその他の技術仕様;
  - (c) 第 10 条に示す移管及び受継の過程のための個別の覚書。

By 31 December 2022, the Commission shall establish, by means of implementing acts:

- (a) the minimum technical specifications and standards, including for security and methods for integrity and authenticity verification, underpinning the components of the e-CODEX system referred to in Article 5;
  - (b) the service level requirements for the activities to be carried out by eu-LISA referred to in Article 7 and other necessary technical specifications for those activities, including the number of e-CODEX correspondents;
  - (c) the specific arrangements for the handover and takeover process referred to in Article 10.
2. 欧州委員会は、民事及び刑事の法務上の協力の領域における欧州連合の別の法行為の中でデジタル手順標準の採択が定められていない限り、実装行為により、デジタル手順標準を採択できる。

The Commission may adopt, by means of implementing acts, digital procedural standards, unless the adoption of digital procedural standards is provided for in other Union legal acts in the area of judicial cooperation in civil and criminal matters.

3. 本条の第 1 項及び第 2 項に示す実装行為は、第 19 条第 2 項に示す審議手続に従って採択される。

The implementing acts referred to in paragraphs 1 and 2 of this Article shall be adopted in accordance with the examination procedure referred to in Article 19(2).

4. 欧州委員会は、欧州連合の機関、組織、事務局及び部局によって運営管理される許可された e-CODEX アクセスポイントのリスト及び当該個々の許可された e-CODEX アクセスポイントが適用しているデジタル手続標準のリストを維持管理する。欧州委員会は、eu-LISA に対し、遅滞なく、当該リスト及び同リストの変更を通知する。

The Commission shall maintain a list of authorised e-CODEX access points which are operated by Union institutions, bodies, offices and agencies and of the digital procedural standards which each of those authorised e-CODEX access points applies. The Commission shall notify that list and any changes

thereto to eu-LISA without delay.

5. 欧州委員会は、欧州委員会が許可した e-CODEX アクセスポイントの数に比例し、かつ、当該許可された e-CODEX アクセスポイントが適用するデジタル手続標準の数に比例する数の e-CODEX 連絡担当者を指定する。当該 e-CODEX 連絡担当者に限り、本条の第 1 項(b)によって採択される実装行為に定める条件の下で、欧州連合の機関、組織、事務局及び部局によって運営管理されている e-CODEX システムと関係する第 7 条第 1 項(f)に示す技術上の支援を要請し、その支援を受ける資格をもつ。欧州委員会は、eu-LISA に対し、欧州委員会が指定した e-CODEX 連絡担当者のリスト及び同リストの変更を通知する。

The Commission shall designate a number of e-CODEX correspondents in proportion to the number of e-CODEX access points which it has authorised and to the number of digital procedural standards which those authorised e-CODEX access points apply. Only those e-CODEX correspondents shall be entitled to request and receive technical support as referred to in Article 7(1), point (f), in relation to the e-CODEX system operated by Union institutions, bodies, offices and agencies, under the terms set out in implementing acts adopted pursuant to paragraph 1, point (b), of this Article. The Commission shall notify a list of the e-CODEX correspondents it has designated and any changes thereto to eu-LISA.

## 第 7 条 eu-LISA の職責

### Article 7 Responsibilities of eu-LISA

1. eu-LISA は、ゲートウェイを除き、第 5 条に示す e-CODEX システムの構成要素に関して職責を負い、とりわけ、以下の職務に関して職責を負う：
  - (a) ソフトウェア製品及びそれ以外の資産を作成すること、維持管理すること、防護に関するものを含め、バグを修正すること及びアップデートすること、並びに、許可された e-CODEX アクセスポイントを運営管理する法主体に対して当該ソフトウェア製品及びそれ以外の資産を配布すること；
  - (b) e-CODEX システムの構成要素、e-CODEX システムの支援ソフトウェア製品及びそれ以外の資産と関連する文書を準備すること、維持管理すること及びアップデートすること、並びに、許可された e-CODEX アクセスポイントを運営管理する法主体に対して当該文書を配布すること；
  - (c) 当該個々の許可された e-CODEX アクセスポイントが適用するデジタル手順標準を含め、許可された e-CODEX アクセスポイントの網羅的なリストを含む設定ファイルを作成すること、維持管理すること及びアップデートすること、並びに、許可された e-CODEX アクセスポイントを運営管理する法主体に対して当該設定ファイルを配布すること；
  - (d) 第 6 条第 2 項に示す実装行為から帰結する技術的な修正及び新機能の追加のような、緊急の要請に対応するため、または e-CODEX 諮問グループから要請された場合における、e-CODEX システムの技術的な修正、及び、新版のソフトウェアとして公表される新機能の追加を行うこと；

- (e) 許可された e-CODEX アクセスポイントを包摂し、接続性を含め、検査活動を支援すること及び調整すること;
- (f) e-CODEX システムとの関係において e-CODEX 連絡担当者に対する技術的な支援を提供すること;
- (g) デジタル手順標準を作成すること、配置すること、維持管理すること及びアップデートすること、並びに、e-CODEX アクセスポイントを運営管理する法主体に対し、当該デジタル手順標準を配布すること;
- (h) eu-LISA に対して通知された許可された e-CODEX アクセスポイントのリスト及び当該個々の許可された e-CODEX アクセスポイントが適用するデジタル手順標準のリストを eu-LISA の Web サイト上で公表すること;
- (i) 第 6 条第 2 項に示す実装行為の準備の過程における欧州委員会の部署からの技術上の助言及び支援を求める要請に対応すること;
- (j) e-CODEX 連絡担当者とのワークショップを開催準備すること及び促進することを含め、新たなデジタル手順標準の必要性を評価すること、新たなデジタル手順標準を評価すること及び準備すること;
- (k) デジタル手順標準が基盤とする EU の e 法務コア語彙を作成すること、維持管理すること及びアップデートすること;
- (l) 第 11 条に定めるセキュリティ運用基準を作成すること及び配布すること;
- (m) オンラインの訓練素材を提供することを含め、規則(EU) 2018/1726 に従った e-CODEX システムの技術上の利用に関し、全ての関連する利害関係者に対するものを含め、訓練を提供すること。

eu-LISA shall be responsible for the components of the e-CODEX system referred to in Article 5, with the exception of the gateway, and, in particular, for the following tasks:

- (a) developing, maintaining, fixing bugs in and updating, including as regards security, software products and other assets and distributing them to the entities operating authorised e-CODEX access points;
- (b) preparing, maintaining and updating the documentation relating to the components of the e-CODEX system, its supporting software products and other assets, and distributing that documentation to the entities operating authorised e-CODEX access points;
- (c) developing, maintaining and updating a configuration file containing an exhaustive list of authorised e-CODEX access points, including the digital procedural standards which each of those authorised e-CODEX access points applies, and distributing it to the entities operating authorised e-CODEX access points;
- (d) making technical changes and adding new features, published as new software versions, to the e-CODEX system in order to respond to emerging requirements, such as those resulting from the implementing acts referred to in Article 6(2), or where requested by the e-CODEX Advisory Group;
- (e) supporting and coordinating testing activities, including connectivity, involving the authorised e-CODEX access points;

- (f) providing technical support for the e-CODEX correspondents in relation to the e-CODEX system;
- (g) developing, deploying, maintaining and updating the digital procedural standards and distributing them to the entities operating authorised e-CODEX access points;
- (h) publishing on its website a list of the authorised e-CODEX access points which have been notified to it and the digital procedural standards which each of those authorised e-CODEX access points applies;
- (i) responding to requests for technical advice and support from the Commission services in the context of the preparation of the implementing acts referred to in Article 6(2);
- (j) evaluating the need for, and assessing and preparing, new digital procedural standards, including by organising and facilitating workshops with the e-CODEX correspondents;
- (k) developing, maintaining and updating the EU e-Justice Core Vocabulary on which the digital procedural standards are based;
- (l) developing and distributing security operating standards, as provided for in Article 11;
- (m) providing training, including to all relevant stakeholders, on the technical use of the e-CODEX system in accordance with Regulation (EU) 2018/1726, including providing online training materials.

2. eu-LISA は、以下の付加的な職務に関して職責を負う:

- (a) eu-LISA の職務を遂行するために必要となる eu-LISA の技術サイト内のハードウェア及びソフトウェア IT インフラを提供すること、運営管理すること及び維持管理すること;
- (b) e-CODEX システムの残りの部分の完全性及び可用性を確保しつつ、中央検査プラットフォームを提供すること、運営管理すること及び維持管理すること;
- (c) Web サイトまたはソーシャルメディアプラットフォームを含め、大規模な通信経路のセットによって、一般公衆に対し、e-CODEX システムに関して情報提供すること;
- (d) e-CODEX システム及び eu-LISA によって遂行される活動と関連する技術的ではない情報を準備すること、アップデートすること及びオンラインで配信すること。

eu-LISA shall be responsible for the following additional tasks:

- (a) providing, operating and maintaining the hardware and software IT infrastructure in its technical sites necessary for carrying out its tasks;
- (b) providing, operating and maintaining a central testing platform, while ensuring the integrity and availability of the rest of the e-CODEX system;
- (c) informing the general public about the e-CODEX system by means of a set of large-scale communication channels, including websites or social media platforms;
- (d) preparing, updating and distributing online non-technical information relating to the e-CODEX system and the activities it carries out.

3. 第 1 項(f)の目的のために、eu-LISA は、業務時間内のオンコールベースで、ゲートウェイに関するものを含め、技術上の支援に関する単一連絡先をもつ e-CODEX 連絡担当者に対して資源を提供できるようにする。

For the purposes of point (f) of paragraph 1, eu-LISA shall make resources available on an on-call basis during business hours to provide e-CODEX correspondents with a single point of contact for technical support, including for the gateway.

## 第 8 条 構成国の職責

### Article 8 Responsibilities of the Member States

1. 構成国は、適用可能な国内法及び欧州連合法に従い、当該構成国内の被接続システムのための e-CODEX アクセスポイントを許可する。構成国は、当該許可された e-CODEX アクセスポイントのリスト及び個々の許可された e-CODEX アクセスポイントが適用するデジタル手順標準のリストを維持管理する。構成国は、eu-LISA に対し、遅滞なく、当該リスト及び同リストの変更を通知する。構成国は、当該構成国の許可された e-CODEX アクセスポイントを監督し、その条件の下で許可が与えられた条件に継続的に適合していることを確保する。構成国は、当該構成国の許可された e-CODEX アクセスポイントを第三国内で運営管理してはならない。

Member States shall authorise e-CODEX access points for the connected systems in their territory in accordance with applicable national and Union law. Member States shall maintain a list of those authorised e-CODEX access points and of the digital procedural standards which each authorised e-CODEX access point applies. Member States shall notify that list and any changes thereto to eu-LISA without delay. Member States shall supervise their authorised e-CODEX access points, ensuring that the conditions under which authorisation was granted are continuously met. Member States shall not operate their authorised e-CODEX access points in third countries.

2. 各構成国は、当該構成国が許可した e-CODEX アクセスポイントの数に比例し、かつ、当該許可された e-CODEX アクセスポイントが適用するデジタル手順標準の数に比例する数の e-CODEX 連絡担当者を指定する。当該 e-CODEX 連絡担当者に限り、第 6 条の第 1 項(b)によって採択される実装行為に定める条件の下で、第 7 条第 1 項(f)に示す技術上の支援を要請し、その支援を受ける資格をもつ。各構成国は、eu-LISA に対し、当該構成国が指定した e-CODEX 連絡担当者のリスト及び同リストの変更を通知する。

Each Member State shall designate a number of e-CODEX correspondents in proportion to the number of e-CODEX access points which it has authorised and to the number of digital procedural standards which those authorised e-CODEX access points apply. Only those e-CODEX correspondents shall be entitled to request and receive technical support as referred to in Article 7(1), point (f), under the terms set out in implementing acts adopted pursuant to Article 6(1), point (b). Each Member State shall notify a list of the e-CODEX correspondents it has designated and any changes thereto to eu-LISA.

## 第 9 条 許可された e-CODEX アクセスポイントを運営管理する法主体の職責

## Article 9 Responsibilities of entities operating authorised e-CODEX access points

1. 許可された e-CODEX アクセスポイントを運営管理する法主体は、当該 e-CODEX アクセスポイントを安全に設置することに関し、及び、当該 e-CODEX アクセスポイントを安全に運営管理することに関して職責を負う。当該職責は、被接続システムとの間で当該 e-CODEX アクセスポイントが互換性をとれるようにするための第 5 条第 2 項(b)に示すコネクタの必要な補正を含める。

An entity operating an authorised e-CODEX access point shall be responsible for setting it up securely and operating it securely. That responsibility shall include the necessary adaptations to the connector referred to in Article 5(2), point (b), to make it compatible with any connected systems.

2. 許可された e-CODEX アクセスポイントを運営管理する法主体は、その e-CODEX アクセスポイントを許可した構成国に対し、第 15 条第 1 項に定める統計データ並びに民事及び刑事の法務上の協力の分野において採択された欧州連合の関連法行為に定める統計データを提供する。

An entity operating an authorised e-CODEX access point shall provide the Member State which has authorised the e-CODEX access point with the statistical data set out in Article 15(1) and in the relevant Union legal acts adopted in the area of judicial cooperation in civil and criminal matters.

3. 許可された e-CODEX アクセスポイント及び被接続システムの運営管理から生ずる損害に関する責任は、適用可能な法律を基礎として、当該許可された e-CODEX アクセスポイントを運営する法主体が負う。

The responsibility for any damage resulting from the operation of an authorised e-CODEX access point and any connected systems shall be borne, on the basis of the applicable law, by the entity operating that authorised e-CODEX access point.

## 第 10 条 移管及び受継

### Article 10 Handover and takeover

1. e-CODEX システムを運営管理する法主体は、2022 年 12 月 31 日までに、eu-LISA に対し、第 6 条第 1 項(c)により採択される実装行為に定めるように、無事な移管過程及び同過程の無事な完了のための基準並びに関連文書を含め、e-CODEX システムの移管のための詳細な手立てを定める共通移管文書を提出する。移管文書は、e-CODEX システムと関連する知的財産権または利用権並びに別紙に列挙する支援ソフトウェア製品、文書及びそれ以外の資産に関する条項も含めるものとし、eu-LISA が、第 7 条に従って eu-LISA の職責を遂行できるようにする。

The entity managing the e-CODEX system shall, by 31 December 2022, submit a common handover document to eu-LISA specifying the detailed arrangements for the transfer of the e-CODEX system,



including the criteria for a successful handover process and for the successful completion of that process and related documentation, as established by the implementing acts adopted pursuant to Article 6(1), point (c). The handover document shall also include provisions on intellectual property rights or usage rights relating to the e-CODEX system and the supporting software products, documentation and other assets listed in the Annex, enabling eu-LISA to carry out its responsibilities in accordance with Article 7.

2. 第 1 項に示す移管文書の提出後の 6 か月の間において、e-CODEX システムを運営管理する法主体と eu-LISA との間で移管及び受継の過程が起きる。移管までの間、e-CODEX システムを運営管理する法主体は、e-CODEX システムに関する全ての職責を保持し、かつ、e-CODEX システムに対するいかなるタイプの修正も行われなければならないこと、及び、e-CODEX システムの保守管理を遂行する目的以外の目的のためにいかなる新たなソフトウェアのリリースも配布されないことを確保する。

Within the six-month period following the delivery of the handover document referred to in paragraph 1, a handover and takeover process shall take place between the entity managing the e-CODEX system and eu-LISA. Until the handover, the entity managing the e-CODEX system shall retain full responsibility for it and shall ensure that no changes to the e-CODEX system are made and that no new software release is delivered other than for the purpose of carrying out corrective maintenance of the e-CODEX system.

3. 欧州委員会は、第 1 項に示す基準を基礎として、e-CODEX システムを運営管理する法主体及び eu-LISA によって e-CODEX システムの移転に関する詳細な手立てが正確に実装されることを確保するため、移管及び受継の過程を監視する。

The Commission shall monitor the handover and takeover process in order to ensure that the detailed arrangements for the transfer of the e-CODEX system are correctly implemented by the entity managing the e-CODEX system and by eu-LISA, on the basis of the criteria referred to in paragraph 1. The Commission shall update the European Parliament and the Council by 31 July 2023 on the handover and takeover process.

4. eu-LISA は、2023 年 7 月 1 日及び 2023 年 12 月 31 日の間において、e-CODEX システムを運営管理する法主体及び eu-LISA の意見聴取を経た上で、移管及び受継の過程が無事に完了したことを欧州委員会が宣言した日に、e-CODEX システムに関する職責を受継する。

eu-LISA shall take over responsibility for the e-CODEX system on the date on which the Commission declares the successful completion of the handover and takeover process, between 1 July 2023 and 31 December 2023, after consulting the entity managing the e-CODEX system and eu-LISA.

## 第 11 条 セキュリティ

### Article 11 Security

1. e-CODEX システムを無事に受継した後、eu-LISA は、第 7 条第 2 項に示すハードウェア及びソフトウェア IT インフラのセキュリティを含め、その職務を遂行する際に高いレベルのセキュリティを維持することに関する職責を負う。とりわけ、eu-LISA は、e-CODEX システムの中で処理される情報の機密性区分及び eu-LISA の情報セキュリティ規則を考慮に入れた上で、e-CODEX 保安計画を策定及び維持すること、そして、同保安計画に従って e-CODEX システムが運営管理されることを確保する。同保安計画は、許可された e-CODEX アクセスポイントを運営管理する法主体が参加する e-CODEX システムのソフトウェアセキュリティ評価を含め、定期的なセキュリティ検査及びセキュリティ監査を定める。

After the successful takeover of the e-CODEX system, eu-LISA shall be responsible for maintaining a high level of security when carrying out its tasks, including the security of the hardware and software IT infrastructure referred to in Article 7(2). In particular, eu-LISA shall establish and maintain an e-CODEX security plan and ensure that the e-CODEX system is operated in accordance with that security plan, taking into account the classification of the information processed in the e-CODEX system and eu-LISA's information security rules. The security plan shall provide for regular security inspections and audits, including software security assessments, of the e-CODEX system with the participation of the entities operating authorised e-CODEX access points.

2. eu-LISA の職責を遂行する際、eu-LISA は、バイデザインのセキュリティの原則並びにバイデザイン及びバイデフォルトのデータ保護の原則を実装する。

When carrying out its responsibilities, eu-LISA shall implement the principles of security by design and data protection by design and by default.

3. 第 6 条第 1 項(a)により採択される実装行為の中で定められる技術上の基準、及び、本条の第 6 項に示すセキュリティ規則及び指針を考慮に入れた上で、許可された e-CODEX アクセスポイントを運営管理する法主体は、当該許可された e-CODEX アクセスポイントを介して送信されるデータの防護に関する職責を含め、当該許可された e-CODEX アクセスポイントを安全に設置することに関し、及び、当該許可された e-CODEX アクセスポイントを安全に運営管理することに関し、独占的な職責をもつ。

Entities operating authorised e-CODEX access points shall have the exclusive responsibility for setting them up securely and operating them securely, including for the security of data transmitted through them, taking into consideration the technical standards set out in the implementing acts adopted pursuant to Article 6(1), point (a), and the security rules and guidance referred to in paragraph 6 of this Article.

4. 許可された e-CODEX アクセスポイントを運営管理する法主体は、eu-LISA に対し、また、国内行

政機関もしくは国内法に基づいて認可された法人によって運営管理される許可された e-CODEX アクセスポイントの場合には、当該許可された e-CODEX アクセスポイントが列挙されているリストを維持管理している構成国に対し、また、欧州連合の機関、組織、事務局または部局によって運営管理される許可された e-CODEX アクセスポイントの場合には、欧州委員会に対し、遅滞なく、セキュリティインシデントを通知する。

Entities operating authorised e-CODEX access points shall notify, without delay, any security incident to eu-LISA and, in the case of authorised e-CODEX access points operated by a national public authority or legal person authorised under national law, to the Member State that maintains the list on which those authorised e-CODEX access points are listed or, in the case of authorised e-CODEX access points operated by a Union institution, body, office or agency, to the Commission.

5. eu-LISA が脆弱性もしくはセキュリティインシデントを検出したときは、または、第 4 項に定めるセキュリティインシデントの通知の受領に応じて、eu-LISA は、そのセキュリティインシデントを分析し、かつ、そのセキュリティインシデントによる影響を受ける許可された e-CODEX アクセスポイントを運営管理する法主体及び e-CODEX 諮問グループに対し、遅滞なく連絡する。

Where eu-LISA detects any vulnerabilities or security incidents or on receipt of a notification of a security incident as provided for in paragraph 4, eu-LISA shall analyse the security incident and inform the entities operating authorised e-CODEX access points impacted by it and the e-CODEX Advisory Group without delay.

6. eu-LISA は、許可された e-CODEX アクセスポイントと関連するセキュリティ規則及び運用指針を策定する。許可された e-CODEX アクセスポイントを運営管理する法主体は、eu-LISA に対し、許可された e-CODEX アクセスポイントと関連するセキュリティ規則を当該許可された e-CODEX アクセスポイントを運営管理する法主体が遵守している旨を言明する宣言書を提供する。同宣言書は、年次で、または、それ以外にも変更を要するときはいつでも、アップデートされる。

eu-LISA shall develop security rules and guidance regarding authorised e-CODEX access points. Entities operating authorised e-CODEX access points shall provide eu-LISA with statements proving their compliance with the security rules regarding authorised e-CODEX access points. Those statements shall be updated on a yearly basis or whenever a change is otherwise required.

## 第 12 条 e-CODEX 諮問グループ

### Article 12 e-CODEX Advisory Group

1. 2023 年 1 月 1 日からのものとして、規則(EU) 2018/1726 の第 27 条第 1 項(dc)によって設けられた e-CODEX 諮問グループは、とりわけ、eu-LISA の年次作業計画及びその年次活動報告書の準備の過程において、eu-LISA に対し、e-CODEX システムと関連する必要な専門知識を提供す

る。e-CODEX 諮問グループは、特定のデジタル手順標準を含め、個別の事項を検討する目的のために、e-CODEX 諮問グループの何名かの構成員によって構成されるサブグループを設け得る。

As from 1 January 2023, the e-CODEX Advisory Group, established pursuant to Article 27(1), point (dc), of Regulation (EU) 2018/1726, shall provide eu-LISA with the necessary expertise related to the e-CODEX system, in particular in the context of the preparation of its annual work programme and its annual activity report. The e-CODEX Advisory Group may set up sub-groups, composed of some of its members, for the purpose of examining specific matters, including specific digital procedural standards.

2. とりわけ、e-CODEX 諮問グループは：
  - (a) 構成国内の e-CODEX システムの実装状態に事後対応し；
  - (b) 新たなデジタル手順標準の必要性を評価し、新たなデジタル手順標準を評価及び準備し；
  - (c) 知識の共有を促進し；
  - (d) 第 6 条第 1 項(b)により採択される実装行為に定めるサービスレベルの要求事項の eu-LISA による遵守を監視し；
  - (e) 第 16 条に示す報告書の草案の版に関する意見を提供する。

The e-CODEX Advisory Group shall, in particular:

- (a) follow up on the state of implementation of the e-CODEX system in the Member States;
  - (b) evaluate the need for, and assess and prepare, new digital procedural standards;
  - (c) promote knowledge sharing;
  - (d) monitor eu-LISA's compliance with the service level requirements set out in the implementing act adopted pursuant to Article 6(1), point (b);
  - (e) provide an opinion on a draft version of the report referred to in Article 16.
3. 第 10 条に示す移管及び受継の期間内、e-CODEX 諮問グループは、移管及び受継の過程が無事に完了するまで、定期的に、かつ、少なくとも各偶数月に、及び、その後は、少なくとも 6 か月毎に会合する。

During the handover and takeover process referred to in Article 10, the e-CODEX Advisory Group shall meet regularly, at least every second month until the handover and takeover process is successfully completed and at least every six months thereafter.

4. e-CODEX 諮問グループは、個々の会合の後、e-CODEX 計画運営会議に対して報告する。e-CODEX 諮問グループは、e-CODEX 計画運営会議の職務を支援するため、技術上の専門知識を提供する。

The e-CODEX Advisory Group shall report after each meeting to the e-CODEX Programme Management Board. The e-CODEX Advisory Group shall provide technical expertise to support the

tasks of the e-CODEX Programme Management Board.

5. e-CODEX 諮問グループは、法務当局の構成員、法律実務家及び職業専門家組織であつて、e-CODEX システムから影響を受ける者、e-CODEX システムを利用する者または e-CODEX システムに参加する者を含め、関連する利害関係者及び専門家を e-CODEX 諮問グループの作業に関与させる。

The e-CODEX Advisory Group shall involve relevant stakeholders and experts in its work, including members of the judiciary, legal practitioners and professional organisations, which are affected by, use, or participate in the e-CODEX system.

### 第 13 条 e-CODEX 計画運営会議

#### Article 13 e-CODEX Programme Management Board

1. 2023 年 1 月 1 日までに、eu-LISA の運営会議は、常置の e-CODEX 計画運営会議を設ける。

By 1 January 2023, eu-LISA's Management Board shall establish a permanent e-CODEX Programme Management Board.

e-CODEX 計画運営会議は:

- (a) eu-LISA の運営会議に対し、とりわけ、第 10 条に示す移管及び受継の期間内、諸活動の優先順序及びそれ以外の戦略上の確約を考慮した上で、e-CODEX システムの長期的な持続性に関して助言し;
- (b) e-CODEX システムの適切な運営管理を確保し;かつ、
- (c) 法務当局の独立の原則の尊重を監視し、かつ、それが必要なときは、予防の活動または是正の活動を促進する。

The e-CODEX Programme Management Board shall:

- (a) advise eu-LISA's Management Board on the long-term sustainability of the e-CODEX system, in particular during the handover and takeover process referred to in Article 10, with regard to the prioritisation of activities, and other strategic commitments;
- (b) ensure the adequate management of the e-CODEX system; and
- (c) monitor respect for the principle of the independence of the judiciary and prompt preventive or corrective action, where necessary.

e-CODEX 計画運営会議は、eu-LISA の運営会議の構成員を代表する任務をもつてはならない。

The e-CODEX Programme Management Board shall not have a mandate to represent the members of eu-LISA's Management Board.

2. e-CODEX 計画運営会議は、以下の 10 名の構成員によって構成される:
  - (a) 第 12 条に示す e-CODEX 諮問グループの議長;
  - (b) eu-LISA の運営会議によって任命された 8 名の構成員;及び
  - (c) 欧州委員会から任命された 1 名の構成員。

The e-CODEX Programme Management Board shall be composed of the following ten members:

- (a) the chairperson of the e-CODEX Advisory Group referred to in Article 12;
- (b) eight members appointed by eu-LISA's Management Board; and
- (c) one member appointed by the Commission.

e-CODEX 計画運営会議の各構成員は、代替要員をもつ。eu-LISA の運営会議は、e-CODEX 計画運営会議が任命した同会議の構成員及び代替要員が、法務の分野を含め、必要な専門知識及び当該構成国の職務の遂行と関連する専門知識をもつことを確保する。

Each member of the e-CODEX Programme Management Board shall have an alternate. eu-LISA's Management Board shall ensure that the members of the e-CODEX Programme Management Board and the alternates which it appoints have the necessary experience, including in the field of justice, and expertise regarding the performance of their tasks.

3. e-CODEX 計画運営会議の構成員及び代替要員の任期は、4 年とし、再任され得る。

The term of office of the members of the e-CODEX Programme Management Board and their alternates shall be four years and shall be renewable.

4. eu-LISA は、e-CODEX 計画運営会議の作業に参加する。その目的のために、eu-LISA の 1 名の代表は、e-CODEX システムと関連する作業に関し、及び、それ以外の関連する作業及び活動に関して報告するため、e-CODEX 計画運営会議の会合に参加する。

eu-LISA shall participate in the work of the e-CODEX Programme Management Board. To that end, one representative of eu-LISA shall attend the meetings of the e-CODEX Programme Management Board in order to report on work regarding the e-CODEX system and on any other related work and activities.

5. e-CODEX 計画運営会議は、少なくとも 6 か月に 1 度会合し、かつ、それが必要なときは、より頻回に会合する。e-CODEX 計画運営会議は、定期的に、かつ、少なくとも各会合の後に、eu-LISA の運営会議に対し、e-CODEX システムの状態及び進捗状況に関する書面の報告書を提出する。

The e-CODEX Programme Management Board shall meet at least once every six months and more often when necessary. The e-CODEX Programme Management Board shall submit written reports regularly, and at least after every meeting, to eu-LISA's Management Board on the status and progress of the e-CODEX system.

6. e-CODEX 計画運営会議は、とりわけ、以下の事項に関する規定を含む e-CODEX 計画運営会議の  
手続規則を策定する:
- (a) 議長及び副議長の選任並びに議長及び副議長の任期;
  - (b) 会合の場所;
  - (c) 会合の準備;
  - (d) 法務当局の構成員、法律実務家及び職業専門家組織であって、e-CODEX システムから影響を受ける者、e-CODEX システムを利用する者または e-CODEX システムに参加する者を含め、利害関係者及び専門家の会合への参加;
  - (e) e-CODEX 計画運営会議の構成員ではない eu-LISA の運営会議の構成員が、e-CODEX 計画運営会議の作業について完全に情報提供を受け続けることを確保する連絡計画。

The e-CODEX Programme Management Board shall establish its rules of procedure, which shall include, in particular, rules on:

- (a) the choice of the chairperson and of the deputy chairperson and their terms of office;
  - (b) meeting venues;
  - (c) the preparation of meetings;
  - (d) the admission of stakeholders and experts to meetings, including members of the judiciary, legal practitioners, and professional organisations which are affected by, use, or participate in the e-CODEX system;
  - (e) communication plans ensuring that members of eu-LISA's Management Board who are not members of the e-CODEX Programme Management Board are kept fully informed of the work of the e-CODEX Programme Management Board.
7. 規則(EU)2018/1726 の第 21 条第 1 項は、e-CODEX 計画運営会議の議長及び副議長に関し、準用して適用される。

Article 21(1) of Regulation (EU) 2018/1726 shall apply mutatis mutandis as regards the chairperson and the deputy chairperson of the e-CODEX Programme Management Board.

8. e-CODEX 計画運営会議の構成員及び同構成員の代替要員にかかる全ての旅費及び滞在費は、合理的かつ比例的なものとし、eu-LISA の手続規則に従い、eu-LISA によって支払われる。

All travel and subsistence expenses incurred by the members of the e-CODEX Programme Management Board and their alternates shall be reasonable and proportionate and be paid by eu-LISA in accordance with its rules of procedure.

9. eu-LISA は、e-CODEX 計画運営会議に対し、事務局を提供する。

eu-LISA shall provide the secretariat for the e-CODEX Programme Management Board.

## 第 14 条 法務当局の独立性

### Article 14 Independence of the judiciary

1. この規則の下にある法主体の職責を遂行する際、全ての法主体は、権力分立の原則を考慮に入れた上で、法務当局の独立性の原則を尊重する。

When carrying out their responsibilities under this Regulation, all entities shall respect the principle of the independence of the judiciary, having regard to the principle of separation of powers.

2. その目的のために、第 12 条及び第 13 条により、eu-LISA は、e-CODEX システムに関して eu-LISA に対して提供された資源を、その全体において、この規則の下にある e-CODEX システムの運営管理のために充てるものとし、かつ、e-CODEX システムの運営管理への法務当局の代表の関与を確保する。

For that purpose, eu-LISA shall commit the resources provided to it for the e-CODEX system in their entirety to its operation under this Regulation and shall ensure the involvement of justice representatives in the management of the e-CODEX system, pursuant to Articles 12 and 13.

## 第 15 条 通知

### Article 15 Notifications

1. e-CODEX システムの職責を eu-LISA が無事に受継した後の毎年 1 月 31 日までに、構成国は、eu-LISA に対し、以下の統計データを通知する：
  - (a) 欧州連合の別の法行為に基づき均等な通知手続が適用されない限り、対応する許可された e-CODEX アクセスポイント及びデジタル手順標準毎に仕分けられた、当該構成国の領土内の被接続システムのための許可された e-CODEX アクセスポイントを介して送受信された技術メッセージの数；
  - (b) 欧州連合の別の法行為に基づき均等な通知手続が適用されない限り、当該構成国の領土内の被接続システムのための許可された e-CODEX アクセスポイントを運営管理する法主体によって対処されたインシデントであって、e-CODEX システムのセキュリティに対して影響を与えたものの数及びタイプ。

By 31 January of every year after eu-LISA successfully takes over responsibility for the e-CODEX system, Member States shall notify eu-LISA of the following statistical data:

- (a) the number of technical messages sent and received through each authorised e-CODEX access point for the connected systems within their territory, grouped by corresponding authorised e-CODEX access point and digital procedural standard, unless an equivalent notification procedure applies under another Union legal act;
- (b) the number and type of incidents encountered by entities operating authorised e-CODEX access



points for the connected systems within their territory which have impacted the security of the e-CODEX system, unless an equivalent notification procedure applies under another Union legal act.

2. e-CODEX システムの職責を eu-LISA が無事に受継した後の毎年 1 月 31 日までに、欧州委員会は、eu-LISA に対し、以下の統計データを通知する:
  - (a) 欧州連合の別の法行為に基づき均等な通知手続が適用されない限り、対応する許可された e-CODEX アクセスポイント及びデジタル手順標準毎に仕分けられた、欧州連合の機関、組織、事務局または部局によって運営管理されている個々の許可された e-CODEX アクセスポイントを介して送受信された技術メッセージの数;
  - (b) 欧州連合の別の法行為に基づき均等な通知手続が適用されない限り、当該法主体が欧州連合の機関、組織、事務局及び部局である場合、個々の許可された e-CODEX アクセスポイントを運営管理する法主体によって対処されたインシデントであって、e-CODEX システムのセキュリティに対して影響を与えたものの数及びタイプ。

By 31 January of every year after eu-LISA successfully takes over responsibility for the e-CODEX system, the Commission shall notify eu-LISA of the following statistical data:

- (a) the number of technical messages sent and received through each authorised e-CODEX access point operated by a Union institution, body, office or agency, grouped by corresponding authorised e-CODEX access point and digital procedural standard, unless an equivalent notification procedure applies under another Union legal act;
  - (b) the number and type of incidents encountered by entities operating authorised e-CODEX access points, where those entities are Union institutions, bodies, offices and agencies, which have impacted the security of the e-CODEX system, unless an equivalent notification procedure applies under another Union legal act.
3. 本条の第 1 項及び第 2 項に基づく通知は、第 6 条第 4 項及び第 8 条第 1 項に示す許可された e-CODEX アクセスポイントのリスト及びデジタル手順標準のリストがアップデートされているかどうかを確認する。

Notifications under paragraphs 1 and 2 of this Article shall confirm whether the lists of authorised e-CODEX access points and digital procedural standards referred to in Article 6(4) and Article 8(1) are up to date.

## 第 16 条 監視及び報告

### Article 16 Monitoring and reporting

1. e-CODEX システムの職責を eu-LISA が受継した 2 年後に、かつ、その後は 2 年毎に、eu-LISA は、欧州委員会に対し、e-CODEX システムのセキュリティを含め、e-CODEX システムの技術上の稼働状況及び利用に関する報告書を提出する。

Two years after it takes over responsibility for the e-CODEX system, and every two years thereafter, eu-LISA shall submit a report to the Commission on the technical functioning and use of the e-CODEX system, including the security of the e-CODEX system.

2. eu-LISA は、第 6 条第 4 項、第 8 条第 1 項及び第 15 条により欧州委員会及び構成国から受領したデータを統合し、かつ、本条の第 1 項に定める報告書の一部として以下の指標を提供する:
  - (a) 報告期間内に e-CODEX システムが利用されたデジタル手順標準のリスト及び数;
  - (b) 個々の構成国毎及び個々のデジタル手順標準毎の許可された e-CODEX アクセスポイントの数;
  - (c) 個々の許可された e-CODEX アクセスポイント間における個々のデジタル手順標準毎の e-CODEX システムを介して送信された技術メッセージの数;
  - (d) e-CODEX システムのセキュリティに影響を与えるインシデントの数及びタイプ並びに e-CODEX 保安計画の遵守に関する情報。

eu-LISA shall consolidate the data received from the Commission and the Member States pursuant to Article 6(4), Article 8(1) and Article 15 and provide the following indicators as part of the report provided for in paragraph 1 of this Article:

- (a) the list and number of digital procedural standards for which the e-CODEX system has been used during the reporting period;
  - (b) the number of authorised e-CODEX access points for each Member State and for each digital procedural standard;
  - (c) the number of technical messages sent through the e-CODEX system for each digital procedural standard between each of the authorised e-CODEX access points;
  - (d) the number and type of incidents impacting the security of the e-CODEX system and information on compliance with the e-CODEX security plan.
3. e-CODEX システムの職責を eu-LISA が受継した 3 年後に、かつ、その後は 4 年毎に、欧州委員会は、e-CODEX システムの全体評価書を作成する。同全体評価書は、この規則の適用の評価、求められた目的に対して達成された結果の検討を含めるものとし、かつ、将来のあり得る活動を提案し得る。その評価書を作成する際、欧州委員会は、客観的な根拠を基礎として、e-CODEX 計画運営会議の役割及びその継続も再検討し、また、その必要があるときは、改善策を提案する。欧州委員会は、欧州議会及び理事会に対し、その全体評価書を送付する。

Three years after eu-LISA takes over responsibility for the e-CODEX system, and every four years thereafter, the Commission shall produce an overall evaluation of the e-CODEX system. That overall evaluation shall include an assessment of the application of this Regulation and an examination of results achieved against objectives pursued and may propose possible future actions. When producing its evaluations, the Commission shall also re-examine the role of the e-CODEX Programme Management Board and its continuation based on objective grounds and, if necessary, shall propose improvements. The Commission shall transmit the overall evaluation to the European Parliament and to the Council.

## 第 17 条 国際機関との協力

### Article 17 Cooperation with international organisations

1. eu-LISA は、国際公法によって規律される国際機関もしくは同機関の下部組織との間で、または、それ以外の関連法主体もしくは組織であって、複数の国家間の協定によって設置され、もしくは、複数の国家間の協定を基礎として設置されたものとの間で、当該機関、下部組織、それ以外の関連法主体または組織が、e-CODEX を利用する際に技術上の支援を要請し、それを受けることができるようにするため、作業覚書を締結できる。当該作業覚書は、規則(EU) 2018/1726 の第 43 条に従って締結される。

eu-LISA may conclude working arrangements with international organisations or their subordinate bodies, governed by public international law, or other relevant entities or bodies, which are set up by, or on the basis of, an agreement between two or more countries, in order to allow them to request and receive technical support when using the e-CODEX system. Those working arrangements shall be concluded in accordance with Article 43 of Regulation (EU) 2018/1726.

2. 本条の第 1 項に示す作業覚書は、そのような技術上の支援が第 20 条第 1 項に示す費用に影響を与えないことを条件として、第 6 条第 1 項 1(b)により採択された実装行為に定める条件の下で、第 7 条第 1 項(f)に示す技術上の支援を要請し、それを受ける資格のある連絡担当者として労務提供するための、国際機関、組織または法主体毎に 1 名の自然人の指定を認めることができる。

The working arrangements referred to in paragraph 1 of this Article may allow for the designation of one natural person per international organisation, body or entity to serve as a correspondent who shall be entitled to request and receive technical support as referred to in Article 7(1), point (f), under the terms set out in the implementing acts adopted pursuant to Article 6(1), point (b), provided that such technical support does not affect the costs referred to in Article 20(1).

### 第 3 章 改正条項

#### Chapter 3 Amending Provisions

#### 第 18 条 規則 2018/1726 の改正

##### Article 18 Amendments to Regulation (EU) 2018/1726

規則(EU) 2018/1726 は、以下のとおり改正される:

Regulation (EU) 2018/1726 is amended as follows:

(1) 第 1 条は、以下のとおり改正される:

(a) 以下の項が挿入される:

「4a. 局は、技術上の改良を含め、民事及び刑事の法務上の協力の分野におけるデータの国境を越える電子的な交換のためのコンピュータ化されたシステム(e-CODEX システム)の開発及び業務運営管理に関する職責を負う。」;

(b) 第 5 項は、以下の文によって置き換えられる:

「5. 局は、それが適切なときは、この規則の第 14 条に示す調査研究における発展、並びに、この規則の第 15 条に示す実験プロジェクト及び概念実証の結果を考慮に入れた上で、TFEU の第 67 条ないし第 89 条を基礎として、当該システムを規律する欧州連合の関連する法行為によってそのように定められている場合に限り、既存のシステムを含め、本条の第 3 項、第 4 項及び第 4 項 a に示すシステム以外の、自由、保安及び法務の領域における大規模 IT システムの準備、開発または業務運営管理に関して職責を負わせ得る。」;

Article 1 is amended as follows:

(a) the following paragraph is inserted:

‘4a. The Agency shall be responsible for the development and operational management, including technical evolutions, of the computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (the “e-CODEX system”).’;

(b) paragraph 5 is replaced by the following:

‘5. The Agency may be made responsible for the preparation, development or operational management of large-scale IT systems in the area of freedom, security and justice other than those referred to in paragraphs 3, 4 and 4a of this Article, including existing systems, only if so provided by relevant Union legal acts governing those systems, based on Articles 67 to 89 TFEU, taking into account, where appropriate, the developments in research referred to in Article 14 of this Regulation and the results of pilot projects and proofs of concept referred to in Article 15 of this Regulation.’;

(2) 以下の条が挿入される:

**「第 8 条 b e-CODEX システムと関連する職務**

e-CODEX システムとの関係において、局は、以下の職務を遂行する:

- (a) 欧州議会及び理事会の規則(EU) (EU) 2022/850 によって局に与えられた職務<sup>(\*)</sup>;
- (b) オンラインの訓練素材の提供を含め、e-CODEX システムの技術上の利用に関する訓練と関連する職務。

<sup>(\*)</sup> 民事及び刑事の法務上の協力の分野におけるデータの国境を越える電子的な交換のためのコンピュータ化されたシステム (e-CODEX システム) に関する並びに規則(EU) 2018/1726 を改正する欧州議会及び理事会の 2022 年 5 月 30 日の規則(EU) 2022/850 (OJ L 150, 31.5.2022, p. 1).」;

the following article is inserted:

‘ Article 8b Tasks related to the e-CODEX system

In relation to the e-CODEX system, the Agency shall perform:

- (a) the tasks conferred on it by Regulation (EU) 2022/850 of the European Parliament and of the Council<sup>(\*)</sup>;
- (b) tasks relating to training on the technical use of the e-CODEX system, including provision of online training materials.

<sup>(\*)</sup> Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (OJ L 150, 31.5.2022, p. 1).’;

(3) 第 14 条において、第 1 項は、以下の文によって置き換えられる:

「1. 局は、SIS II, VIS, Eurodac, EES, ETIAS, DubliNet, ECRIS-TCN, e-CODEX システム及び第 1 条第 5 項に示す他の大規模 IT システムの業務運営管理と関連する調査研究における発展を監視する。」;

in Article 14, paragraph 1 is replaced by the following:

‘ 1. The Agency shall monitor developments in research relevant for the operational management of SIS II, VIS, Eurodac, the EES, ETIAS, DubliNet, ECRIS-TCN, the e-CODEX system and other large-scale IT systems as referred to in Article 1(5).’;

- (4) 第 17 条第 3 項において、第 2 副項の後に以下の副項が挿入される:

「第 1 条(4a)及び第 8 条 b に示す e-CODEX システムの開発及び業務運営管理と関連する職務は、エストニアのタリンにおいて遂行される。」;

in Article 17, paragraph 3, the following subparagraph is inserted after the second subparagraph:

‘The tasks relating to the development and operational management of the e-CODEX system referred to in Article 1(4a) and Article 8b shall be carried out in Tallinn, Estonia.’;

- (5) 第 19 条第 1 項は、以下のとおり改正される:

- (a) (ff)は、以下の文によって置き換えられる:

「(ff) 以下のシステムの技術上の稼働状況に関する報告書を採択すること:

- (i) 欧州議会及び理事会の規則(EU) 2018/1861<sup>(\*)</sup>の第 60 条第 7 項並びに欧州議会及び理事会の規則 2018/1862<sup>(\*\*)</sup>の第 74 条第 8 項による SIS;
- (ii) 規則(EC) No 767/2008 の第 50 条第 3 項及び決定 2008/633/JHA の第 17 条第 3 項による VIS;
- (iii) 規則(EU) 2017/2226 の第 72 条第 4 項による EES;
- (iv) 規則(EU) 2018/1240 の第 92 条第 4 項による ETIAS;
- (v) 規則(EU) 2019/816 の第 36 条第 8 項による ECRIS-TCN 及び ECRIS の参考実装;
- (vi) 規則(EU) 2019/817 の第 78 条第 3 項及び規則(EU) 2019/818 の第 74 条第 3 項による相互運用性コンポーネント;
- (vii) 規則 2022/850 の第 16 条第 1 項による e-CODEX システム;

<sup>(\*)</sup> 国境検問の分野におけるシェンゲン情報システム(SIS)の設置、運用及び利用に関する、並びに、シェンゲン協定実装条約を改正し、規則(EC) No 1987/2006 を改正する欧州議会及び理事会の 2018 年 11 月 28 日の規則(EU) 2018/1861 (OJ L 312, 7.12.2018, p. 14).

<sup>(\*\*)</sup> 刑事における警察協力及び法務上の協力の分野におけるシェンゲン情報システム(SIS)の設置、運用及び利用に関する、並びに、理事会決定 2007/533/JHA を改正及び廃止し、欧州議会及び理事会の規則(EC) No 1986/2006 及び委員会決定 2010/261/EU を廃止する欧州議会及び理事会の 2018 年 11 月 28 日の規則(EU) 2018/1862 (OJ L 312, 7.12.2018, p. 56).;

- (b) (mm)は、以下の文によって置き換えられる:

「(mm) 以下の情報の年次の公表を確保すること:

- (i) 規則(EU) 2018/1861 の第 7 条第 3 項及び規則(EU) 2018/1862 の第 7 条第 3 項それぞれによる SIS の国内システム(N.SIS)の事務局及び SIRENE 事務局のリストと共に、規則(EU) 2018/1861 の第 41 条第 8 項及び規則(EU) 2018/1862 の第 56 条第 7 項による SIS に含まれているデータの直接の検索を許可された職務権限のある機関のリスト;
- (ii) 規則(EU) 2017/2226 の第 65 条第 2 項による職務権限のある機関のリスト;
- (iii) 規則(EU) 2018/1240 の第 87 条第 2 項による職務権限のある機関のリスト;
- (iv) 規則(EU) 2019/816 の第 34 条第 2 項による中央当局のリスト;
- (v) 規則(EU) 2019/817 の第 71 条第 1 項及び規則(EU) 2019/818 の第 67 条第 1 項による機関のリスト;
- (vi) 規則(EU) 2022/850 の第 7 条第 1 項の(h)による許可された e-CODEX アクセスポイントのリスト;」;

in Article 19, paragraph 1 is amended as follows:

(a) point (ff) is replaced by the following:

“(ff) adopt reports on the technical functioning of the following:

- (i) SIS pursuant to Article 60(7) of Regulation (EU) 2018/1861 of the European Parliament and of the Council<sup>(\*)2</sup> and Article 74(8) of Regulation (EU) 2018/1862 of the European Parliament and of the Council<sup>(\*)3</sup>;
- (ii) VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA;
- (iii) EES pursuant to Article 72(4) of Regulation (EU) 2017/2226;
- (iv) ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240;
- (v) ECRIS-TCN and the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816;
- (vi) the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817 and Article 74(3) of Regulation (EU) 2019/818;
- (vii) the e-CODEX system pursuant to Article 16(1) of Regulation (EU) 2022/850;

<sup>(\*)2</sup> Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).”

<sup>(\*)3</sup> Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing

Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).';"

(b) point (mm) is replaced by the following:

'(mm) ensure annual publication of the following:

- (i) the list of competent authorities authorised to search directly the data contained in SIS pursuant to Article 41(8) of Regulation (EU) 2018/1861 and Article 56(7) of Regulation (EU) 2018/1862, together with the list of Offices of the national systems of SIS (N.SIS) and SIRENE Bureaux pursuant to Article 7(3) of Regulation (EU) 2018/1861 and Article 7(3) of Regulation (EU) 2018/1862, respectively;
- (ii) the list of competent authorities pursuant to Article 65(2) of Regulation (EU) 2017/2226;
- (iii) the list of competent authorities pursuant to Article 87(2) of Regulation (EU) 2018/1240;
- (iv) the list of central authorities pursuant to Article 34(2) of Regulation (EU) 2019/816;
- (v) the list of authorities pursuant to Article 71(1) of Regulation (EU) 2019/817 and Article 67(1) of Regulation (EU) 2019/818;
- (vi) the list of authorised e-CODEX access points pursuant to Article 7(1), point (h), of Regulation (EU) 2022/850 ;';

(6) 第 27 条第 1 項において、以下の号が挿入される:

「(dc) e-CODEX 諮問グループ;」。

in Article 27(1), the following point is inserted:

'(dc) e-CODEX Advisory Group;'



## 第 4 章 最終規定

### Chapter 4 Final Provisions

#### 第 19 条 委員会の手続

##### Article 19 Committee procedure

1. 欧州委員会は、委員会による補佐を受ける。同委員会は、規則(EU) No 182/2011 の意味における委員会である。

The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. 本項に対する参照が行われるときは、規則(EU) No 182/2011 の第 5 条が適用される。

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

#### 第 20 条 費用

##### Article 20 Costs

1. 第 7 条に示す職務の遂行にかかる費用は、欧州連合の一般予算の負担とする。

The costs incurred in the performance of the tasks referred to in Article 7 shall be borne by the general budget of the Union.

2. 第 8 条及び第 9 条に示す職務のための費用は、構成国または許可された e-CODEX アクセスポイントを運営管理する法主体の負担とする。

The costs for the tasks referred to in Articles 8 and 9 shall be borne by the Member States or the entities operating authorised e-CODEX access points.

#### 第 21 条 発効

##### Article 21 Entry into force

この規則は、EU 官報上のその公示の 20 日後に発効する。

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

この規則は、その全部について拘束力を持ち、諸条約に従い構成国において直接に適用される。

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

ブリュッセルにおいて、2022 年 5 月 30 日に行われた。

Done at Brussels, 30 May 2022.

欧州議会として  
For the European Parliament

議長 R. METSOLA  
The President R. METSOLA

理事会として  
For the Council

議長 B. LE MAIRE  
The President B. LE MAIRE

## 別紙

第 10 条の下で eu-LISA に対して移管されるソフトウェア製品、文書及びそれ以外の資産  
Software Products, Documentation and other Assets to be Handled Over to eu-LISA under Article 10

- (1) 中央検査プラットフォーム;
- (2) 第 7 条第 1 項(c)に示す職務の遂行において補助するために使用されるソフトウェア製品である設定管理ツール;
- (3) 第 7 条に示す職務の一部の遂行において補助するために使用されるソフトウェア製品であるメタデータワークベンチ;
- (4) 長期間にわたり利用案件を横断して、データの一貫性及びデータの品質を確保するために使用される、二次利用可能な意味論上の用語及び定義のための資産である EU の e 法務コア語彙;
- (5) e-CODEX システムのそれ以外の資産が遵守しなければならない技術標準の選択に関し、関連する利害関係者に対して技術上の有益な知識を提供するために使用される文書であるアーキテクチャ文書。

- (1) The central testing platform;
- (2) The Configuration Management Tool, which is a software product used to assist in the performance of the task referred to in Article 7(1), point (c);
- (3) Metadata Workbench, which is a software product used to assist in the performance of parts of the tasks referred to in Article 7;
- (4) The EU e-Justice Core Vocabulary, which is an asset for reusable semantical terms and definitions used to ensure data consistency and data quality over time and across use cases;
- (5) Architecture documentation, which is documentation used to provide technical and informative knowledge to relevant stakeholders on the choice of standards with which other assets of the e-CODEX system must comply.

## 委員会決定(EU) 2023/2099

### [参考訳]

2023 年 12 月 29 日  
明治大学法学部教授  
夏井 高人

COMMISSION DECISION (EU) 2023/2099 of 28 September 2023 confirming the participation of Ireland in Regulation (EU) 2022/850 of the European Parliament and of the Council on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system) (OJ L 241, 29.9.2023, p. 144-144) のテキスト (英語版) に基づいて和訳を試みた。

原文のテキストを入手できるサイトの URL は、下記のとおりである。

<http://data.europa.eu/eli/dec/2023/2099/oj>  
[2023 年 12 月 6 日確認]

この委員会決定(EU) 2023/2099 の参考訳は、あくまでも原文を読む際の参考として提供しているものであり、個人的な見解としての法解釈の結果を「日本語以外の言語で書かれた文書の日本語による翻訳文」というスタイルを用いて表現した文書の一種である。

### — 解 説 —

#### 1. 委員会決定(EU) 2023/2099 について

規則(EU) 2022/850 (OJ L 150, 1.6.2022, p. 1-19) の前文(49)では、アイルランドが同規則の採択手続に参加せず、それゆえに同規則がアイルランドを拘束することはない旨が述べられているけれども、その後、アイルランドから欧州委員会に対する通知によってアイルランドが同規則を受諾し、同規則によって拘束される意思をもつことが確認された。

委員会決定(EU) 2023/2099 は、このような経緯で規則(EU) 2022/850 に参加する意思を明確にしたアイルランドに対して規則(EU) 2022/850 が適用されるようにするために必要な措置として、欧州委員会によって採択された決定である。

#### 2. 参考訳作成における基本方針

この参考訳においては、委員会決定(EU) 2023/2099 の前文(recital)及び条文(articles)の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし、原文を表示することが無意味な部分(特に脚注内)に関しては、原文または訳文の表示を省略した。

この参考訳は、あくまでも委員会決定(EU) 2023/2099 の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は、現時点における研究成果を反映するものである。将来、更に研究を深めた結果として修正すべき部分を発見したときは、その時点において、改訂版等を作成すべきかどうかを検討する。

参考訳の訳出に際しては原則として直訳とすることとしたが、直訳のままでは日本語になりにくい箇所に関しては、やむを得ず意訳とした。

この参考訳に訳注はない。参考訳中にある脚注は、全て原注である。

この参考訳は、Eur-lex のデータ二次利用条件を遵守して作成した。

### 3. 関連参考訳

e-CODEX 規則(EU) 2022/850 の参考訳は、法と情報雑誌 9 巻 1 号 1～57 頁にある。

eu-LISA 規則(EU) 2018/1726 の参考訳は、法と情報雑誌 4 巻 3 号 138～188 頁にある。

この参考訳の校正等に関し、唐亀侑久氏(株式会社ラック)の助力を得た。

\*\*\*

**民事及び刑事における法務上の協力の分野におけるデータの国境を越える  
電子的な交換のためのコンピュータ化されたシステム(e-CODEX システム)に関する  
欧州議会及び理事会の規則(EU) 2022/850 へのアイルランドの参加を確認する  
2023 年 9 月 28 日の委員会決定(EU) 2023/2099**

Commission Decision (EU) 2023/2099 of 28 September 2023 confirming the participation of Ireland  
in Regulation (EU) 2022/850 of the European Parliament and of the Council  
on a computerised system for the cross-border electronic exchange of data  
in the area of judicial cooperation in civil and criminal matters (e-CODEX system)

(EEA に適用される正文)

(Text with EEA relevance)

欧州委員会は、

欧州連合条約及び欧州連合の機能に関する条約に附属する自由、保安及び法務の領域に関する英国及びアイルランドの地位に関する議定書(第 21 号)、及び、とりわけ、その第 4 条に鑑み、  
アイルランドからの、民事及び刑事における法務上の協力の分野におけるデータの国境を越える電子的な交換のためのコンピュータ化されたシステム(e-CODEX システム)に関する並びに規則(EU) 2018/1726を改正する 2022 年 5 月 30 日の欧州議会及び理事会の規則(EU) 2022/850<sup>1</sup>を受諾し、かつ、同規則によって拘束されることのアイルランドの意思の通知に鑑み、

THE EUROPEAN COMMISSION,

Having regard to Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and in particular Article 4 thereof,

Having regard to the notification by Ireland of its wish to accept and be bound by Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726<sup>(1)</sup>,

Whereas:

- (1) 2023 年 6 月 28 日の欧州委員会宛書簡により、アイルランドは、議定書(第 21 号)の第 4 条に従い、規則(EU) 2022/850 を受諾し、かつ、同規則によって拘束されることのアイルランドの意思を通知した。

---

<sup>1</sup> OJ L 150, 1.6.2022, p. 1.

By letter to the Commission of 28 June 2023, Ireland notified its wish, in accordance with Article 4 of Protocol (No 21), to accept and be bound by Regulation (EU) 2022/850.

- (2) 規則(EU) 2022/850 へのアイルランドの参加には何らの条件も付されておらず、かつ、移行措置の必要性も存在しない。

There are no conditions attached to the participation of Ireland in Regulation (EU) 2022/850 and there is no need for transitional measures.

- (3) それゆえ、規則(EU) 2022/850 へのアイルランドの参加が確認されるべきである。

The participation of Ireland in Regulation (EU) 2022/850 should therefore be confirmed.

- (4) 可能な限り速やかに規則(EU) 2022/850 をアイルランドに適用できるようにするため、この決定は、その公示の翌日に発効すべきである、

In order to allow Ireland to apply Regulation (EU) 2022/850 as soon as possible, this Decision should enter into force on the day following that of its publication,

HAS ADOPTED THIS DECISION:

以上のとおりであるので、この決定を採択する:

## 第 1 条

### Article 1

規則(EU) 2022/850 へのアイルランドの参加が確認される。

The participation of Ireland in Regulation (EU) 2022/850 is confirmed.

## 第 2 条

### Article 2

この決定は、EU 官報上のその公示の翌日に発効する。

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

ブリュッセルにおいて、2023 年 9 月 28 日に行われた。

Done at Brussels, 28 September 2023.

欧州委員会として  
For the Commission

議長 Ursula VON DER LEYEN  
The President Ursula VON DER LEYEN



## 指令(EU) 2023/977

### 〔参考訳〕

2023 年 12 月 26 日  
明治大学法学部教授  
夏井 高人

DIRECTIVE (EU) 2023/977 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA (OJ L 134, 22.5.2023, p. 1-24)のテキスト(英語版)に基づいて和訳を試みた。

原文のテキストを入手できるサイトの URL は、下記のとおりである。

<http://data.europa.eu/eli/dir/2023/977/oj>  
[2023 年 12 月 6 日確認]

この指令(EU) 2023/977 の参考訳は、あくまでも原文を読む際の参考として提供しているものであり、個人的な見解としての法解釈の結果を「日本語以外の言語で書かれた文書の日本語による翻訳文」というスタイルを用いて表現した文書の一種である。

### — 解 説 —

指令(EU) 2023/977 は、指令(EU) 2023/977 は、EU のセキュリティユニオン戦略(EU Security Union Strategy)の中に位置づけられている組織犯罪対策立法の一部として、「スウェーデン枠組み決定 (Swedish Framework Decision)」とのニックネームで知られている理事会枠組み決定 2006/960/JHA (OJ L 386, 29.12.2006, p. 89-100)を廃止し、同枠組み決定と置き換わる法令である。

指令(EU) 2023/977 は、2023 年 5 月 10 日に採択された。

指令(EU) 2023/977 は、2023 年 6 月 11 日に発効した。

指令(EU) 2023/977 の条項に定められている規範内容を構成国の国内法として移植して実装する国内法化の期限は、第 13 条を除き、2024 年 12 月 11 日である。

指令(EU) 2023/977 の第 13 条の国内法化の期限は 2027 年 6 月 11 日である。

理事会枠組み決定 2006/960/JHA は、2024 年 12 月 11 日の経過をもって廃止される(第 21 条参照)

シェンゲン協定実装条約(the Convention implementing the Schengen Agreement)の第 39 条及び第 46 条の中で指令(EU) 2023/977 と関連する部分は、2024 年 12 月 11 日の経過をもって、指令(EU) 2023/977 の関連条項によって置き換えられる。

## 1. 指令(EU) 2023/977 について

### 1.1 立法の経緯

指令(EU) 2023/977 の立法の経緯に関しては、その立法提案(COM(2021) 782 final, 2021/0411 (COD))の中で詳細に述べられている。

理事会枠組み決定 2006/960/JHA は、法執行機関の間における情報交換と情報共有について定めておりながら、そのための共通の手順や方法等が明確ではなく、あまり利用されなかったらしい。このことは、指令(EU) 2023/977 の前文中でも言及されていることであるが、立法提案(COM(2021) 782 final, 2021/0411 (COD))の中では、より詳細にそのことが説明されている。

指令(EU) 2023/977 においては、構成国の法執行機関の間における情報の交換のための具体的な方法として、Europol の SIENA (Secure Information Exchange Network Application)を使用することとされている(第 13 条参照)。

ただし、幾つかの例外が認められており、それに該当するときは、SIENA 以外の通信経路も利用できる(前文(26)参照)。

指令(EU) 2023/977 が定めるとおり、現実には、SIENA を用いた通信が原則としての通信経路となるかどうかは、今後の運用状況を見ないと何とも言えない。

### 1.2 適用範囲

指令(EU) 2023/977 は、EU の構成国の法執行機関とシェンゲン協定に加盟している国の法執行機関に適用される法令である。それゆえ、指令(EU) 2023/977 は、それらの国以外の第三国との間の情報交換には適用されない。第三国との間における捜査関係情報の送付に関しては、別の法令が適用される(前文(10)参照)。

ただし、国際機関である Interpol との関係は別であり、Interpol の国内拠点、各構成国の単一連絡部局の構成員となるので、そのことを通じて、構成国間の情報交換に関与し得ることになる(第 15 条第 2 項参照)。

なお、ここでいう「第三国」とは、EU の構成国及びシェンゲン協定の加盟国を除く国という意味をもち、シェンゲン協定とは関係をもたない EU 法における「第三国」の用例とは異なっていることに留意すべきである。

指令(EU) 2023/977 において第三国が関係するのは、ある構成国(A 国)から別の構成国(B 国)に

対して送付される情報が、最初は第三国(X 国)から入手された情報である場合、A 国から B 国への情報の送付の前に、当該送付に関して X 国から当該 A 国から B 国への送付について同意を得ることが要件とされているという点に関してのみである(第 3 条(d), 前文(15)参照)。

EU 域内において、構成国から Europol に対して情報が送付される場合も同じである(第 12 条第 2 項参照)。

当該第三国から同意が得られなかった場合、当該情報を求める要請は、当該第三国の同意が得られないことを理由に拒否される(第 6 条第 1 項(h))。

### 1. 3 指令(EU) 2023/977 の採択後に採択された法令の特定

指令(EU) 2023/977 の前文(14)の中にある「刑事手続における電子証拠のための及び刑事手続後の拘禁刑の執行のための欧州提出命令及び保全命令に関する欧州議会及び理事会の規則(Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings)」とは、規則(EU) 2023/1543(OJ L 191, 28.7.2023, p. 118–180)のことを指す。

指令(EU) 2023/977 の前文(14)の中にある「刑事手続における電子証拠の収集の目的のための指定された拠点の指定及び法律上の代理者の指名に関する整合化された規定を定める欧州議会及び理事会の指令(Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings)」とは、指令(EU) 2023/1544(OJ L 191, 28.7.2023, p. 181–190)のことを指す。

### 1. 4 指令(EU) 2023/977 の原文中にある誤記等の問題

指令(EU) 2023/977 の原文(英語版)には明らかな誤りが見られる。

それらが訂正されるべき誤記等に該当すると欧州委員会が判断する場合、所定の手続を経て EU 官報上で公表されるその正誤表(corrigendum)によっていずれ訂正されることになる予想されるが、Eur-lex 上で 2023 年 12 月 13 日の時点において確認できた範囲内では、指令(EU) 2023/977 の原文(英語版)に適用される正誤表は公表されていない。

## 2. 参考訳作成における基本方針

この参考訳においては、指令(EU) 2023/977 の前文(recital)、条文(articles)及び別紙(Annex)の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし、原文を表示することが無意味な部分(特に脚注内)に関しては、原文または訳文の表示を省略した。

この参考訳は、あくまでも指令(EU) 2023/977 の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は、現時点における研究成果を反映するものである。将来、更に研究を深めた結果として修正すべき部分を発見したときは、その時点において、改訂版等を作成すべきかどうかを検討する。

参考訳の訳出に際しては原則として直訳とすることとしたが、直訳のままでは日本語にかなりにくい箇所に関しては、やむを得ず意訳とした。

この参考訳に訳注はない。参考訳中にある脚注は、全て原注である。訳注等による個別の説明がなければ当該箇所の訳出の理由がわかりにくいと想定される箇所に関しては、必要に応じて、「参考訳作成において留意した事項」の中で説明を加えることとした。

読みやすさを重視し、条文中の号(point)の表記を一部省略した。例えば、「point(a)」は「第(a)号」であるが、「第」と「号」を省略し、「(a)」と表記することにした。

この参考訳は、Eur-lex のデータ二次利用条件を遵守して作成した。

### 3. 参考訳作成において留意した事項

この参考訳は指令(EU) 2023/977 の注釈書ではないので、それらの箇所を全てを指摘することは避け、必要に応じて合理的に解釈した上で訳文を作成することにした。

ここでは、特に説明を加えないと誤訳ではないかと誤解される危険性がある箇所を中心に、この参考訳作成において留意した事項を摘記する。

\*\*\*

指令(EU) 2023/977 の前文(42)の中にある「concerning the latters' association」との箇所は、一見すると「concerning the latter's association」の誤記のように見えるが、この「latters」が「the Republic of Iceland and the Kingdom of Norway」を指すものであるとして理解すれば、誤記ではない。この参考訳においては、誤記ではないと解した上で、そのように訳出することにした。

指令(EU) 2023/977 の前文(44)の脚注(27)の中にある「on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association」との箇所は、明白に、「on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association」の誤記である。

この点に関し、ドイツ語版及びフランス語版には誤記がない。

この参考訳においては、あるべき正しい表現を前提として訳出することにした。英語版の原文のままでは、英語文としても日本語文としても意味のある文とはならず、正しく訳出できない。

### 3. 訳語に関する補足的説明

#### Requests or request

「requests」または「request」は、行為としての要請を示す場合と要請を行うための文書としての要請書を示す場合とがあり、一般的には、同一の法令内においては、単数形とするか複数形とするかにより、要請の行為を示しているのか文書を示しているのかを識別できるようにしてある。

ところが、指令(EU) 2023/977 においては、これらの語が統一的ではない態様で使用されているため、文脈から判断して、要請の行為を示しているのか文書を示しているのかを識別するしかない。

この参考訳においては、文脈から合理的に判断して適宜訳し分けることにした。

#### Intelligence

枠組み決定 2006/960/JHA の第 2 条(d)において定義されているとおり、EU の構成国の法執行機関の間における情報交換の文脈において使用される場合、「information and/or intelligence」は、「information and/or data」の別表現であると解される。枠組み決定 2006/960/JHA の表題も「on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union」となっており、この中でも「information and intelligence」が用いられている。

枠組み決定 2006/960/JHA の第 2 条(d)においては、「information and/or intelligence」が、捜査機関によって保有されている情報及びデータと民間組織によって保有されている情報及びデータの両方を含むものとして定義されていた。そのため、民間組織によって保有されているものを考慮に入れた上で、枠組み決定 2006/960/JHA の参考訳(法と情報雑誌 2 巻 5 号 95～110 頁所収)においては、「information and intelligence」を「情報と調査結果」と訳すことにした。ここで「調査結果」という語を用い、「捜査結果」とはしなかったのは、枠組み決定 2006/960/JHA においては、捜査機関が保有する情報だけではなく民間組織が保有する情報も含まれており、このうち(捜査の権限をもたない)民間組織が保有する情報に関しては「捜査結果」があり得ないことを重視したためである。

ところが、指令(EU) 2023/977 の定義条項には「intelligence」の定義が含まれておらず、前文の中で、主として枠組み決定 2006/960/JHA と関係する文脈において「intelligence」が使用されているだけであり、また、指令(EU) 2023/977 の表題も「on the exchange of information between the law enforcement authorities of Member States」となっていて「information and intelligence」から「information」へと改められている。

そこで、この参考訳においては、枠組み決定 2006/960/JHA の条項の文言を示すことが明らかな箇所に関しては「information and intelligence」を「情報及び知識」と訳すことにし、それ以外の部分に関しては、文脈に即して合理的に訳出することにした。

なお、枠組み決定 2006/960/JHA 及び指令(EU) 2023/977 のいずれにおいても、「intelligence」は、構成国の諜報機関が保有している諜報活動上の情報等を含まない。

#### 4. 関連参考訳

理事会枠組み決定 2006/960/JHA の参考訳は、法と情報雑誌 2 巻 5 号 95～110 頁にある。理事会枠組み決定 2002/584/JHA の参考訳は、法と情報雑誌 4 巻 5 号 185～213 頁にある。

e-CODEX 規則(EU) 2022/850 の参考訳は、法と情報雑誌 9 巻 1 号 1～57 頁にある。指令 2014/41/EU の参考訳は、法と情報雑誌 3 巻 7 号 199～245 頁にある。

規則(EU) 2021/1149 の参考訳は、法と情報雑誌 6 巻 3 号 1～103 頁にある。規則(EU) 2018/1861 の参考訳は、法と情報雑誌 4 巻 4 号 89～146 頁にある。規則(EU) 2018/1862 の参考訳は、法と情報雑誌 4 巻 6 号 1～70 頁にある。規則(EU) 2018/1241 による改正後の Europol 規則(EU) 2016/794 の参考訳は、法と情報雑誌 4 巻 4 号 8～68 頁にある。規則(EU) 2018/1860 の参考訳は、法と情報雑誌 4 巻 4 号 69～88 頁にある。理事会決定 2008/615/JHA の参考訳は、法と情報雑誌 2 巻 2 号 155～181 頁にある。理事会決定 2008/616/JHA の参考訳は、法と情報雑誌 2 巻 9 号 116～200 頁にある。相互運用性規則(EU) 2019/818 の参考訳は、法と情報雑誌 4 巻 8 号 158～231 頁にある。

規則 (EU) 2016/679(一般データ保護規則)の参考訳・再訂版は、法と情報雑誌 3 巻 5 号 1～114 頁にある。規則(EU)2018/1725 の参考訳は、法と情報雑誌 4 巻 1 号 1～81 頁にある。指令 2002/58/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 158～187 頁にある。指令(EU) 2016/680 の参考訳は、法と情報雑誌 2 巻 1 号 41～140 頁にある。PNR 指令(EU) 2016/681 の参考訳は、法と情報雑誌 2 巻 3 号 119～155 頁にある。

この参考訳の校正等に関し、唐亀侑久氏(株式会社ラック)の助力を得た。

\*\*\*

**構成国の法執行機関の間における情報の交換に関する  
及び理事会枠組み決定 2006/960/JHA を廃止する  
欧州議会及び理事会の 2023 年 5 月 10 日の指令(EU) 2023/977**

Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023  
on the exchange of information between the law enforcement authorities of Member States  
and repealing Council Framework Decision 2006/960/JHA

欧州議会及び欧州連合の理事会は、  
欧州連合の機能に関する条約、とりわけ、同条約の第 87 条第 2 項(a)に鑑み、  
欧州委員会からの提案に鑑み、  
立法案を国内議会に送付した後、  
通常の立法手続に従って審議し<sup>1</sup>、

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,  
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 87(2), point  
(a), thereof,  
Having regard to the proposal from the European Commission,  
After transmission of the draft legislative act to the national parliaments,  
Acting in accordance with the ordinary legislative procedure<sup>(1)</sup>

Whereas:

- (1) 複数国にわたる犯罪活動は、欧州連合の域内保安に対する重大な脅威を示しており、また、調整され、的を絞った、そして、変化に適応した対応を要求している。現地で活動を遂行している国内当局は、犯罪及びテロ行為との闘いの最前線に位置しているが、欧州連合レベルの活動では、情報の交換と関連する効率的かつ実効的な協力を確保することが最も重要である。更に、とりわけ、組織犯罪及びテロリズムは、域内保安と対外保安との間の結びつきの象徴的存在である。複数国にわたる犯罪活動は、国境を越えて拡大し、そして、動的であり複雑なものとなりつつある広範な犯罪活動に従事する組織犯罪及びテロリストグループにおいてその姿を現す。それゆえ、職務権限のある法執行機関が、より効率的な態様で、犯罪行為を防止、検出及び捜査できることを確保するための改善された法的枠組みの必要性がある。

Transnational criminal activities pose a significant threat to the internal security of the Union and call for a coordinated, targeted and adapted response. While national authorities operating on the ground are on

---

<sup>1</sup> 欧州議会の 2023 年 3 月 15 日付け意見書(官報未搭載)及び理事会の 2023 年 4 月 24 日付け決定。  
Position of the European Parliament of 15 March 2023 (not yet published in the Official Journal) and decision of the Council of 24 April 2023.



the frontline in the fight against crime and terrorism, action at Union level is paramount to ensuring efficient and effective cooperation as regards the exchange of information. Furthermore, organised crime and terrorism, in particular, are emblematic of the link between internal and external security. Transnational criminal activities spread across borders and manifest themselves in organised crime and terrorist groups that engage in a wide range of increasingly dynamic and complex criminal activities. There is, therefore, a need for an improved legal framework to ensure that competent law enforcement authorities can prevent, detect and investigate criminal offences in a more efficient manner.

- (2) 域内国境管理が存在しないことによって特徴づけられている自由、保安及び法務の領域の発展のため、ある構成国の職務権限のある法執行機関が、適用可能な欧州連合法及び国内法の範囲内で、当該法執行機関の別の構成国内の同じ職務権限のある法執行機関にとってアクセス可能な情報への均等なアクセスを獲得できる可能性をもつことが不可欠である。この点に関し、職務権限のある法執行機関は、実効的に、かつ、欧州連合全域にわたり、協力すべきである。それゆえ、犯罪行為を防止すること、検知することまたは捜査するという目的のための関連情報の交換に関する警察の協力は、域内国境管理のない相互依存する領域内における公共の保安を支える措置の必須の構成要素である。テロリズムを含め、犯罪及び犯罪活動に関する情報の交換は、自然人の安全を保護すること、及び、法律によって保護されている法人の重要な利益を安全確保することという全体的な目的に奉仕する。

For the development of an area of freedom, security and justice, which is characterised by the absence of internal border controls, it is essential that competent law enforcement authorities in one Member State have, within the framework of the applicable Union and national law, the possibility to obtain equivalent access to the information available to their colleagues in another Member State. In that regard, competent law enforcement authorities should cooperate effectively and across the Union. Therefore, police cooperation on the exchange of relevant information for the purpose of preventing, detecting or investigating criminal offences is an essential component of the measures that underpin public security in an interdependent area without internal border controls. The exchange of information on crime and criminal activities, including terrorism, serves the overall objective of protecting the security of natural persons and safeguarding important interests of legal persons protected by law.

- (3) 組織犯罪グループの主流は、3 か国を超える国内に存在し、かつ、様々な犯罪活動に従事する異なる国籍をもつ者によって構成されている。組織犯罪グループの組織構造は、強力で効率的な通信システムと当該犯罪組織の構成員の国境を越える協力のある、かつてなく精緻化されたものである。

The majority of organised crime groups are present in more than three countries and are composed of members with multiple nationalities who engage in various criminal activities. The structure of organised crime groups is ever more sophisticated, with strong and efficient communication systems and cooperation between their members across borders.

- (4) 国境を越える犯罪と実効的に闘うため、職務権限のある法執行機関が迅速に情報を交換し、かつ、相互に業務遂行上の協力をすることは、最も大きな重要性をもつ。近年、職務権限のある法執行機関の間における国境を越える協力が改善されたとはいえ、一定の実務上及び法律上のハードルが存在し続けている。この点に関し、理事会勧告(EU) 2022/915<sup>2</sup>は、国境を越える業務遂行上の協力の更なる拡大において、構成国を助けることになる。

To fight cross-border crime effectively, it is of paramount importance that competent law enforcement authorities swiftly exchange information and cooperate operationally with one another. Although cross-border cooperation between the competent law enforcement authorities has improved in recent years, certain practical and legal hurdles continue to exist. In that respect, Council Recommendation (EU) 2022/915<sup>(2)</sup> will assist the Member States in further enhancing cross-border operational cooperation.

- (5) 幾つかの構成国は、例えば、国境領域における近隣構成国からの警察官による共同巡視に焦点を当てた、国境を越える協力を強化するための実験プロジェクトを設けた。多数の構成国が、情報の交換を含め、国境を越える協力を強化するための二か国間協定も締結し、または、多国間協定さえも締結した。この指令は、そのような協定の中で定められた情報の交換に関する規定が、この指令が適用される場合にはこの指令と互換性をもつことを条件として、そのようにできることに対して制限を加えない。反対に、構成国は、そのような実験プロジェクト及び協定から習得したベストプラクティス及び教訓を交換すること、そして、それらの諸点と関連する利用可能な欧州連合の資金提供、とりわけ、欧州議会及び理事会の規則(EU) 2021/1149<sup>3</sup>によって設けられた域内保安基金からの資金提供を利用することが推奨される。

Some Member States have developed pilot projects to strengthen cross-border cooperation, focusing, for example, on joint patrols by police officers from neighbouring Member States in border regions. A number of Member States have also concluded bilateral or even multilateral agreements to strengthen cross-border cooperation, including the exchange of information. This Directive does not limit such possibilities, provided that the rules on the exchange of information set out in such agreements are compatible with this Directive where it applies. On the contrary, Member States are encouraged to exchange best practice and lessons learnt from such pilot projects and agreements and to make use of available Union funding in that regard, in particular from the Internal Security Fund, established by Regulation (EU) 2021/1149 of the European Parliament and of the Council<sup>(3)</sup>.

- (6) 犯罪行為の防止及び検知の目的のための構成国間の情報交換は、1990 年 6 月 19 日に採択さ

---

<sup>2</sup> 法執行業務遂行協力に関する 2022 年 6 月 9 日の理事会勧告(EU) 2022/915 (OJ L 158, 13.6.2022, p. 53).

Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation (OJ L 158, 13.6.2022, p. 53).

<sup>3</sup> 域内保安基金を設ける欧州議会及び理事会の 2021 年 7 月 7 日の規則(EU) 2021/1149 (OJ L 251, 15.7.2021, p. 94).

Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund (OJ L 251, 15.7.2021, p. 94).

れた 1985 年 6 月 14 日のシェンゲン協定実装条約<sup>4</sup>, とりわけ, 同条約の第 39 条及び第 46 条によって規律される。理事会枠組み決定 2006/960/JHA<sup>5</sup> は, 当該条約の条項を一部置き換え, 職務権限のある法執行機関の間における情報及び調査結果の交換のための新たな規定を導入した。

The exchange of information between Member States for the purpose of preventing and detecting criminal offences is regulated by the Convention implementing the Schengen Agreement of 14 June 1985<sup>(4)</sup>, adopted on 19 June 1990, in particular Articles 39 and 46 thereof. Council Framework Decision 2006/960/JHA<sup>(5)</sup> partially replaced those provisions and introduced new rules for the exchange of information and intelligence between competent law enforcement authorities.

- (7) 理事会規則(EU) No 1053/2013<sup>6</sup>の下で遂行された評価を含め, 諸評価は, 枠組み決定 2006/960/JHA が十分に明確なものではないということ, そして, 構成国間における関連情報の適切かつ迅速な交換を確保していないことを示した。諸評価は, 部分的には, シェンゲン協定実装条約の適用範囲と同枠組み決定の適用範囲との間の実務上で遭遇する明確性の欠如のゆえに, 同枠組み決定が実際にはほとんど利用されていないということも示した。

Evaluations, including those carried out under Council Regulation (EU) No 1053/2013<sup>(6)</sup>, have indicated that Framework Decision 2006/960/JHA is not sufficiently clear and does not ensure the adequate and rapid exchange of relevant information between Member States. Evaluations have also indicated that that Framework Decision is scarcely used in practice, in part due to the lack of clarity encountered in practice between the scope of the Convention implementing the Schengen Agreement and the scope of that Framework Decision.

---

<sup>4</sup> 当該国の共通国境における検問の漸進的廃止に関するベネルクス経済共同体諸国の政府, ドイツ連邦共和国の政府及びフランス共和国の政府の間における 1985 年 6 月 14 日のシェンゲン協定を実装する条約 (OJ L 239, 22.9.2000, p. 19).

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (OJ L 239, 22.9.2000, p. 19).

<sup>5</sup> 欧州連合の構成国の法執行機関の間における情報及び知識の交換の簡素化に関する 2006 年 12 月 18 日の理事会枠組み決定 2006/960/JHA (OJ L 386, 29.12.2006, p. 89).

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006, p. 89).

<sup>6</sup> シェンゲン協定の適用を検証するための評価及び監視の仕組みを設け, シェンゲンの評価及び実装に関する独立委員会を設置する 1998 年 9 月 16 日の執行委員会の決定を廃止する 2013 年 10 月 7 日の理事会規則(EU) No 1053/2013 (OJ L 295, 6.11.2013, p. 27).

Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen *acquis* and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p. 27).

- (8) それゆえ、不一致を解消するため、そして、異なる構成国の職務権限のある法執行機関の間における情報の適切かつ迅速な交換を容易にするため及び確保するための明確かつ整合化された規定を設けるためという観点から、並びに、社会のグローバル化及びデジタル化という文脈における場合を含め、組織犯罪の急速に変化し、拡大するという性質に対し、職務権限のある法執行機関が適応できるようにするためという観点から、現行の法的枠組みは、アップデートされるべきである。

Therefore, the existing legal framework should be updated with a view to eliminating discrepancies and to establishing clear and harmonised rules to facilitate and ensure the adequate and rapid exchange of information between the competent law enforcement authorities of different Member States and to allow the competent law enforcement authorities to adapt to the rapidly changing and expanding nature of organised crime, including in the context of the globalisation and digitalisation of society.

- (9) とりわけ、この指令は、犯罪行為を防止すること、検知することまたは捜査することを目的とする情報の交換を適用範囲とすべきであり、それによって、そのような交換が関係する範囲内において、シェンゲン協定実装条約の第 39 条及び第 46 条と完全に置き換わり、かつ、必要な法的確実性を提供すべきである。加えて、関連規定は、実務における当該規定の実効的な適用を容易にするため、簡素化され、かつ、明確化されるべきである。

In particular, this Directive should cover the exchange of information for the purpose of preventing, detecting or investigating criminal offences, thereby fully superseding, in so far as such exchanges are concerned, Articles 39 and 46 of the Convention implementing the Schengen Agreement and providing the necessary legal certainty. In addition, the relevant rules should be simplified and clarified in order to facilitate their effective application in practice.

- (10) この指令の下にある構成国間の、犯罪情報の収集の段階から犯罪捜査の段階までの様々な捜査段階における情報の交換の横断的な側面を規律する整合化された規定を定める必要がある。当該規定は、犯罪行為を防止すること、検知することまたは捜査することを目的とする二国間協定または多国間協定を根拠として複数の構成国の間で設置される警察及び税関の協力拠点を介する情報の交換を含めるべきである。ただし、当該規定は、第三国との間の二国間の情報の交換を含めてはならない。この指令に定める規定は、欧州議会及び理事会の規則(EU) 2016/794<sup>7</sup>、規則(EU) 2018/1860<sup>8</sup>、規則(EU) 2018/1861<sup>9</sup>、規則(EU) 2018/1862<sup>10</sup>、欧州議会及び理事会の指令

---

<sup>7</sup> 法執行の協力のための欧州連合局(Europol)に関する、並びに、理事会決定 2009/371/JHA、理事会決定 2009/934/JHA、理事会決定 2009/935/JHA、理事会決定 2009/936/JHA 及び理事会決定 2009/968/JHA を置き換えて廃止する欧州議会及び理事会の 2016 年 5 月 11 日の規則(EU) 2016/794(OJ L 135, 24.5.2016, p. 53).

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

<sup>8</sup> 不法滞在中の第三国国民の帰国のためのシェンゲン情報システムの利用に関する欧州議会及び理事会の 2018 年 11 月 28 日の規則(EU) 2018/1860 (OJ L 312, 7.12.2018, p. 1).

(EU) 2016/681<sup>11</sup> 及び指令(EU) 2019/1153<sup>12</sup>, 理事会決定 2008/615/JHA<sup>13</sup> 及び理事会決定 2008/616/ JHA<sup>14</sup> のような, そのような交換のための個別の制度または枠組みに関する欧州連合法の規定の適用に対して影響を与えてはならない。

It is necessary to lay down harmonised rules governing the crosscutting aspects of the exchange of information between Member States under this Directive at different stages of an investigation, from the

---

Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1).

<sup>9</sup> 国境検問の分野におけるシェンゲン情報システム(SIS)の構築, 運営及び利用に関する, 並びに, シェンゲン協定実装条約を改正し, 及び, 規則(EC) No 1987/2006 を改正及び廃止する欧州議会及び理事会の 2018 年 11 月 28 日の規則(EU) 2018/1861 (OJ L 312, 7.12.2018, p. 14).

Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

<sup>10</sup> 刑事における警察協力及び法務上の協力の分野におけるシェンゲン情報システム(SIS)の構築, 運営及び利用に関する, 理事会決定 2007/533/JHA を改正及び廃止し, 欧州議会及び理事会の規則(EC) No 1986/2006, 委員会決定 2010/261/EU を廃止する欧州議会及び理事会の 2018 年 11 月 28 日の規則(EU) 2018/1862 (OJ L 312, 7.12.2018, p. 56).

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

<sup>11</sup> テロリスト犯罪及び重大犯罪の防止, 検知, 捜査及び訴追のための旅客名記録(PNR)データの利用に関する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/681 (OJ L 119, 4.5.2016, p. 132).

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p. 132).

<sup>12</sup> 一定の犯罪行為の防止, 検知, 捜査または訴追のための信用情報及びその他の情報の利用を容易にする規定を定める, 並びに, 理事会決定 2000/642/JHA を廃止する欧州議会及び理事会の 2019 年 6 月 20 日の指令(EU) 2019/1153 (OJ L 186, 11.7.2019, p. 122).

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.7.2019, p. 122).

<sup>13</sup> とりわけテロリズム及び国境を越える犯罪との闘いにおける国境を越える協力の強化に関する 2008 年 6 月 23 日の理事会決定 2008/615/JHA (OJ L 210, 6.8.2008, p. 1).

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).

<sup>14</sup> とりわけテロリズム及び国境を越える犯罪との闘いにおける国境を越える協力の強化に関する理事会決定 2008/615/JHA の実装に関する 2008 年 6 月 23 日の理事会決定 2008/616/JHA (OJ L 210, 6.8.2008, p. 12).

Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

phase of gathering criminal intelligence to the phase of criminal investigation. Those rules should include the exchange of information through Police and Customs Cooperation Centres set up between two or more Member States on the basis of bilateral or multilateral arrangements for the purpose of preventing, detecting or investigating criminal offences. However, those rules should not include the bilateral exchange of information with third countries. The rules laid down in this Directive should not affect the application of rules of Union law on specific systems or frameworks for such exchanges, such as Regulations (EU) 2016/794<sup>(7)</sup>, (EU) 2018/1860<sup>(8)</sup>, (EU) 2018/1861<sup>(9)</sup> and (EU) 2018/1862<sup>(10)</sup> of the European Parliament and of the Council, Directives (EU) 2016/681<sup>(11)</sup> and (EU) 2019/1153<sup>(12)</sup> of the European Parliament and of the Council, and Council Decisions 2008/615/JHA<sup>(13)</sup> and 2008/616/JHA<sup>(14)</sup>.

- (11) 「犯罪行為」は、欧州連合の司法裁判所によって解釈されるものとしての欧州連合法の自律的な概念である。この指令の目的のために、犯罪との実効的な闘いの利益において、「犯罪行為」は、この指令に定める情報を求める要請の拒否のための根拠を妨げることなく、当該構成国において刑罰が科され得るか否かに拘わらず、かつ、情報を提供する構成国の犯罪法の下においてもその行為が処罰され得るか否かに拘わらず、この指令に従った情報の提供の要請による場合と、この指令に従った情報の自発による提供による場合のいずれであっても、情報を受領する構成国の犯罪法の下において処罰され得る行為のことを指すと理解されるべきである。

‘Criminal offence’ is an autonomous concept of Union law as interpreted by the Court of Justice of the European Union. For the purposes of this Directive, in the interest of effectively combating crime, ‘criminal offence’ should be understood as referring to any conduct punishable under the criminal law of the Member State that receives information, either pursuant to a request or pursuant to an own-initiative provision of information in accordance with this Directive, irrespective of the penalty that can be imposed in that Member State and irrespective of whether the conduct is also punishable under the criminal law of the Member State that provides information, without prejudice to the grounds for refusal of requests for information set out in this Directive.

- (12) この指令は、税関当局間における相互補助及び協力に関し、欧州連合条約の第 K.3 条を根拠として起草された条約(ナポリ II)<sup>15</sup>を妨げない。

This Directive is without prejudice to the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations<sup>(15)</sup> (Naples II).

- (13) この指令は、欧州連合法の適用範囲外にある活動の過程における情報の処理に対しては適用されないため、国家安全保障と関係する活動は、この指令の適用範囲内にはない。

---

<sup>15</sup> OJ C 24, 23.1.1998, p. 2.

Since this Directive does not apply to the processing of information in the course of an activity which falls outside the scope of Union law, activities concerning national security do not fall within the scope of this Directive.

- (14) この指令は、法務上の手続における証拠としての情報の提供及び利用を規律しない。とりわけ、この指令は、この指令に従って提供される情報を証拠として利用する権利を創設するものとして理解されてはならず、また、その結果として、この指令は、そのような利用のために、情報を提供する構成国の同意を得ることを定める適用可能な法律中の要件に対して影響を与えない。この指令は、刑事手続における電子証拠のための及び刑事手続後の拘禁刑の執行のための欧州提出命令及び保全命令に関する欧州議会及び理事会の規則、欧州議会及び理事会の指令 2014/41/EU<sup>16</sup>、並びに、刑事手続における電子証拠の収集の目的のための指定された拠点の指定及び法律上の代理者の指名に関する整合化された規定を定める欧州議会及び理事会の指令のような、証拠に関する欧州連合の法行為に対して影響を与えない。その結果として、この指令の下においてそのようにすることを構成国が求められていない場合であっても、この指令の下において情報を提供する構成国は、その情報を提供する時点またはその後の時点において、国内法の下においてそれが必要なときは、その構成国間で発効している法務上の協力に関する法律文書の利用を介する場合を含め、法務上の手続における当該情報の証拠としての利用に対して同意することが認められるべきである。

This Directive does not govern the provision and use of information as evidence in judicial proceedings. In particular, it should not be understood as establishing a right to use the information provided in accordance with this Directive as evidence and, consequently, it does not affect any requirement provided for in the applicable law to obtain the consent of the Member State providing the information for such use. This Directive does not affect Union legal acts on evidence, such as a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, Directive 2014/41/EU of the European Parliament and of the Council<sup>(16)</sup> and a Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. Consequently, even though they are not required to do so under this Directive, Member States providing information under this Directive should be allowed to consent, at the time of providing the information or thereafter, to the use of that information as evidence in judicial proceedings, including, where necessary under national law, through the use of instruments regarding judicial cooperation in force between the Member States.

---

<sup>16</sup> 刑事における欧州捜査令状に関する欧州議会及び理事会の 2014 年 4 月 3 日の指令 2014/41/EU (OJ L 130, 1.5.2014, p. 1).

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1).

- (15) この指令の下にある全ての情報の交換は、5 つの基本原則、すなわち、可用性の原則、均等なアクセスの原則、機密性の原則、データの保有の原則及びデータの信頼性の原則に従うべきである。それらの基本原則がこの指令の更に個別的な条項を妨げることはないが、当該基本原則は、それが関連するとき、この指令の解釈及び適用を導くべきである。第一に、可用性の原則は、ある構成国の単一連絡部局または職務権限のある法執行機関にとって利用可能な関連情報が、可能な最大限の範囲で、別の構成国の単一連絡部局または職務権限のある法執行機関にとっても利用可能であるべきであるということを目指すものとして理解されるべきである。ただし、同原則は、情報を求める要請の拒否の根拠に関する条項もしくは法務上の許可に関する条項のような、正当な理由がある場合において情報の可用性を制限するこの指令の個別の条項の適用に対して影響を与えてはならず、または、その情報を共有する前にその情報を最初に提供した構成国もしくはは第三国の同意を得るべき義務の適用に対して影響を与えてはならない。第二に、均等なアクセスの原則により、より個別的なこの指令の条項に服して、構成国は、関連情報に対して別の構成国の単一連絡部局及び職務権限のある法執行機関がもつアクセスが、当該情報に対して当該構成国自身の単一連絡部局及び職務権限のある法執行機関がもつアクセスと実質的に同一であることを確保し、そして、より強く制限的でもより弱く制限的でもないことを確保すべきである。第三に、機密性の原則は、構成国に対し、当該構成国の単一連絡部局または職務権限のある法執行機関に対して提供される機密としての標識のある情報を取扱う場合において、国内法に定める機密性に関する規定に従って同様のレベルの機密性を確保することにより、機密性に関する相互の国内規定を尊重することを要求する。第四に、データの保有の原則により、別の構成国からまたは第三国から最初に入手された情報は、当該構成国または第三国の同意があり、かつ、当該構成国または第三国によって加えられた条件に従う場合に限り、提供されるべきである。第五に、データの信頼性の原則により、不正確、不完全または最新ではないと判断された個人データは、消去または訂正されるべきであり、または、当該データの処理は、しかるべく制限されるべきであり、かつ、当該データの受領者は、遅滞なく通知を受けるべきである。

All exchanges of information under this Directive should be subject to five general principles, namely the principles of availability, equivalent access, confidentiality, data ownership and data reliability. While those principles are without prejudice to the more specific provisions of this Directive, they should guide its interpretation and application where relevant. First, the principle of availability should be understood as indicating that relevant information available to the Single Point of Contact or the competent law enforcement authorities of one Member State should also be available, to the largest extent possible, to the Single Point of Contact or the competent law enforcement authorities of other Member States. However, that principle should not affect the application, where justified, of specific provisions of this Directive restricting the availability of information, such as those on the grounds for refusal of requests for information and on judicial authorisations, or of the obligation to obtain the consent of the Member State or third country that initially provided the information prior to sharing it. Second, pursuant to the principle of equivalent access, Member States should ensure that the access that the Single Point of Contact and the competent law enforcement authorities of other Member States have to relevant information is substantially the same as, and thus neither stricter nor less strict than, the access that their own Single Point of Contact and the competent law enforcement authorities have to that information,



subject to the more specific provisions of this Directive. Third, the principle of confidentiality requires Member States to respect one another's national rules on confidentiality when treating information marked as confidential that is provided to their Single Point of Contact or to their competent law enforcement authorities, by ensuring a similar level of confidentiality in accordance with the rules on confidentiality set out in national law. Fourth, pursuant to the principle of data ownership, information initially obtained from another Member State or from a third country should only be provided with the consent of and in accordance with the conditions imposed by that Member State or third country. Fifth, pursuant to the principle of data reliability, personal data that are found to be inaccurate, incomplete or no longer up to date should be erased or rectified or the processing of those data should be restricted, as appropriate, and any recipient of those data should be notified without delay.

- (16) 構成国間における情報の適切かつ迅速な交換を容易にすること及び確保することという目的を達成するため、この指令は、一定の明確で、簡素化され、かつ、整合化された要件に従い、別の構成国の単一連絡部局を名宛人とする情報を求める要請により、構成国が情報を入手する可能性を提供すべきである。情報を求める要請書の内容に関しては、この指令は、とりわけ、網羅的であり、かつ、十分に詳細な態様で、かつ、ケースバイケースの評価の必要性を妨げることなく、情報を求める要請が緊急であると判断されるべき状況、当該要請書がミニマムのものとして含めるべき細目、及び、当該要請書がどの言語によって提出されるべきかを定めるべきである。

In order to achieve the objective of facilitating and ensuring the adequate and rapid exchange of information between Member States, this Directive should provide the possibility for Member States to obtain information by addressing a request for information to the Single Point of Contact of other Member States, in accordance with certain clear, simplified and harmonised requirements. As regards the content of requests for information, this Directive should specify, in particular, in an exhaustive and sufficiently detailed manner and without prejudice to the need for a case-by-case assessment, the situations in which requests for information are to be considered urgent, the details they are to contain as a minimum and in which language they are to be submitted.

- (17) 各構成国の単一連絡部局は、いかなる場合においても、別の構成国の単一連絡部局に対して情報を求める要請書を提出できるべきであるが、柔軟性の利益において、構成国は、それに加えて、別の構成国の単一連絡部局に対してそのような要請を提出する目的のために指定された法執行機関として欧州の協力に包摂され得る幾つかの当該構成国の職務権限のある法執行機関を指定することが認められるべきである。各構成国は、欧州委員会に対し、当該構成国の指定された法執行機関のリストを提出すべきである。当該リストに変更があるときは、構成国は、欧州委員会に対し、連絡すべきである。欧州委員会は、そのリストをオンラインで公表すべきである。ただし、単一連絡部局がこの指令の下にある単一連絡部局の調整の機能を遂行できるようにするため、構成国が、別の構成国の単一連絡部局に対して情報を求める要請書を提出することを当該構成国の幾つかの職務権限のある法執行機関に対して認めることを決定するときは、当該構成国は、当該構成国の単一連絡部局に対してコピーを常に送付することにより、当該構成国の単一連絡部局が、現在進行中の全ての情報を求める要請及び同要請と関係する通信に気づかせる。構成

国は、厳格にミニマムに、個人データの正当化されない重複を制限することに努めるべきである。

While the Single Points of Contact of each Member State should, in any event, be able to submit requests for information to the Single Point of Contact of another Member State, in the interest of flexibility, Member States should be allowed, in addition, to designate some of their competent law enforcement authorities, which might be involved in European cooperation, as designated law enforcement authorities for the purpose of submitting such requests to the Single Points of Contact of other Member States. Each Member State should submit to the Commission a list of its designated law enforcement authorities. Member States should inform the Commission where there are any changes to that list. The Commission should publish the lists online. In order for Single Points of Contact to be able to perform their coordinating functions under this Directive, it is, however, necessary that, where a Member State decides to allow some of its competent law enforcement authorities to submit requests for information to the Single Points of Contact of other Member States, that Member State makes its Single Point of Contact aware of all outgoing requests for information and of any communications relating thereto, by always putting its Single Point of Contact in copy. Member States should seek to limit the unjustified duplication of personal data to a strict minimum.

- (18) 単一連絡部局に対して提出された、情報を求める要請書の迅速な処理を確保するため、期限が必要である。期限は、明確かつ比例的であり、かつ、情報を求める要請が緊急として判断されるべきかどうか、及び、その要請が直接にアクセス可能な情報と関係するか間接にアクセス可能な情報と関係するかを考慮に入れるべきである。それが客観的に正当化されるときは、ある程度の柔軟性を許容しつつ、適用可能な期限の遵守を確保するため、要請先構成国の職務権限のある法務当局が必要な法務上の許可を与えることを決定するための付加的な期間を必要とするときに限り、その範囲内で、例外として、当該期限の適用を免れ得るべきである。そのような必要性は、例えば、情報を求める要請から生じる事柄の範囲が広いことや複雑性を理由として生じ得る。特定の案件において一刻を争う機会を逃さないことを可能な限り確保するため、要請先構成国は、当該情報がその要請と関連して利用可能な唯一の情報ではない場合であっても、その情報が単一連絡部局によって把握されたならば直ちに、要請された情報を提供すべきである。要請された残余の情報は、後にその情報が単一連絡部局によって把握されたならば直ちに、提供されるべきである。

Time limits are necessary to ensure the rapid processing of requests for information submitted to a Single Point of Contact. Time limits should be clear and proportionate and take into account whether the request for information is to be considered as urgent and whether the request relates to directly accessible information or indirectly accessible information. In order to ensure compliance with the applicable time limits while allowing for a degree of flexibility, where objectively justified, it should only be possible, on an exceptional basis, to deviate from those time limits where, and in so far as, the competent judicial authority of the requested Member State needs additional time to decide on granting the necessary judicial authorisation. Such a need could arise, for example, because of the broad scope or the complexity of the matters raised by the request for information. In order to ensure, as far as possible, that time-critical

opportunities to take action in specific cases are not missed, the requested Member State should provide any requested information as soon as it is held by the Single Point of Contact, even where that information is not the only information available that is relevant to the request. The rest of the requested information should be provided thereafter, as soon as it is held by the Single Point of Contact.

- (19) 単一連絡部局は、正当事由のない情報の提供または比例的ではない量の情報の提供を避けるため、要請された情報がこの指令の目的を達成するために必要かつ比例的なものであるかどうか、及び、その要請を正当化する客観的理由の説明が十分に明確かつ詳細であるかどうかを評価すべきである。

The Single Points of Contact should assess whether the information requested is necessary for and proportionate to achieving the purposes of this Directive and whether the explanation of the objective reasons justifying the request is sufficiently clear and detailed, so as to avoid the unjustified provision of information or the provision of disproportionate amounts of information.

- (20) 例外的な案件において、当該構成国の単一連絡部局に対して提出された情報を求める要請を構成国が拒否することが客観的に正当化され得る。この指令によって作り出された制度が法の支配を全面的に遵守して実効的に稼働することを確保するため、それらの例外的な案件は、網羅的に定められるべきであり、かつ、制限的に解釈されるべきである。ただし、この指令に定める規定は、必要性の原則及び比例性の原則に重点を置いており、それによって、その要請が基本的な権利の明白な侵害を伴うような場合を含め、情報を求める要請の濫用に抗する安全確保を提供している。それゆえ、構成国は、当該構成国の一般的なデューデリジエンスの表現として、この指令の下で当該構成国に対して提出された要請書の、必要性の原則及び比例性の原則の遵守を常に検証すべきであり、また、当該構成国が不遵守だと判断した当該要請を拒否すべきである。その要請を拒否する理由が、要請された情報の一部のみと関連するときは、残余の情報は、この指令に定める期限内に提供されるべきである。情報を求める要請の必然性のない拒否を避けるため、しかるべく、要請元構成国の単一連絡部局または指定された法執行機関は、求めに応じて、情報を求める要請を処理するために必要な明確化または特定を提供すべきである。適用可能な期限は、要請元構成国の単一連絡部局、または、それが適用可能なときは、要請元構成国の指定された法執行機関が、明確化または特定を求める要請を受けた時から、停止されるべきである。ただし、当該明確化または特定がなければ、この指令に列挙する理由のいずれかのゆえにその情報を求める要請が拒否されなければならないような場合のように、明確化または特定が客観的に必要かつ比例的である場合に限り、明確化または特定を求め得るべきである。実効的な協力の利益において、期限の停止を導くことなく、別の状況において、必要な明確化または特定を求めることもなお可能とすべきである。

In exceptional cases, it might be objectively justified for a Member State to refuse a request for information submitted to its Single Point of Contact. In order to ensure the effective functioning of the system created by this Directive in full compliance with the rule of law, those cases should be specified exhaustively and interpreted restrictively. However, the rules set out in this Directive place a strong

emphasis on the principles of necessity and proportionality, thereby providing safeguards against any misuse of requests for information, including where it would entail manifest breaches of fundamental rights. The Member States, as an expression of their general due diligence, should therefore always verify the compliance of requests submitted to them under this Directive with the principles of necessity and proportionality and should refuse those requests they find to be non-compliant. Where the reasons for refusing the request relate only to parts of the information requested, the remaining information should be provided within the time limits set out in this Directive. In order to prevent unnecessary refusals of requests for information, the Single Point of Contact or the designated law enforcement authority of the requesting Member State, as applicable, should, on request, provide clarification or specifications that are needed to process the request for information. The applicable time limits should be suspended from the moment that the Single Point of Contact or, where applicable, the designated law enforcement authority of the requesting Member State receives the request for clarification or specifications. However, it should be possible to request clarification or specifications only where clarification or specifications are objectively necessary and proportionate such that without them the request for information would have to be refused for one of the reasons listed in this Directive. In the interest of effective cooperation, it should also remain possible to request necessary clarification or specifications in other situations, without this leading to the suspension of the time limits.

- (21) 実際には多様であり得る業務遂行上の需要を考慮した必要な柔軟性を許容するため、この指令は、単一連絡部局に対して提出される情報を求める要請に加え、情報の交換の別の 2 つの手段を定めるべきである。第一の手段は、事前の要請のない、単一連絡部局または職務権限のある法執行機関から別の構成国の単一連絡部局または職務権限のある法執行機関に対する情報の無要請提供、すなわち、当該単一連絡部局または当該職務権限のある法執行機関の自発による単一連絡部局または職務権限のある法執行機関からの情報の提供である。第二の手段は、単一連絡部局または職務権限のある法執行機関から別の構成国の職務権限のある法執行機関に対して直接に提出される情報を求める要請書に基づく情報の提供である。両者の情報交換手段に関し、この指令は、とりわけ、関連する単一連絡部局への連絡を保つことに関する、及び、自発による情報の提供に関しては、情報が提供されるべき状況及び使用されるべき言語に関する、限定された数のミニマムの要件のみを定める。それらの要件は、情報を提供する際に使用されるべき言語に関してこの指令に定める規定の遵守が必要な場合のような、当該情報を別の構成国に対して提供するために当該職務権限のある法執行機関自身の構成国の単一連絡部局に対して職務権限のある法執行機関が情報を提供する状況下においても、適用されるべきである。

In order to allow for the necessary flexibility in view of operational needs that might vary in practice, this Directive should provide for two other means of exchanging information, in addition to requests for information submitted to the Single Points of Contact. The first one is the unsolicited provision of information by a Single Point of Contact or by a competent law enforcement authority to the Single Point of Contact or a competent law enforcement authority of another Member State without a prior request, namely the provision of information on its own initiative. The second one is the provision of information upon a request for information submitted either by a Single Point of Contact or by a competent law

enforcement authority directly to a competent law enforcement authority of another Member State. In respect of both means of exchange of information, this Directive sets out only a limited number of minimum requirements, in particular on keeping the relevant Single Points of Contact informed and, as regards own-initiative provisions of information, the situations in which information is to be provided and the language to be used. Those requirements should also apply to situations in which a competent law enforcement authority provides information to the Single Point of Contact of its own Member State in order to provide that information to another Member State, such as where it is necessary to comply with the rules set out in this Directive on the language to be used when providing information.

- (22) 国内法の中でそれが定められる場合、情報の提供に関する法務上の事前の許可の要件は、尊重されるべき重要な安全確保を構成する。ただし、構成国の法制度は、この点に関して異なっており、また、この指令は、国内の情報交換と構成国間の情報交換とが実体的にも手続的にも均等な態様で取り扱われるべきことを要求する規定及び条件を除き、国内法の中で定められる法務上の事前の許可と関係する規定及び条件に影響を与えるものとして理解されてはならない。更に、そのような要件の適用と関連する遅延と複雑化をミニマムに保つため、しかるべく、職務権限のある法務当局の構成国の単一連絡部局または職務権限のある法執行機関は、要求元構成国の単一連絡部局または指定された法執行機関との間の協力と関連するときは、可能な限り速やかに法務上の許可を得るための実務上及び法律上の全ての手立てをとるべきである。この指令の法的根拠は欧州連合の機能に関する条約(TFEU)の第 87 条第 2 項(a)に基づく法執行の協力に限定されるものではあるが、この指令は、法務当局に対しても適用があり得る。

The requirement of a prior judicial authorisation for the provision of information, where provided in national law, constitutes an important safeguard which should be respected. However, the Member States' legal systems are different in that respect and this Directive should not be understood as affecting the rules and conditions concerning prior judicial authorisations laid down in national law, other than requiring that domestic exchanges and exchanges between Member States be treated in an equivalent manner, both on substance and procedurally. Furthermore, in order to keep any delays and complications relating to the application of such a requirement to a minimum, the Single Point of Contact or the competent law enforcement authorities, as applicable, of the Member State of the competent judicial authority should take all practical and legal steps, where relevant in cooperation with the Single Point of Contact or the designated law enforcement authority of the requesting Member State, to obtain the judicial authorisation as soon as possible. Although the legal basis of this Directive is limited to law enforcement cooperation under Article 87(2), point (a), of the Treaty on the Functioning of the European Union (TFEU), this Directive might be of relevance to judicial authorities.

- (23) この指令の下にある全ての情報の交換との関係において、欧州連合法に従った個人データの保護が確保されることは、とりわけ重要である。その目的のために、この指令の下における単一連絡部局または職務権限のある法執行機関による個人データの処理は、欧州議会及び理事会の指令(EU) 2016/680<sup>17</sup>を全面的に遵守して遂行されるべきである。規則(EU) 2016/794 により、法執行の協力のための欧州連合局(Europol)は、同規則に定める規定に従ってデータを処理すべき

である。同指令及び同規則は、この指令により影響を受けない。とりわけ、単一連絡部局及び職務権限のある法執行機関によって交換される個人データが、規則(EU) 2016/794 の別紙Ⅱのセクション B に列挙されたデータ主体の類型毎のデータ類型の制限内にあることが定められるべきである。従って、容疑者と関係するデータと、証人、被害者またはそれ以外のグループに属する者との間で、より厳格な制限を適用するための明確な区別が行われるべきである。更に、可能な範囲内で、そのような個人データは、当該個人データの正確性及び信頼性に従って区別されるべきである。正確性及び信頼性を確保するため、事実上、個人に対する評価とは区別されるべきである。単一連絡部局、または、それが適用可能なときは、職務権限のある法執行機関は、個人データの正確性及び信頼性を確保するため、データの無用の重複を避けるため、そして、古くなっているデータのリスクまたは当該単一連絡部局もしくは職務権限のある法執行機関にとって既に利用可能ではなくなっているデータのリスクを削減するため、可能な限り迅速に、この指令の下にある情報を求める要請を処理すべきである。個人データが不正確であることが明らかとなるときは、当該データは、訂正または消去されるべきあり、また、当該個人データの処理は、遅滞なく、制限されるべきである。

It is particularly important that the protection of personal data, in accordance with Union law, be ensured in connection with all exchanges of information under this Directive. To that end, any personal data processing by a Single Point of Contact or a competent law enforcement authority under this Directive should be carried out in full compliance with Directive (EU) 2016/680 of the European Parliament and of the Council<sup>17</sup>. Pursuant to Regulation (EU) 2016/794, the European Union Agency for Law Enforcement Cooperation (Europol) is to process data in accordance with the rules set out therein. That Directive and that Regulation are unaffected by this Directive. In particular, it should be specified that any personal data exchanged by Single Points of Contacts and competent law enforcement authorities remain limited to the categories of data per category of data subject listed in Section B of Annex II to Regulation (EU) 2016/794. Accordingly, a clear distinction should be made between the data concerning suspects and the data concerning witnesses, victims, or persons belonging to other groups, for which stricter limitations apply. Furthermore, as far as possible, any such personal data should be distinguished in accordance with their degree of accuracy and reliability. In order to ensure accuracy and reliability, facts should be distinguished from personal assessments. The Single Points of Contact or, where applicable, competent law enforcement authorities should process requests for information under this Directive as quickly as possible in order to ensure the accuracy and reliability of personal data, to avoid unnecessary

---

<sup>17</sup> 犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行の目的のために職務権限のある機関による個人データの処理と関連する自然人の保護及びそのデータの支障のない移転に関する、並びに、理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU)2016/680(OJ L 119, 4.5.2016, p. 89).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

duplication of data, and to reduce the risk of data becoming outdated or no longer being available to them. Where it appears that the personal data are incorrect, they should be rectified or erased or their processing should be restricted without delay.

- (24) 要請による場合または自発的な場合のいずれでも、単一連絡部局による適切かつ迅速な情報の提供ができるようにするため、職務権限のある法執行機関が相互に理解することが重要である。要請された情報の提供を含め、情報の全ての交換、そのような拒否の理由を含め、情報を求める要請の拒否、並びに、それが適用可能なときは、明確化または特定を求める要請及び特定の要請と関連して提供された明確化または特定は、その言語によって当該要請書が提出された言語により、送信されるべきである。それゆえ、要請された情報の提供の遅延が言語の障壁によって生ずることを避けるため、そして、翻訳の費用を抑制するため、構成国は、その言語によって当該構成国の単一連絡部局が名宛人となることができ、かつ、その言語によって当該単一連絡部局が通信できる 1 または複数の言語のリストを設けるべきである。英語は、欧州連合内における法執行の協力と関連する実務において広く理解され、利用されている言語であるので、同リストの中に英語が含まれるべきである。構成国は、欧州委員会に対し、当該リスト及び同リストのアップデートを提供すべきである。欧州委員会は、それらのリストをとりまとめたものをオンラインで公表すべきである。

In order to allow for the adequate and rapid provision of information by Single Points of Contact, either upon request or on their own initiative, it is important that the competent law enforcement authorities understand each other. All exchanges of information, including the provision of requested information, refusals of requests for information, including the reasons for such refusals, and, where applicable, requests for clarification or specifications and clarification or specifications provided which relate to a specific request should be transmitted in the language in which that request was submitted. Therefore, to prevent delays in the provision of requested information caused by language barriers and to limit translation costs, Member States should establish a list of one or more languages in which their Single Point of Contact can be addressed and in which it can communicate. Since English is a language that is broadly understood and used in practice with regard to law enforcement cooperation within the Union, it should be included on that list. Member States should provide that list and any updates thereto to the Commission. The Commission should publish online a compilation of those lists.

- (25) 欧州の市民の安全と防護を確保するため、Europol が、職務権限のある法執行機関を支える欧州連合の刑事情報のハブとしての Europol の役割を満すために必要な情報をもつことが不可欠である。それゆえ、構成国間において情報が交換されるときは、単一連絡部局もしくは職務権限のある法執行機関に対して提出された情報を求める要請書により情報が交換されるのかどうか、または、当該単一連絡部局もしくは当該職務権限のある法執行機関の自発により単一連絡部局もしくは職務権限のある法執行機関から提供されるのかどうかとは無関係に、Europol の目的の適用範囲内にある犯罪行為とそれが関係する場合、ケースバイケースで、この指令の下で提出された情報を求める要請書のコピーまたはこの指令の下で交換された情報のコピーが規則(EU) 2016/794 の第 7 条第 6 項に従って Europol に送付されるべきかどうかに関し、評価が行われるべ

きである。そのような評価は、犯罪行為の適用範囲が関係している限り、規則(EU) 2016/794 に定める Europol の目的を基礎とすべきである。構成国は、そのようにすることが、関係する構成国の保安上の必須の利益と反するような場合、現在進行中の捜査の成功もしくは個人の安全を危険に晒すような場合、または、国家安全保障の分野における組織もしくは具体的な諜報活動と関連する情報を開示するような場合においては、情報を求める要請書のコピーまたは交換された情報のコピーを Europol に対して送付することを義務づけられてはならない。更に、データの保有の原則に従い、かつ、Europol による情報の処理の目的の決定及びその情報の処理の制限に関して規則(EU) 2016/794 に定める義務を妨げることなく、別の構成国または第三国から最初に入手された情報は、当該別の構成国または第三国がその同意を与えた場合に限り、Europol に対して提供されるべきである。構成国は、当該構成国の単一連絡部局の職員及び職務権限のある法執行機関の職員が、この指令の下で交換されるどの情報が Europol の任務の範囲内にあり、かつ、Europol が Europol の目的を満たすために必要であるかを迅速かつ正確に識別するために適切に支援を受け、かつ、訓練を受けることを確保すべきである。

To ensure the safety and security of European citizens, it is essential that Europol hold the necessary information to fulfil its role as the Union's criminal information hub supporting the competent law enforcement authorities. Therefore, when information is exchanged between Member States, irrespective of whether it is exchanged pursuant to a request for information submitted to a Single Point of Contact or competent law enforcement authority or whether it is provided by a Single Point of Contact or competent law enforcement authority on its own initiative, an assessment should be made, on a case-by-case basis, as to whether a copy of the request for information submitted under this Directive or of the information exchanged under this Directive should be sent to Europol in accordance with Article 7(6) of Regulation (EU) 2016/794 where it concerns a criminal offence falling within the scope of the objectives of Europol. Such assessments should be based on Europol's objectives as set out in Regulation (EU) 2016/794 in so far as the scope of the criminal offence is concerned. Member States should not be obliged to send a copy of the request for information or of the information exchanged to Europol where it would be contrary to the essential interests of the security of the Member State concerned, where it would jeopardise the success of an ongoing investigation or the safety of an individual or where it would disclose information relating to organisations or specific intelligence activities in the field of national security. Moreover, in accordance with the principle of data ownership and without prejudice to the obligation set out in Regulation (EU) 2016/794 concerning the determination of the purpose of, and restrictions on, the processing of information by Europol, information initially obtained from another Member State or a third country should be provided to Europol only where that Member State or third country has given its consent. Member States should ensure that the staff of their Single Point of Contact and competent law enforcement authorities are adequately supported and trained to quickly and accurately identify which information exchanged under this Directive falls within the mandate of Europol and is necessary for it to fulfil its objectives.

- (26) 構成国間における法執行情報の送信のために使用される通信経路の増加という問題は、そのことが、そのような情報の適切かつ迅速な交換を阻害し、また、個人データの防護と関係するリスク



を増大させるので、解消されるべきである。それゆえ、単一連絡部局に対する及び直接に職務権限のある法執行機関に対する情報を求める要請書の送付、そのような要請による情報の提供、並びに、当該単一連絡部局及び当該職務権限のある法執行機関の自発による単一連絡部局及び職務権限のある法執行機関からの情報の提供、情報を求める要請の拒否、明確化及び特定に関する通信、情報を求める要請書のコピーまたは情報のコピーの単一連絡部局及び Europol に対する送付を含め、この指令の下にある全ての送信及び通信に関し、規則(EU) 2016/794 に従って Europol によって管理及び開発されている安全な情報交換ネットワークアプリケーション(SIENA)の利用が義務づけられるべきである。その目的のために、全ての単一連絡部局、及び、情報の交換に関与するかもしれない全ての職務権限のある法執行機関は、SIENA と直接に接続されるべきである。捜査網の活動遂行に関与する警察官のような最前線の官吏が SIENA を利用できるようにするため、それが適切なときは、モバイル機器上でも業務遂行できるべきである。その点に関し、SIENA の全面運用には幾つかの構成国の現行の覚書の変更を伴い、かつ、当該構成国の職員が訓練を受けることを要するので、SIENA の全面運用を可能とするための短い移行期間が定められるべきである。業務遂行上の現実を考慮に入れるため、そして、職務権限の法執行機関の間における良好な協力を妨げないため、構成国は、当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関が、正当理由のある限定された数の状況下において、別の安全な通信経路を利用することを許容し得るべきである。構成国が、情報を求める要請の緊急性のゆえに、当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関に対して別の通信経路を使用することを許容する場合、当該構成国は、それが実務に適しており、かつ、業務遂行上の必要性と一貫しているときは、その状況が緊急のものではなくなった後、SIENA を利用することに戻るべきである。SIENA の利用は、構成国内における国内的な情報の交換に関しては義務的であってはならない。

The problem of the proliferation of communication channels used for the transmission of law enforcement information between Member States should be remedied because it hinders the adequate and rapid exchange of such information and increases the risks concerning the security of personal data. Therefore, the use of the Secure Information Exchange Network Application (SIENA), managed and developed by Europol in accordance with Regulation (EU) 2016/794, should be made mandatory for all transmissions and communications under this Directive, including the sending of requests for information to Single Points of Contact and directly to competent law enforcement authorities, the provision of information pursuant to such requests and the provision of information by Single Points of Contact and competent law enforcement authorities on their own initiative, communications on refusals of requests for information, clarification and specifications, and the sending of copies of requests for information or information to Single Points of Contact and Europol. To that end, all Single Points of Contact, and all competent law enforcement authorities that might be involved in exchanges of information, should be directly connected to SIENA. To allow frontline officers, such as police officers involved in dragnet operations, to use SIENA, it should also be operational on mobile devices, where appropriate. In that regard, a short transition period should be provided for in order to allow for the full roll-out of SIENA because it entails a change of the current arrangements in some Member States and requires those staff be trained. In order to take into account the operational reality and not to hamper good cooperation

between competent law enforcement authorities, Member States should be able to allow their Single Point of Contact or their competent law enforcement authorities to use another secure communication channel in a limited number of justified situations. Where Member States permit their Single Point of Contact or their competent law enforcement authorities to use another communication channel due to the urgency of the request for information, they should, where practicable and consistent with operational needs, revert to using SIENA after the situation ceases to be urgent. The use of SIENA should not be mandatory for internal exchanges of information within a Member State.

- (27) 情報の流れを簡素化し、容易にし、かつ、より良く管理するため、各構成国は、単一連絡部局を設置または指定すべきである。単一連絡部局は、この指令の下にある情報の交換を調整すること及び容易にすることに関する職務権限をもつべきである。各構成国は、欧州委員会に対し、当該構成国の単一連絡部局の設置または指定及び同設置または同指定の変更を通知すべきである。欧州委員会は、当該設置または指定及び同設置または同指定のアップデートを公表すべきである。単一連絡部局は、とりわけ、麻薬取引、サイバー犯罪、人身取引及びテロリズムのような、国境を越える犯罪と共同して闘う必要が増加していることと関係して、職務権限のある法執行機関が相互に通信する方法の断片化から帰結する情報の流れの障害を緩和することに寄与すべきである。単一連絡部局は、この指令の下にある法執行の目的のための国境を越える情報の交換と関係する単一連絡部局の調整の機能を単一連絡部局が実効的に満たすことができるための、多数の、個別の、ミニマムの職務を割当てられ、かつ、そのための一定のミニマムの能力をもつべきである。

In order to simplify, facilitate and better manage information flows, each Member State should establish or designate a Single Point of Contact. Single Points of Contact should be competent for coordinating and facilitating the exchange of information under this Directive. Each Member State should notify the Commission of the establishment or designation of its Single Point of Contact and any changes thereto. The Commission should publish those notifications and any updates thereto. The Single Points of Contact should, in particular, contribute to mitigating the obstacles to information flows resulting from the fragmentation of the way in which competent law enforcement authorities communicate with one another, in response to the growing need to jointly tackle cross-border crime, such as drug trafficking, cybercrime, trafficking in human beings, and terrorism. The Single Points of Contact should be assigned a number of specific, minimum tasks and have certain minimum capabilities so that they are able to effectively fulfil their coordinating functions in respect of the cross-border exchange of information for law enforcement purposes under this Directive.

- (28) 単一連絡部局は、欧州連合の及び国際的な、関連する全てのデータベース及びプラットフォームへのユーザフレンドリなアクセスをもつことによることを含め、適用可能な欧州連合法及び国内法の中で指定された手立てに従い、当該単一連絡部局の構成国の中で利用可能な全ての情報へのアクセスをもつべきである。この指令の要件、とりわけ、期限に関する要件に適合できるため、単一連絡部局は、適切な翻訳能力を含め、予算及び職員の面において十分な資源の提供を受けるべきであり、また、単一連絡部局は、24時間体制で機能すべきである。この点に関し、受信す

る情報を求める要請を選別し、処理し、及び、仕分けることのできるフロントデスクをもつことは、単一連絡部局の実効性及び効率性を増加させ得る。単一連絡部局は、常時、当該単一連絡部局が自由に利用でき、必要な法務上の許可を与える職務権限をもつ法務当局ももつべきである。実務上では、例えば、そのような法務当局がその単一連絡部局の施設内に物理的に所在することを確保することにより、または、その単一連絡部局の施設内においてそのような法務当局の機能を利用でき、もしくは、求めに応じて直接に利用できることを確保することにより、それが実行され得る。

The Single Points of Contact should have access to all information available within their Member State, including by having user-friendly access to all relevant Union and international databases and platforms, in accordance with the arrangements specified in the applicable Union and national law. In order to be able to meet the requirements of this Directive, in particular those on time limits, the Single Points of Contact should be provided with adequate resources in terms of budget and staff, including adequate translation capabilities, and they should function around the clock. In that regard, having a front desk that is able to screen, process and channel incoming requests for information could increase their efficiency and effectiveness. Single Points of Contact should also have at their disposition, at all times, judicial authorities competent to grant necessary judicial authorisations. In practice, that can be done, for example, by ensuring the physical presence of such judicial authorities within the premises of the Single Point of Contact or the functional availability of such judicial authorities either within the premises of the Single Point of Contact or directly available on call.

- (29) この指令の下にある単一連絡部局の調整機能を単一連絡部局が実効的に遂行できるようにするため、単一連絡部局は、この指令の下にある情報の適切かつ迅速な交換にとってその包摂が必要となる当該構成国の職務権限のある法執行機関からの職員によって構成されるべきである。当該要件に適合するために必要となる組織及び構成の詳細に関して決定するのは、個々の構成国ではあるが、犯罪行為の防止、検知または捜査に関する職責を負う警察、税関及びそれ以外の職務権限のある法執行機関、並びに、別の構成国に派遣または補職される連絡官と専門官のような、地域事務所と二国間事務所のための可能な連絡先、及び、Europol のような、関連する欧州連合の法執行機関は、単一連絡部局と表現され得る。ただし、実効的な調整の利益において、ミニマムのもので、単一連絡部局は、欧州連合の関連する法行為または国際協定によって設置され、かつ、当該欧州連合の法行為によって個別に規律されている情報の交換に対してはこの指令が適用されないことに拘わらず、Europol 国内ユニット、SIRENE 事務局及び Interpol の国内中央事務局によって構成されるべきである。

In order for them to be able to effectively perform their coordinating functions under this Directive, the Single Points of Contact should be composed of staff from those competent law enforcement authorities whose involvement is necessary for the adequate and rapid exchange of information under this Directive. While it is for each Member State to decide on the precise organisation and composition needed to meet that requirement, police, customs and other competent law enforcement authorities responsible for preventing, detecting or investigating criminal offences and possible contact points for regional and

bilateral offices, such as liaison officers and attachés seconded or posted in other Member States and relevant Union law enforcement agencies, such as Europol, could be represented in the Single Points of Contact. However, in the interest of effective coordination, at a minimum, the Single Points of Contact should be composed of representatives of the Europol national unit, the SIRENE Bureau and the Interpol National Central Bureau, as established by the relevant Union legal act or international agreement and notwithstanding that this Directive does not apply to the exchange of information specifically regulated by those Union legal acts.

- (30) 当該過程における機微の情報の取扱いを含め、国境を越える法執行の協力の特別の要件に鑑み、単一連絡部局及び職務権限のある法執行機関の職員が、適法、効率的かつ実効的な態様で、この指令の下にある当該職員の機能を果たすために必要となる知識及び技能をもつことが不可欠である。とりわけ、単一連絡部局の職員は、当該職員の職業上の需要と個別の背景事情に対応し、この指令に定める規定の適用のために必要な別の構成国の単一連絡部局及び職務権限のある法執行機関との間の当該職員の連絡を容易にする、欧州連合レベルと国内レベルで提供される適切かつ定期的な訓練課程の提供を受け、かつ、そこから受益することを推奨されるべきである。この点に関し、データ処理ツールと IT システムの適切な利用に対し、個人データの保護、法執行の協力及び機密情報の取扱いに特に焦点を当てて、法務及び内務の分野における欧州連合及び国内の関連する法的枠組みに関する知識の伝達に対し、そして、言語の障壁を解消することを助けるため、その言語によって当該関係する構成国の単一連絡部局が情報を交換できる旨を関係する構成国が示した言語に対し、特別の注意が払われるべきである。訓練を提供する目的のために、構成国は、それが適切なときは、欧州議会及び理事会の規則(EU) 2015/2219<sup>18</sup>によって設置された法執行訓練のための欧州連合局(CEPOL)から提供される訓練課程及び関連ツールも活用し、その職員が Europol において 1 週間過ごす可能性を検討し、そして、CEPOL 交換計画のような、欧州連合の予算から資金拠出される計画及びプロジェクトの下で行われる関連提案を活用すべきである。

Given the specific demands of cross-border law enforcement cooperation, including the handling of sensitive information in that context, it is essential for the staff of the Single Points of Contact and the competent law enforcement authorities to have the necessary knowledge and skills to carry out their functions under this Directive in a lawful, efficient and effective manner. In particular, the staff of the Single Points of Contact should be offered, and encouraged to benefit from, adequate and regular training courses, provided both at Union and at national level, which correspond to their professional needs and specific backgrounds and which facilitate their contacts with the Single Points of Contact and competent law enforcement authorities of other Member States needed for the application of the rules set out in this

---

<sup>18</sup> 法執行訓練のための欧州連合局(CEPOL)に関する、及び、理事会決定 2005/681/JHA を置き換えて廃止する欧州議会及び理事会の 2015 年 11 月 25 日の規則(EU) 2015/2219 (OJ L 319, 4.12.2015, p. 1).

Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA (OJ L 319, 4.12.2015, p. 1).

Directive. In that respect, particular attention should be paid to the proper use of data processing tools and IT systems, to imparting knowledge about the relevant Union and national legal frameworks in the area of Justice and Home Affairs, with a particular focus on the protection of personal data, law enforcement cooperation and the handling of confidential information, and to the languages in which the Member State concerned has indicated that its Single Point of Contact is able to exchange information, with a view to helping overcome language barriers. For the purpose of providing the training, Member States should also, where appropriate, make use of the training courses and relevant tools offered by the European Union Agency for Law Enforcement Training (CEPOL), established by Regulation (EU) 2015/2219 of the European Parliament and of the Council<sup>(18)</sup>, consider the possibility for the staff to spend a week at Europol, and make use of relevant offers made under programmes and projects funded by the Union budget, such as the CEPOL exchange programme.

- (31) 技術上の技能と法律上の知識に加え、相互信頼及び共通理解は、この指令の下にある効率的かつ実効的な国境を越える法執行の協力の前提条件である。共同の業務遂行を通じて獲得される人的な接触と専門知識の共有は、信頼の構築と欧州連合の共通の警察文化の発展を促進する。構成国は、別の構成国の職務権限のある法執行機関の作業手法、捜査のアプローチ及び組織構造に関する知識の移転に焦点を当てた共同訓練課程及び職員の交換も検討すべきである。

In addition to technical skills and legal knowledge, mutual trust and common understanding are prerequisites for efficient and effective cross-border law enforcement cooperation under this Directive. Personal contacts acquired through joint operations and the sharing of expertise facilitate the building of trust and the development of a common Union culture of policing. Member States should also consider joint training courses and staff exchanges which focus on the transfer of knowledge about the working methods, investigative approaches and organisational structures of competent law enforcement authorities in other Member States.

- (32) 単一連絡部局及び職務権限のある法執行機関の職員のための訓練課程への参加を増加させるため、構成国は、そのような職員に関し、特別のインセンティブも検討し得る。

To increase participation in training courses for the staff of the Single Points of Contact and the competent law enforcement authorities, Member States could also consider specific incentives for such staff.

- (33) 単一連絡部局が、この指令の下で当該単一連絡部局の個々の職務を、とりわけ、情報の交換と関連する職務を実効的かつ効率的な態様で遂行できるようにするための一定のミニマムの機能と能力をもつ単一の電子的な事件管理システムを、単一連絡部局が配置及び運用する必要がある。事件管理システムは、単一連絡部局が情報の交換を管理できるようにするワークフローシステムである。欧州議会及び理事会の規則(EU) 2019/818<sup>19</sup>によって策定されたユニバーサルメッ

---

<sup>19</sup> 警察及び法務上の協力、難民及び移民の領域における EU の情報システム間の相互運用性の枠組みを設けることに関する、並びに、規則(EU) 2018/1726、規則(EU) 2018/1862 及び規則(EU) 2019/816 を改正する

セージフォーマットの標準が事件管理システムの開発において使用されることが望ましい。

It is necessary that the Single Points of Contact deploy and operate a single electronic case management system having certain minimum functions and capabilities in order to allow them to carry out each of their tasks under this Directive in an effective and efficient manner, in particular as regards the exchange of information. The case management system is a workflow system allowing Single Points of Contact to manage the exchange of information. It is desirable that the universal message format standard established by Regulation (EU) 2019/818 of the European Parliament and of the Council<sup>(19)</sup> be used in the development of the case management system.

- (34) 指令(EU) 2016/680 に定める規定は、事件管理システム内にある個人データの処理に適用される。処理は、記録保存を含む。個人データの明確かつ実効的な保護の利益において、同指令に定める規定は、この指令の中で更に具体的に定められるべきである。とりわけ、個人データが処理される目的のために必要な期間よりも長くデータ主体の識別を許容する方式で維持されてはならないという指令(EU) 2016/680 に定める要件に関し、この指令は、個人データを含むこの指令の下で交換される情報を単一連絡部局が受領したときは、この指令の下にある当該単一連絡部局の職務を当該単一連絡部局が遂行するために必要かつ比例的な範囲内にある場合に限り、その単一連絡部局が事件管理システムの中で個人データを維持すべきことを定めるべきである。当該条件に適合しなくなったときは、単一連絡部局は、事件管理システムからその個人情報を不可逆的に消去すべきである。指令(EU) 2016/680 に定める記録保存の期限及び見直しの期限に関する規定に従い、必要かつ比例的な範囲内に限り個人データが維持されることを確保するため、単一連絡部局は、当該要件に適合し続けているか否かを定期的に見直すべきである。その目的のために、最初の見直しは、この指令の下にある情報の交換が完了した時の後、すなわち、情報の最後の項目が提供された時点または当該項目と関連する最後の通信が交換された時点から遅くとも 6 か月以内に行われるべきである。ただし、そのような見直し及び削除に関するこの指令の要件は、犯罪行為の防止、検知及び捜査に関する職務権限のある国内機関が、欧州連合法を遵守し、とりわけ、指令(EU) 2016/680 を遵守し、国内法に基づき当該構成国の国内犯罪記録の中にある個人データを維持できることに対し、影響を与えてはならない。

The rules set out in Directive (EU) 2016/680 apply to the processing of personal data in the case management system. Processing includes storage. In the interests of clarity and the effective protection of personal data, the rules set out in that Directive should be further specified in this Directive. In particular, as regards the requirement set out in Directive (EU) 2016/680 that personal data be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are

---

欧州議会及び理事会の 2019 年 5 月 20 日の規則(EU) 2019/818 (OJ L 135, 22.5.2019, p. 85).

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

processed, this Directive should specify that, where a Single Point of Contact receives information exchanged under this Directive containing personal data, the Single Point of Contact should keep the personal data in the case management system only in so far as it is necessary and proportionate for it to carry out its tasks under this Directive. Where that is no longer the case, the Single Point of Contact should irrevocably delete the personal data from the case management system. In order to ensure that the personal data is kept only for as long as necessary and proportionate, in accordance with rules concerning time limits for storage and review set out in Directive (EU) 2016/680, the Single Point of Contact should regularly review whether those requirements continue to be met. For that purpose, a first review should take place at the latest six months after an exchange of information under this Directive has concluded, that is, the moment at which the last item of information has been provided or the latest communication relating thereto has been exchanged. The requirements of this Directive regarding such review and deletion should, however, not affect the possibility for the national authorities competent for the prevention, detection and investigation of criminal offences to keep the personal data in their national criminal files under national law, in compliance with Union law, in particular Directive (EU) 2016/680.

- (35) この指令の下にある情報の交換において単一連絡部局及び職務権限のある法執行機関を補助するため、そして、構成国間における欧州の共通の警察文化を育成するため、構成国は、当該構成国の単一連絡部局及び職務権限のある法執行機関の間における実務上の協力を推進すべきである。とりわけ、理事会は、この指令の目的のための情報の交換と関連する経験及びベストプラクティスを共有するため、少なくとも年 1 回、単一連絡部局の長の会合を開催すべきである。それ以外の形態の協力は、法執行上の情報の交換に関するマニュアルを作成すること、直接または間接にアクセス可能な情報、単一連絡部局、指定された法執行機関及び言語上の体制に関する国内ファクトシートまたはそれら以外の共通手続に関する文書のとりまとめ、ワークフローと関連する困難に対処すること、関連する法的枠組みの特性に関する認識を向上させること、並びに、しかるべく、関連する単一連絡部局間の会合の開催を含めるべきである。

In order to assist Single Points of Contact and competent law enforcement authorities in the exchange of information under this Directive and to foster a common European police culture between Member States, the Member States should encourage practical cooperation among their Single Points of Contact and competent law enforcement authorities. In particular, the Council should organise meetings of the Heads of the Single Points of Contact at least on an annual basis to share experience and best practice regarding the exchange of information for the purposes of this Directive. Other forms of cooperation should include the drafting of manuals on law enforcement information exchange, the compilation of national fact sheets on directly and indirectly accessible information, Single Points of Contact, designated law enforcement authorities and language regimes, or other documents on common procedures, the addressing of difficulties regarding workflows, awareness-raising about the specificities of relevant legal frameworks and the organisation, as appropriate, of meetings between relevant Single Points of Contact.

- (36) この指令の適用に必要な監視及び評価を実現可能とするため、構成国は、この指令の実装に関する一定のデータを収集し、かつ、欧州委員会に対し、年次で提供することを要求されるべきで

ある。この要件は、とりわけ、職務権限のある法執行機関の間における関連する国境を越える情報の交換を定量化する比較データの欠如を解消するために必要であり、また、この指令の実装と関連する欧州委員会の報告義務を容易にもする。同目的のために要求されるデータは、事件管理システム及び SIENA によって、自動的に生成されるべきである。

To enable the necessary monitoring and evaluation of the application of this Directive, Member States should be required to collect and annually provide to the Commission certain data concerning the implementation of this Directive. That requirement is necessary, in particular, to remedy the lack of comparable data quantifying relevant cross-border information exchanges between competent law enforcement authorities and also facilitates the reporting obligation of the Commission regarding the implementation of this Directive. Data required for that purpose should be automatically generated by the case management system and SIENA.

- (37) 複数国にわたる犯罪及びテロリズムの国境を越える性質は、構成国に対し、そのような犯罪行為の防止、検知または捜査のために、相互に依拠することを要求する。この指令の目的、すなわち、職務権限のある法執行機関の間及び Europol に対する適切かつ迅速な情報の流れを確保することは、構成国によっては十分に達成され得ず、その活動の規模及び影響のゆえに、情報の交換に関する共通の規定と共通の文化の確立により、そして、現代のツールと通信経路により、欧州連合レベルでより良く達成され得るので、欧州連合は、欧州連合条約 (TEU) の第 5 条に定める補完性の原則に従い、措置を採択できる。同条に定める比例性の原則に従い、この指令は、当該目的を達成するために必要なところを超えることがない。

The cross-border nature of transnational crime and terrorism requires Member States to rely on one another to prevent, detect or investigate such criminal offences. Since the objective of this Directive, namely ensuring adequate and rapid information flows between competent law enforcement authorities and to Europol, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level through the establishment of common rules and a common culture on the exchange of information and through modern tools and communication channels, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

- (38) 欧州データ保護監督官は、欧州議会及び理事会の規則 (EU) 2018/1725<sup>20</sup> の第 42 条第 1 項に従

---

<sup>20</sup> 欧州連合の機関、組織、事務局及び部局による個人データの処理と関連する自然人の保護に関する並びにそのデータの支障のない移動に関する、並びに、規則 (EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則 (EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39).

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and



って意見聴取を受け、2022 年 3 月 7 日にその意見を伝達した。

The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and the Council<sup>(20)</sup> and delivered an opinion on 7 March 2022.

- (39) この指令は、TEU の第 2 条に定めるような、法の支配、自由及び民主主義を含め、それらの上に欧州連合が構築されている諸価値を基盤としている。この指令はまた、基本的な権利及び安全確保を尊重し、かつ、欧州連合基本権憲章(「憲章」)によって認められた基本原則、とりわけ、憲章の第 6 条、第 7 条及び第 8 条にそれぞれ定める自由と防護の権利、私生活と家族生活の尊重及び個人データの保護の権利を尊重し、並びに、TFEU の第 16 条に定める基本原則を尊重する。この指令の下にある個人データの処理は、厳格に必要かつ比例的なところに制限されるべきであり、かつ、明確な条件、厳格な要件、並びに、それが適切なときは、指令(EU)2016/680 によって設置された国内監督機関及び欧州データ保護監督官それぞれの権限に従った当該国内監督機関及び欧州データ保護監督官の実効的な監督に服するべきである。

This Directive builds upon the values on which the Union is founded, as set out in Article 2 TEU, including the rule of law, freedom and democracy. It also respects fundamental rights and safeguards and observes the principles recognised by the Charter of Fundamental Rights of the European Union (the ‘Charter’), in particular the right to liberty and security, the respect for private and family life and the right to the protection of personal data as provided for by Articles 6, 7 and 8 of the Charter respectively, as well as by Article 16 TFEU. Any processing of personal data under this Directive should be limited to that which is strictly necessary and proportionate and subject to clear conditions, strict requirements and effective supervision by the national supervisory authorities established by Directive (EU) 2016/680 and the European Data Protection Supervisor, where appropriate in accordance with their respective mandates.

- (40) TEU 及び TFEU に附属するデンマークの地位に関する議定書第 22 号の第 1 条及び第 2 条に従い、デンマークは、この指令の採択に参加しておらず、この指令によって拘束されることがなく、または、この指令の適用に服さない。この指令がシェンゲン協定を基礎としていることに鑑み、デンマークは、同議定書の第 4 条に従い、この指令に関して理事会が決定した後 6 か月以内に、デンマークが同国の国内法の中にこの指令を実装するかどうかを決定する。

In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application. Given that this Directive builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Directive whether it will implement it in its national law.

---

agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJL 295, 21.11.2018, p. 39).

- (41) TEU 及び TFEU に附属する欧州連合の枠組み内に統合されたシェンゲン協定に関する議定書第 19 号の第 5 条第 1 項及び理事会決定 2002/192/EC<sup>21</sup> の第 6 条第 2 項に従い、アイルランドは、この指令に参加している。

Ireland is taking part in this Directive, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the TEU and to the TFEU, and Article 6(2) of Council Decision 2002/192/EC<sup>(21)</sup>.

- (42) アイスランド及びノルウェーに関しては、この指令は、理事会決定 1999/437/EC<sup>23</sup> の第 1 条第 H 号に示す領域の範囲内にあるシェンゲン協定の実装、適用及び発展へのアイスランド共和国及びノルウェー王国の参加に関して欧州連合の理事会並びにアイスランド共和国及びノルウェー王国によって締結された協定<sup>22</sup> の意味におけるシェンゲン協定の条項の発展を構成する。

As regards Iceland and Norway, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis*<sup>(22)</sup> which fall within the area referred to in Article 1, point H, of Council Decision 1999/437/EC<sup>(23)</sup>.

- (43) スイスに関しては、この指令は、理事会決定 2008/149/JHA<sup>25</sup> の第 3 条を重畳して読み替えられる理事会決定 1999/437/EC の第 1 条第 H 号に示す領域の範囲内にあるシェンゲン協定の実装、適用及び発展へのスイス連邦の参加に関する欧州連合、欧州共同体及びスイス連邦の間の協定<sup>24</sup> の意味におけるシェンゲン協定の条項の発展を構成する。

---

<sup>21</sup> シェンゲン協定の幾つかの条項への参加のためのアイルランドの要請に関する 2002 年 2 月 28 日の理事会決定 2002/192/EC (OJ L 64, 7.3.2002, p. 20).

Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

<sup>22</sup> OJ L 176, 10.7.1999, p. 36.

<sup>23</sup> シェンゲン協定の実装、適用及び発展へのアイスランド共和国及びノルウェー王国の参加に関して欧州連合の理事会並びにアイスランド共和国及びノルウェー王国によって締結された協定の適用のための一定の覚書に関する 1999 年 5 月 17 日の理事会決定 1999/437/EC (OJ L 176, 10.7.1999, p. 31).

Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

<sup>24</sup> OJ L 53, 27.2.2008, p. 52.

<sup>25</sup> シェンゲン協定の実装、適用及び発展へのスイス連邦の参加に関する欧州連合、欧州共同体及びスイス連邦の間の協定の欧州連合に代わる締結に関する 2008 年 1 月 28 日の理事会決定 2008/149/JHA (OJ L 53, 27.2.2008, p. 50).

Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L

As regards Switzerland, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*<sup>(24)</sup> which fall within the area referred to in Article 1, point H, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/149/JHA<sup>(25)</sup>.

- (44) リヒテンシュタインに関しては、この指令は、理事会決定 2011/349/JHA<sup>27</sup> の第 3 条を重畳して読み替えられる理事会決定 1999/437/EC の第 1 条第 H 号に示す領域の範囲内にあるシェンゲン協定の実装、適用及び発展へのスイス連邦の参加に関する欧州連合、欧州共同体及びスイス連邦の間の協定へのリヒテンシュタイン公国の加入に関する欧州連合、欧州共同体、スイス連邦及びリヒテンシュタイン公国の間の議定書<sup>26</sup> の意味におけるシェンゲン協定の条項の発展を構成する、

As regards Liechtenstein, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*<sup>(26)</sup> which fall within the area referred to in Article 1, point H, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/349/EU<sup>(27)</sup>,

以上のとおりであるので、この指令を採択する:

HAVE ADOPTED THIS DIRECTIVE:

---

53, 27.2.2008, p. 50).

<sup>26</sup> OJ L 160, 18.6.2011, p. 21.

<sup>27</sup> 刑事における法務上の協力及び警察の協力と特に関連するシェンゲン協定の実装、適用及び発展へのスイス連邦の参加に関する欧州連合、欧州共同体及びスイス連邦の間の協定へのリヒテンシュタイン公国の加入に関する欧州連合、欧州共同体、スイス連邦及びリヒテンシュタイン公国の間の議定書の欧州連合に代わる締結に関する 2011 年 3 月 7 日の理事会決定 2011/349/EU (OJ L 160, 18.6.2011, p. 1).

Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

## 第 I 章 総則的な規定

### Chapter I General Provisions

#### 第 1 条 対象事項及び適用範囲

##### Article 1 Subject matter and scope

1. この指令は、犯罪行為を防止すること、検知することまたは捜査することという目的のための職務権限のある法執行機関の間における適切かつ迅速な情報の交換に関する整合化された規定を定める。

This Directive establishes harmonised rules for the adequate and rapid exchange of information between the competent law enforcement authorities for the purpose of preventing, detecting or investigating criminal offences.

とりわけ、この指令は、以下に関する規定を定める：

- (a) 構成国によって設置または指定された単一連絡部局に対して提出される情報を求める要請書、とりわけ、そのような要請書の内容に関しては、そのような要請による情報の提供、単一連絡部局の職務上の言語、要請を受けた情報を提供するための義務的な期限、及び、そのような要請を拒否する理由；
- (b) 構成国から別の構成国の単一連絡部局または職務権限のある法執行機関に対する当該構成国の自発による関連情報の提供、とりわけ、そのような情報が提供される状況及び態様；
- (c) この指令の下にある全ての情報の交換のために使用されるデフォルトの通信経路、及び、職務権限のある法執行機関の間における直接の情報の交換と関係して単一連絡部局に対して提供される情報；
- (d) この指令の下にある単一連絡部局の職務を遂行するための単一の電子的な事件管理システムの配置及び運用に関する事項を含め、各構成国の単一連絡部局の設置または指定並びに組織、職務、構成及び能力。

In particular, this Directive establishes rules on:

- (a) requests for information submitted to the Single Points of Contact established or designated by the Member States, in particular on the content of such requests, the provision of information pursuant to such requests, the working languages of the Single Points of Contact, mandatory time limits for providing requested information and the reasons for the refusal of such requests;
- (b) the provision by a Member State, on its own initiative, of relevant information to the Single Points of Contact or to the competent law enforcement authorities of other Member States, in particular the situations and the manner in which such information is to be provided;
- (c) the default channel of communication to be used for all exchanges of information under this Directive and the information to be provided to the Single Points of Contact in relation to the exchange of information directly between the competent law enforcement authorities;

(d) the establishment or designation and the organisation, tasks, composition and capabilities of each Member State's Single Point of Contact, including on the deployment and operation of a single electronic case management system for carrying out their tasks under this Directive.

2. この指令は、欧州連合の別の法行為によって個別に規律されている犯罪行為を防止すること、検知することまたは捜査することを目的とする職務権限のある法執行機関の間における情報の交換に対して適用してはならない。この指令またはそれ以外の欧州連合の法行為に基づく当該職務権限のある法執行機関の義務を妨げることなく、構成国は、二国間協定または多国間協定による場合を含め、犯罪行為を防止すること、検知することまたは捜査することを目的とする別の構成国の職務権限のある法執行機関との間の情報の交換を更に容易にする条項を採択または維持できる。

This Directive shall not apply to exchanges of information between the competent law enforcement authorities for the purpose of preventing, detecting or investigating criminal offences that are specifically regulated by other Union legal acts. Without prejudice to their obligations under this Directive or other Union legal acts, Member States may adopt or maintain provisions further facilitating the exchange of information with the competent law enforcement authorities of other Member States for the purpose of preventing, detecting or investigating criminal offences, including by means of bilateral or multilateral arrangements.

3. この指令は、構成国に対し、以下の義務を課さない:
- (a) 強制的な措置によって情報を入手すること;
  - (b) 別の構成国の職務権限のある法執行機関に対してその情報を提供することだけを目的として情報を記録保存すること;
  - (c) 法務上の手続における証拠として使用されるために、別の構成国の職務権限のある法執行機関に対して情報を提供すること。

This Directive does not impose any obligation on Member States to:

- (a) obtain information by means of coercive measures;
- (b) store information for the sole purpose of providing it to the competent law enforcement authorities of other Member States;
- (c) provide information to the competent law enforcement authorities of other Member States to be used as evidence in judicial proceedings.

4. この指令は、この指令に従って提供される情報を法務上の手続における証拠として使用する権利を創設しない。情報を提供する構成国は、法務上の手続において証拠として当該情報を使用することに対し、同意を与え得る。

This Directive does not establish any right to use the information provided in accordance with this Directive as evidence in judicial proceedings. The Member State providing the information may consent

to its use as evidence in judicial proceedings.

## 第 2 条 定義

### Article 2 Definitions

この指令の目的のために:

- (1) 「職務権限のある法執行機関」とは、国内法の下で犯罪行為を防止すること、検知することもしくは捜査することを目的とする権限を行使し、強制措置を講ずる職務権限のある構成国の警察、税関もしくはそれ以外の機関、または、犯罪行為を防止すること、検知することもしくは捜査することを目的とする複数の構成国の間で設置された共同の法主体に参加する機関のことを意味するが、国家安全保障上の問題を特に取り扱う部局またはユニット及びシェンゲン協定実装条約の第 47 条により派遣される連絡官を除外し;
- (2) 「指定された法執行機関」とは、第 4 条第 1 項に従い、別の構成国の単一連絡部局に対して情報を求める要請書を提出する権限をもつ職務権限のある法執行機関のことを意味し;
- (3) 「重大犯罪」とは、以下のいずれかのことを意味し;
  - (a) 理事会枠組み決定 2002/584/JHA<sup>28</sup>の第 2 条第 2 項に示す侵害行為;
  - (b) 規則(EU) 2016/794 の第 3 条第 1 項または第 2 項に示す侵害行為。
- (4) 「情報」とは、犯罪の情報を含め、国内法に基づき、犯罪行為を防止すること、検知することまたは捜査する職務権限のある法執行機関の職務を遂行する目的のための職務権限のある法執行機関と関連する 1 もしくは複数の自然人もしくは法人、事実または状況に関する内容のことを意味し;
- (5) 「利用可能な情報」とは、直接にアクセス可能な情報及び間接にアクセス可能な情報のことを意味し;
- (6) 「直接にアクセス可能な情報」とは、その構成国から情報が要請された構成国の単一連絡部局または職務権限のある法執行機関によって直接にアクセスされ得る、データベース内に保有されている情報のことを意味し;
- (7) 「間接にアクセス可能な情報」とは、国内法によって許容されている場合において、かつ、国内法に従い、強制的な措置なく、その構成国から情報が要請された構成国の単一連絡部局または職務権限のある法執行機関が別の行政機関からまたは当該構成国内に拠点をもつ私人から入手できる情報のことを意味し;
- (8) 「個人データ」とは、指令(EU)2016/680 の第 3 条第 1 号に定義する個人データのことを意味する。

For the purpose of this Directive:

---

<sup>28</sup> 欧州逮捕令状及び構成国間における身柄引渡手続に関する 2002 年 6 月 13 日の理事会枠組み決定 2002/584/JHA (OJ L 190, 18.7.2002, p. 1).

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

- (1) ‘competent law enforcement authority’ means any police, customs or other authority of the Member States competent under national law to exercise authority and to take coercive measures for the purpose of preventing, detecting or investigating criminal offences or any authority that takes part in joint entities set up between two or more Member States for the purpose of preventing, detecting or investigating criminal offences, but excludes agencies or units dealing especially with national security issues and liaison officers seconded pursuant to Article 47 of the Convention implementing the Schengen Agreement;
- (2) ‘designated law enforcement authority’ means a competent law enforcement authority that is authorised to submit requests for information to the Single Points of Contact of other Member States in accordance with Article 4(1);
- (3) ‘serious criminal offence’ means any of the following:
  - (a) an offence as referred to in Article 2(2) of Council Framework Decision 2002/584/JHA<sup>(28)</sup>;
  - (b) an offence as referred to in Article 3(1) or (2) of Regulation (EU) 2016/794;
- (4) ‘information’ means any content concerning one or more natural or legal persons, facts or circumstances relevant to competent law enforcement authorities for the purpose of carrying out their tasks under national law of preventing, detecting or investigating criminal offences, including criminal intelligence;
- (5) ‘information available’ means directly accessible information and indirectly accessible information;
- (6) ‘directly accessible information’ means information held in a database that can be directly accessed by the Single Point of Contact or a competent law enforcement authority of the Member State from which information is requested;
- (7) ‘indirectly accessible information’ means information that a Single Point of Contact or a competent law enforcement authority of the Member State from which information is requested can obtain from other public authorities or from private parties established in that Member State, where permitted by and in accordance with national law, without coercive measures;
- (8) ‘personal data’ means personal data as defined in Article 3, point (1), of Directive (EU) 2016/680.

### 第 3 条 情報の交換と関連する基本原則

#### Article 3 Principles regarding the exchange of information

各構成国は、この指令の下にある全ての情報の交換との関係において、以下のことを確保する:

- (a) 利用可能な情報が、別の構成国の単一連絡部局または職務権限のある法執行機関に対して提供され得る(「可用性の原則」);
- (b) 別の構成国の単一連絡部局及び職務権限のある法執行機関から情報を要請するための条件並びに別の構成国の単一連絡部局及び職務権限のある法執行機関に対して情報を提供するための条件は、当該構成国内における類似の情報の要請及び提供に適用可能な条件と均等である(「均等なアクセスの原則」);
- (c) 構成国は、当該構成国の単一連絡部局または職務権限のある法執行機関に対して提供される機密としての標識のある情報を、その情報を提供した構成国の国内法と類似するレベ

ルの機密性を提供する当該構成国の国内法に定める要件に従って保護する(「機密性の原則」);

- (d) 要請を受けた情報が別の構成国からまたは第三国から最初に入手された場合、構成国は、その情報を最初に提供した構成国または第三国の同意があり、かつ、当該構成国または第三国によってその情報の利用に関して加えられた条件に従う場合に限り、別の構成国または Europol に対し、そのような情報を提供する(「データの保有の原則」);
- (e) この指令の下で交換され、不正確、不完全または最新ではないと判断された個人データは、消去または訂正され、または、当該データの処理は、しかるべく制限され、かつ、その受領者は、遅滞なく通知を受ける(「データの信頼性の原則」)。

Each Member State shall, in connection with all exchanges of information under this Directive, ensure that:

- (a) information available can be provided to the Single Point of Contact or the competent law enforcement authorities of other Member States ('principle of availability');
- (b) the conditions for requesting information from and providing information to the Single Points of Contact and the competent law enforcement authorities of other Member States are equivalent to those applicable for requesting and providing similar information within that Member State ('principle of equivalent access');
- (c) it protects information provided to its Single Point of Contact or competent law enforcement authorities that is marked as confidential in accordance with the requirements set out in its national law offering a similar level of confidentiality as the national law of the Member State that provided the information ('principle of confidentiality');
- (d) where the requested information was initially obtained from another Member State or a third country, it only provides such information to another Member State or to Europol with the consent of, and in accordance with the conditions imposed on its use by, the Member State or third country that initially provided the information ('principle of data ownership');
- (e) personal data exchanged under this Directive that are found to be inaccurate, incomplete or no longer up to date are erased or rectified or that their processing is restricted, as appropriate, and that any recipient is notified without delay ('principle of data reliability').



## 第 II 章 単一連絡部局を介する情報の交換

### Chapter II Exchange of Information through Single Points of Contact

#### 第 4 条 単一連絡部局に対する情報を求める要請

##### Article 4 Requests for information to Single Points of Contact

1. 構成国は、当該構成国の単一連絡部局から、及び、当該構成国の国内法がそのように定めているときは、指定された法執行機関から、別の構成国の単一連絡部局に対して提出される情報を求める要請が、第 2 項ないし第 6 項に定める要件を遵守することを確保する。

Member States shall ensure that requests for information submitted by their Single Point of Contact and, where their national law so provides, the designated law enforcement authorities to the Single Point of Contact of another Member State comply with the requirements set out in paragraphs 2 to 6.

構成国は、欧州委員会に対し、当該構成国の指定された法執行機関のリストを提出する。構成国は、欧州委員会に対し、当該リストに対する変更が存在するときは、連絡する。欧州委員会は、それらのリストをとりまとめたものをオンラインで公表し、かつ、それを最新のものに保つ。

Member States shall submit to the Commission a list of their designated law enforcement authorities. Member States shall inform the Commission where there are changes to that list. The Commission shall publish online a compilation of those lists and keep it up to date.

構成国は、当該構成国の指定された法執行機関が別の構成国の単一連絡部局に対して情報を求める要請書を提出するときは、同時に、当該指定された法執行機関が、当該構成国の単一連絡部局に対して当該要請書のコピーを送付することを確保する。

Member States shall ensure that where their designated law enforcement authorities submit a request for information to the Single Point of Contact of another Member State, at the same time, they send a copy of that request to their Single Point of Contact.

2. 構成国は、その送信が以下の 1 または複数のことを危険に晒すような場合においては、当該構成国の指定された法執行機関が、ケースバイケースで、第 1 項に従って、別の構成国の単一連絡部局に対する情報を求める要請書の提出と同時に、当該情報を求める要請書のコピーを当該構成国の単一連絡部局に対して送付しないことを認め得る：
  - (a) 情報の処理が適切なレベルの機密性を要求する現在進行中の高度に機微な捜査;
  - (b) 緊急の状況または危機管理の状況を含まないテロリズム案件;
  - (c) 個人の安全。

Member States may permit their designated law enforcement authorities not to send, on a case-by-case

basis, a copy of a request for information to their Single Point of Contact at the same time as submitting it to the Single Point of Contact of another Member State in accordance with paragraph 1 where it would jeopardise one or more of the following:

- (a) an ongoing highly sensitive investigation for which the processing of information requires an appropriate level of confidentiality;
- (b) terrorism cases not involving emergency or crisis management situations;
- (c) the safety of an individual.

3. 構成国は、以下のことを信ずる客観的な理由が存在する場合に限り、情報を求める要請書が別の構成国の単一連絡部局に対して提出されることを確保する:

- (a) 要請される情報が、第 1 条第 1 項第 1 副項に示す目的を達成するために必要かつ比例的である;かつ
- (b) 要請される情報が、当該別の構成国にとって利用可能である。

Member States shall ensure that requests for information are submitted to the Single Point of Contact of another Member State only where there are objective reasons to believe that:

- (a) the requested information is necessary for and proportionate to achieving the purpose referred to in Article 1(1), first subparagraph; and
- (b) the requested information is available to that other Member State.

4. 構成国は、別の構成国の単一連絡部局に対して提出される情報を求める要請書が、緊急であるか否かを示し、かつ、そうであるときは、緊急であること理由を与えることを確保する。そのような情報を求める要請は、当の案件の全ての関連する事実及び状況を考慮に入れた上で、要請される情報が以下の 1 または複数であると信ずる客観的な理由が存在するときは、緊急であると判断される:

- (a) 構成国の公共の保安に対する差し迫った重大な脅威の防止のために不可欠な情報;
- (b) 個人の生命または身体の完全性に対する差し迫った脅威を防止するために必要な情報;
- (c) 自由の剥奪に該当する制限措置の維持を含み得る決定を採択するために必要な情報;
- (d) もし緊急に提供されなければ情報としての関連性を喪失する差し迫った危険性があり、かつ、犯罪行為の防止、検知または捜査のために重要であると判断される情報。

Member States shall ensure that any request for information submitted to the Single Point of Contact of another Member State specifies whether it is urgent and, if so, gives reasons for the urgency. Such requests for information shall be considered urgent where, having regard to all relevant facts and circumstances of the case at hand, there are objective reasons to believe that the requested information is one or more of the following:

- (a) essential for the prevention of an immediate and serious threat to the public security of a Member State;
- (b) necessary in order to prevent an imminent threat to life or the physical integrity of a person;
- (c) necessary to adopt a decision that might involve the maintenance of restrictive measures amounting

- to a deprivation of liberty;
- (d) at imminent risk of losing relevance if not provided urgently and is considered important for the prevention, detection or investigation of criminal offences.
5. 構成国は、別の構成国の単一連絡部局に対して提出される情報を求める要請書が、少なくとも以下の事項を含め、当該情報をこの指令に従って適切かつ迅速に処理できるようにするために必要となる全ての詳細情報を含むことを確保する:
- (a) 当の状況の下において合理的に可能な詳細さによる、要請される情報の特定;
  - (b) 事実の記述及び基礎となっている侵害行為の適示を含め、その情報が求められる目的の記述;
  - (c) 要請される情報が要請先構成国にとって利用可能であると信ずる客観的な理由;
  - (d) それが適用されるときは、その情報が要請される目的と、その情報と関係する自然人もしくは法人または法主体との間の関係性の説明;
  - (e) それが適用可能なときは、第 4 項に従い、その要請が緊急であると判断される理由;
  - (f) 当該要請書が提出された目的以外の目的のためのその要請書の中に含まれている情報の利用の制限。

Member States shall ensure that requests for information submitted to the Single Point of Contact of another Member State contain all necessary details to allow for their adequate and rapid processing in accordance with this Directive, including at least the following:

- (a) a specification of the requested information that is as detailed as reasonably possible under the given circumstances;
  - (b) a description of the purpose for which the information is requested, including a description of the facts and indication of the underlying offence;
  - (c) the objective reasons for which it is believed that the requested information is available to the requested Member State;
  - (d) an explanation of the connection between the purpose for which the information is requested and any natural or legal person or entity to which the information relates, where applicable;
  - (e) the reasons for which the request is considered urgent, where applicable, in accordance with paragraph 4;
  - (f) restrictions on the use of the information contained in the request for purposes other than those for which it has been submitted.
6. 構成国は、情報を求める要請書が、第 11 条に従って当該別の構成国によって作成されるリストに含まれている言語中の 1 つにより、別の構成国の単一連絡部局に対して提出されることを確保する。

Member States shall ensure that requests for information are submitted to the Single Point of Contact of another Member State in one of the languages included in the list established by that other Member State in accordance with Article 11.

## 第 5 条 単一連絡部局に対する要請による情報の提供

### Article 5 Provision of information pursuant to requests to Single Points of Contact

1. 構成国は、当該構成国の単一連絡部局が、可能な限り速やかに、かつ、いかなる場合であっても、しかるべく以下の期限内に、第 4 条に従って要請を受けた情報を提供することを確保する:
  - (a) 直接にアクセス可能な情報に関して、緊急の要請の場合においては、8 時間;
  - (b) 間接にアクセス可能な情報に関して、緊急の要請の場合においては、3 暦日;
  - (c) 上記以外の全ての要請の場合においては、7 暦日。

Member States shall ensure that their Single Point of Contact provides the information requested in accordance with Article 4 as soon as possible and in any event within the following time limits, as applicable:

- (a) eight hours in the case of urgent requests relating to directly accessible information;
- (b) three calendar days in the case of urgent requests relating to indirectly accessible information;
- (c) seven calendar days in the case of all other requests.

第 1 副項に定める期限は、情報を求める要請を受理した時に直ちにその進行を開始する。

The time limits set out in the first subparagraph shall commence as soon as the request for information is received.

2. 第 9 条に従った当該構成国の国内法の下において、法務上の許可を得た後に限り要請を受けた情報を構成国が提供できる場合、当該構成国は、そのような許可を得る目的のために必要な範囲内において、本条の第 1 項に定める期限の適用を免れ得る。そのような場合において、構成国は、当該構成国の単一連絡部局が、以下のいずれのことも行うことを確保する:
  - (a) 要請元構成国の単一連絡部局に対し、または、それが適用可能なときは、要請元構成国の指定された法執行機関に対し、予想される遅延の期間及び当該遅延の理由を示して、予想される遅延を直ちに連絡する;
  - (b) 要請元構成国の単一連絡部局に対し、または、それが適用可能なときは、要請元構成国の指定された法執行機関に対し、その後もアップデートされることを維持し、かつ、法務上の許可を得た後可能な限り速やかに、要請された情報を提供する。

Where, under its national law in accordance with Article 9, a Member State can provide the requested information only after having obtained a judicial authorisation, that Member State may deviate from the time limits set out in paragraph 1 of this Article in so far as necessary for the purpose of obtaining such an authorisation. In such cases, Member States shall ensure that their Single Point of Contact does both of the following:

- (a) immediately inform the Single Point of Contact or, where applicable, the designated law enforcement authority of the requesting Member State of the expected delay, specifying the length of the expected delay and the reasons therefor;

- (b) subsequently keep the Single Point of Contact, or where applicable, the designated law enforcement authority of the requesting Member State updated and provide the requested information as soon as possible after obtaining the judicial authorisation.
3. 構成国は、当該構成国の単一連絡部局が、要請元構成国の単一連絡部局に対し、または、それが適用可能なときは、要請元構成国の指定された法執行機関に対し、その言語によって第 4 条第 6 項に従って提出された情報を求める当該要請書が提出された言語により、第 4 条に従って要請された情報を提供することを確保する。

Member States shall ensure that their Single Point of Contact provides the information requested in accordance with Article 4 to the Single Point of Contact or, where applicable, the designated law enforcement authority of the requesting Member State in the language in which that request for information was submitted in accordance with Article 4(6).

構成国は、当該構成国の単一連絡部局が、要請元構成国の単一連絡部局に対し、同構成国の指定された法執行機関に対する要請された情報の提供と同時に、要請された情報のコピーを送付することを確保する。

Member States shall ensure that their Single Point of Contact sends a copy of the requested information to the Single Point of Contact of the requesting Member State at the same time as providing the requested information to the designated law enforcement authority of that Member State.

構成国は、その送信が以下の 1 または複数のことを危険に晒すような場合においては、当該構成国の単一連絡部局が、本条に従って、別の構成国の指定された法執行機関に対する情報の提供と同時に、当該情報のコピーを当該別の構成国の単一連絡部局に対して送付しないことを認め得る：

- (d) 情報の処理が適切なレベルの機密性を要求する現在進行中の高度に機微な捜査；
- (e) 緊急の状況または危機管理の状況を含まないテロリズム案件；
- (f) 個人の安全。

Member States may permit their Single Point of Contact not to send, at the same time as providing information to the designated law enforcement authorities of another Member State in accordance with this Article, a copy of that information to the Single Point of Contact of that other Member State where it would jeopardise one or more of the following:

- (a) an ongoing highly sensitive investigation for which the processing of information requires an appropriate level of confidentiality;
- (b) terrorism cases not involving emergency or crisis management situations;
- (c) the safety of an individual.

## 第 6 条 情報を求める要請の拒否

### Article 6 Refusals of requests for information

1. 構成国は、当該構成国の単一連絡部局が、以下のいずれかの理由が適用される範囲内にある場合に限り、第 4 条に従って要請された情報の提供を拒否することを確保する:
  - (a) 要請先構成国の単一連絡部局及び職務権限のある法執行機関にとって、要請を受けた情報が利用可能ではない;
  - (b) 情報を求める要請が第 4 条に定める要件に適合していない;
  - (c) 第 9 条に従って要請先構成国の国内法の下で要求される法務上の許可が拒否された;
  - (d) 要請された情報が、第 10 条(b)に示す類型の個人データの範囲外の個人データを組成する;
  - (e) 要請された情報が、不正確、不完全または最新ではないと判断されたものであり、かつ、指令(EU) 2016/680 の第 7 条第 2 項に従って提供され得ない;
  - (f) 要請された情報の提供が:
    - (i) 要請先構成国の国家安全保障上の必須の利益と反する、または、その利益を危険に晒す;
    - (ii) 現在進行中の犯罪行為の捜査の成功もしくは個人の安全を危険に晒す;
    - (iii) 法人の保護された重要な利益を不適切に侵害する;  
ようだと信ずる客観的な理由が存在する;
  - (g) その要請が:
    - (i) 要請先構成国の法律の下において、その長期が 1 年以下の拘禁刑によって処罰され得る犯罪行為;または
    - (ii) 要請先構成国の法律の下において、犯罪行為ではない事柄;  
と関係している;
  - (h) 要請された情報が、別の構成国または第三国から最初に入手されたものであり、かつ、当該構成国または第三国がその情報の提供に同意しなかった。

Member States shall ensure that their Single Point of Contact only refuses to provide the information requested in accordance with Article 4 in so far as any of the following reasons applies:

- (a) the requested information is not available to the Single Point of Contact and the competent law enforcement authorities of the requested Member State;
- (b) the request for information does not meet the requirements set out in Article 4;
- (c) the judicial authorisation required under the national law of the requested Member State in accordance with Article 9 was refused;
- (d) the requested information constitutes personal data other than those falling within the categories of personal data referred to in Article 10, point (b);
- (e) the requested information has been found to be inaccurate, incomplete or no longer up to date and cannot be provided in accordance with Article 7(2) of Directive (EU) 2016/680;
- (f) there are objective reasons to believe that the provision of the requested information would:
  - (i) be contrary to or would harm the essential interests of the national security of the requested

- Member State;
- (ii) jeopardise the success of an ongoing investigation of a criminal offence or the safety of an individual;
  - (iii) unduly harm the protected important interests of a legal person;
- (g) the request pertains to:
- (i) a criminal offence punishable by a maximum term of imprisonment of one year or less under the law of the requested Member State; or
  - (ii) a matter that is not a criminal offence under the law of the requested Member State;
- (h) the requested information was initially obtained from another Member State or a third country and that Member State or third country has not consented to the provision of the information.

構成国は、当該構成国の単一連絡部局に対して提出された情報を求める要請書が第 4 条に定める要件に従っているかどうかの評価において、とりわけ、基本的な権利の明白な侵害があるかどうかに関して、デューデリジエンスを実施する。

Member States shall exercise due diligence in assessing whether the request for information submitted to their Single Point of Contact is in accordance with the requirements set out in Article 4, in particular as to whether there is a manifest breach of fundamental rights.

情報を求める要請の拒否は、第 1 副項に定める理由と関係する部分に限定して影響するものとし、かつ、それが適用可能なときは、この指令に従って残余の部分の情報を提供すべき義務に対しては影響を及ぼさない。

Any refusal of a request for information shall affect only the part of the requested information to which the reasons set out in the first subparagraph relate and shall, where applicable, not affect the obligation to provide the other parts of the information in accordance with this Directive.

2. 構成国は、当該構成国の単一連絡部局が、要請元構成国の単一連絡部局、または、それが適用可能なときは、要請元構成国の指定された法執行機関に対し、第 5 条第 1 項に定める期限内に、当該拒否の理由を示して、情報を求める要請の拒否を連絡することを確保する。

Member States shall ensure that their Single Point of Contact informs the Single Point of Contact or, where applicable, the designated law enforcement authority of the requesting Member State of the refusal of the request for information, specifying the reasons therefor, within the time limits set out in Article 5(1).

3. それに関連するときは、構成国は、当該構成国の単一連絡部局が、直ちに、要請元構成国の単一連絡部局、または、それが適用可能なときは、要請元構成国の指定された法執行機関に対し、その明確化または特定がなければ拒否されなければならないような情報を求める要請の処理のために必要な明確化または特定を要請することを確保する。

Where relevant, Member States shall ensure that their Single Point of Contact immediately requests, from the Single Point of Contact or, where applicable, the designated law enforcement authority of the requesting Member State, clarification or specifications needed to process a request for information that otherwise would have to be refused.

第 5 条第 1 項に定める期限は、要請元構成国の単一連絡部局、または、それが適用可能なときは、要請元構成国の指定された法執行機関が明確化または特定を求める要請を受けた時から、要請された明確化または特定が提供される時まで、進行を停止する。

The time limits set out in Article 5(1) shall be suspended from the moment that the Single Point of Contact or, where applicable, the designated law enforcement authority of the requesting Member State receives the request for clarification or specifications until the moment the requested clarification or specifications are provided.

4. 情報を求める要請の拒否、そのような拒否の理由、本条の第 3 項に示す明確化または特定を求める要請及び明確化または特定、並びに、それら以外の、別の構成国の単一連絡部局に対して提出された情報を求める要請書と関連する通信は、その言語によって第 4 条第 6 項に従って当該要請書が提出された言語により、送信される。

Refusals of requests for information, reasons for such refusals and requests for clarification or specifications and clarification or specifications as referred to in paragraph 3 of this Article, as well as any other communications relating to the requests for information submitted to the Single Point of Contact of another Member State, shall be transmitted in the language in which that request was submitted in accordance with Article 4(6).



### 第III章 それ以外の情報の交換

#### Chapter III Other Exchanges of Information

#### 第7条 自発による情報の提供

##### Article 7 Own-initiative provision of information

1. 犯罪行為を防止すること, 検知することまたは捜査することという目的のためにそのような情報が当該別の構成国と関連し得ると信ずる客観的な理由が存在するときは, 構成国は, 当該構成国の単一連絡部局を介して, または, 当該構成国の職務権限のある法執行機関を介して, 当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関にとって利用可能な情報を, 当該構成国の自発により, 別の構成国の単一連絡部局または職務権限のある法執行機関に対して提供できる。

Member States may provide, on their own initiative, through their Single Point of Contact or through their competent law enforcement authorities, information available to it or them to the Single Points of Contact or to the competent law enforcement authorities of other Member States where there are objective reasons to believe that such information could be relevant to those other Member States for the purpose of preventing, detecting or investigating criminal offences.

2. 構成国は, 犯罪行為を防止すること, 検知することまたは捜査することという目的のためにそのような情報が当該別の構成国と関連し得ると信ずる客観的な理由が存在するときは, 当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関が, 当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関にとって利用可能な情報を, 当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関の自発により, 別の構成国の単一連絡部局または職務権限のある法執行機関に対して提供することを確保する。ただし, そのような情報との関係において第6条第1項(c)または(f)に示す理由が適用される範囲内においては, そのような義務は存在しない。

Member States shall ensure that their Single Point of Contact or their competent law enforcement authorities provide, on its or their own initiative, information available to it or them to the Single Points of Contact or to the competent law enforcement authorities of other Member States where there are objective reasons to believe that such information could be relevant to those other Member States for the purpose of preventing, detecting or investigating serious criminal offences. However, no such obligation shall exist in so far as the reasons referred to in Article 6(1), point (c) or (f), apply in respect of such information.

3. 構成国は, 当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関が, 当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関の自発により, 第1項または第2項に従って, 別の構成国の単一連絡部局に対し情報を提供する場合, 第11条に従っ

て当該別の構成国によって作成されるリストの中に含まれている言語中の 1 つにより、そのようにすることを確保する。

Member States shall ensure that, where their Single Point of Contact or their competent law enforcement authorities provide information on its or their own initiative to the Single Point of Contact of another Member State in accordance with paragraph 1 or 2, they do so in one of the languages included in the list established by that other Member State in accordance with Article 11.

構成国は、当該構成国の単一連絡部局が、当該単一連絡部局の自発により、別の構成国の職務権限のある法執行機関に対して情報を提供する場合、当該単一連絡部局が、同時に、当該情報のコピーを、当該別の構成国の単一連絡部局に対して送付することを確保する。

Member States shall ensure that, where their Single Point of Contact provides information on its own initiative to the competent law enforcement authority of another Member State, it sends, at the same time, a copy of that information to the Single Point of Contact of that other Member State.

構成国は、当該構成国の職務権限のある法執行機関が、当該職務権限のある法執行機関の自発により、別の構成国に対して情報を提供する場合、当該職務権限のある法執行機関が、同時に、当該情報のコピーを、当該構成国の単一連絡部局に対し、及び、それが適切なときは、当該別の構成国の単一連絡部局に対し、送付することを確保する。

Member States shall ensure that, where their competent law enforcement authorities provide information on their own initiative to another Member State, they send, at the same time, a copy of that information to the Single Point of Contact of their Member State and, where appropriate, to the Single Point of Contact of that other Member State.

4. 構成国は、その送信が以下の 1 または複数のことを危険に晒すような場合においては、当該構成国の職務権限のある法執行機関が、本条に従って、別の構成国の単一連絡部局または職務権限のある法執行機関に対する情報の提供と同時に、当該情報のコピーを当該構成国の単一連絡部局または当該別の構成国の単一連絡部局に対して送付しないことを認め得る：
- (a) 情報の処理が適切なレベルの機密性を要求する現在進行中の高度に機微な捜査；
  - (b) 緊急の状況または危機管理の状況を含まないテロリズム案件；
  - (c) 個人の安全。

Member States may permit their competent law enforcement authorities not to send, at the same time as providing information to the Single Point of Contact or the competent law enforcement authorities of another Member State in accordance with this Article, a copy of that information to the Single Point of Contact of their Member State or to the Single Point of Contact of that other Member State where it would jeopardise one or more of the following:

- (a) an ongoing highly sensitive investigation for which the processing of information requires an

- appropriate level of confidentiality;
- (b) terrorism cases not involving emergency or crisis management situations;
- (c) the safety of an individual.

## 第 8 条 職務権限のある法執行機関に対して直接に提出された要請に応じる情報の交換

### Article 8 The exchange of information upon requests submitted directly to competent law enforcement authorities

1. 構成国は、当該構成国の単一連絡部局が、別の構成国の職務権限のある法執行機関に対して直接に情報を求める要請書を提出する場合、当該単一連絡部局が、同時に、当該要請書のコピーを、当該別の構成国の単一連絡部局に対して送付することを確保する。構成国は、当該構成国の職務権限のある法執行機関中のいずれかがそのような要請により情報を提供する場合、当該職務権限のある法執行機関が、同時に、当該情報のコピーを、当該職務権限のある法執行機関の構成国の単一連絡部局に対して送付することを確保する。

Member States shall ensure that, where their Single Point of Contact submits a request for information directly to a competent law enforcement authority of another Member State, at the same time, it sends a copy of that request to the Single Point of Contact of that other Member State. Member States shall ensure that, where one of their competent law enforcement authorities provides information pursuant to such a request, it sends, at the same time, a copy of that information to the Single Point of Contact of its Member State.

2. 構成国は、当該構成国の職務権限のある法執行機関中のいずれかが、別の構成国の職務権限のある法執行機関に対して直接に、情報を求める要請書を提出する場合またはそのような要請により情報を提供する場合、当該職務権限のある法執行機関が、同時に、当該要請書のコピーまたは当該情報のコピーを、当該職務権限のある法執行機関の構成国の単一連絡部局及び当該別の構成国の単一連絡部局に対して送付することを確保する。

Member States shall ensure that, where one of their competent law enforcement authorities submits a request for information or provides information pursuant to such a request directly to a competent law enforcement authority of another Member State, at the same time, it sends a copy of that request or that information to the Single Point of Contact of its Member State and to the Single Point of Contact of that other Member State.

3. 構成国は、その送信が以下の 1 または複数のことを危険に晒すような場合においては、第 1 項または第 2 項に示す要請書のコピーまたは情報のコピーを送付しないことを認め得る:
  - (a) 情報の処理が適切なレベルの機密性を要求する現在進行中の高度に機微な捜査;
  - (b) 緊急の状況または危機管理の状況を含まないテロリズム案件;
  - (c) 個人の安全。

Member States may permit their Single Point of Contact or competent law enforcement authorities not to send copies of requests or information as referred to in paragraph 1 or 2 where it would jeopardise one or more of the following:

- (a) an ongoing highly sensitive investigation for which the processing of information requires an appropriate level of confidentiality;
- (b) terrorism cases not involving emergency or crisis management situations;
- (c) the safety of an individual.

## 第IV章 第II章及び第III章に基づく情報の提供に関する付加的な規定

### Chapter IV Additional Rules on the Provision of Information under Chapters II and III

#### 第9条 法務上の許可

##### Article 9 Judicial authorisation

1. 構成国は、当該構成国の国内法が、当該構成国内において類似の情報を提供するためにそのような法務上の許可を要求しない場合、第II章または第III章の下において別の構成国の単一連絡部局または職務権限のある法執行機関に対して情報を提供するために、法務上の許可を要求してはならない。

A Member State shall not require a judicial authorisation in order to provide information to the Single Point of Contact or to the competent law enforcement authorities of other Member States under Chapter II or III where its national law does not require such a judicial authorisation for providing similar information within that Member State.

2. 構成国は、第II章または第III章の下において別の構成国の単一連絡部局または職務権限のある法執行機関に対して情報を提供するために当該構成国の国内法の下において法務上の許可が要求される場合、当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関が、直ちに、当該構成国の国内法に従い、可能な限り速やかにそのような法務上の許可を得るために必要となる全ての手立てを講じることを確保する。

Member States shall ensure that, where a judicial authorisation is required under their national law in order to provide information to the Single Point of Contact or to the competent law enforcement authorities of other Member States under Chapter II or III, their Single Point of Contact or their competent law enforcement authorities immediately take all the necessary steps, in accordance with their national law, to obtain such a judicial authorisation as soon as possible.

3. 第2項に示す法務上の許可の要請は、職務権限のある法務当局の構成国の国内法に従って評価され、かつ、判断される。

Requests for judicial authorisation as referred to in paragraph 2 shall be assessed and decided upon in accordance with the national law of the Member State of the competent judicial authority.

#### 第10条 個人データを組成する情報に関する付加的な規定

##### Article 10 Additional rules for information constituting personal data

構成国は、第II章または第III章の下において、当該構成国の単一連絡部局または当該構成国

の職務権限のある法執行機関が、個人データを組成する情報を提供する場合:

- (a) 指令(EU) 2016/680 の第 7 条第 2 項に従い、その個人データが、正確であり、完全であり、かつ、最新であること;
- (b) データ主体の類型毎に定められた個人データの類型が、規則(EU) 2016/794 の別紙 II のセクション B に列挙するデータ主体の類型毎に定められた個人データの類型の制限内にあること、及び、その要請の目的を達成するために必要であり、かつ、比例的であること;
- (c) 当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関が、同時にかつ可能な範囲内において、その個人データの正確性、完全性及び信頼性の程度並びにその個人データが最新のものである範囲を、別の構成国の単一連絡部局または職務権限のある法執行機関が評価できるようにするために必要となる要素も提供すること;

を確保する。

Member States shall ensure that, where their Single Point of Contact or their competent law enforcement authorities provide information under Chapter II or III that constitutes personal data:

- (a) the personal data are accurate, complete and up to date, in accordance with Article 7(2) of Directive (EU) 2016/680;
- (b) the categories of personal data provided per category of data subject remain limited to those listed in Section B of Annex II to Regulation (EU) 2016/794 and are necessary for and proportionate to achieving the purpose of the request;
- (c) their Single Point of Contact or their competent law enforcement authorities also provide, at the same time and in so far as possible, the necessary elements enabling the Single Point of Contact or the competent law enforcement authority of the other Member State to assess the degree of accuracy, completeness and reliability of the personal data and the extent to which the personal data are up to date.

## 第 11 条 言語のリスト

### Article 11 List of languages

1. 構成国は、その言語によって当該構成国の単一連絡部局が情報を交換できる 1 または複数の言語を示すリストを作成し、かつ、最新のものに保つ。同リストは、英語を含めるものとする。

Member States shall establish and keep up to date a list indicating one or more of the languages in which their Single Point of Contact is able to exchange information. That list shall include English.

2. 構成国は、欧州委員会に対し、第 1 項に示すリスト及び同リストのアップデートを提供する。欧州委員会は、それらのリストをとりまとめたものをオンラインで公表し、かつ、それを最新のものに保つ。

Member States shall provide the list referred to in paragraph 1 and any updates thereto to the Commission.

The Commission shall publish online a compilation of those lists and keep it up to date.

## 第 12 条 Europol に対する情報の提供

### Article 12 Provision of information to Europol

1. 構成国は、この指令の第 II 章または第 III 章の下において、当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関が、情報を求める要請書を送付する場合、そのような要請により情報を提供する場合、または、当該単一連絡部局もしくは当該職務権限のある法執行機関の自発により情報を提供する場合、当該単一連絡部局もしくは当該職務権限のある法執行機関の職員が、ケースバイケースで、かつ、規則(EU) 2016/794 の第 7 条第 7 項に服して、その通信と関連する情報が規則(EU) 2016/794 の第 3 条に定める Europol の目的の適用範囲内にある犯罪行為と関係する範囲内において、情報を求める要請書のコピーまたは提供された情報のコピーを Europol に対して送付する必要があるかどうかを評価することも確保する。

Member States shall ensure that, where their Single Point of Contact or their competent law enforcement authorities send requests for information, provide information pursuant to such requests or provide information on its or their own initiative under Chapter II or III of this Directive, the staff of their Single Point of Contact or competent law enforcement authorities also assess, on a case-by-case basis and subject to Article 7(7) of Regulation (EU) 2016/794, whether it is necessary to send a copy of the request for information or of the information provided to Europol, in so far as the information to which the communication relates concerns criminal offences falling within the scope of the objectives of Europol set out in Article 3 of Regulation (EU) 2016/794.

2. 構成国は、本条の第 1 項により、情報を求める要請書のコピーまたは提供された情報のコピーが Europol に対して送付される場合、規則(EU) 2016/794 の第 19 条により、情報の処理の目的及び当該処理に対してあり得る制限が Europol に対して適正に通知されることを確保する。構成国は、別の構成国または第三国から最初に入手された情報が、当該別の構成国または当該第三国がその同意を与えた場合に限り、本条の第 1 項により Europol に対して送付されることを確保する。

Member States shall ensure that, where a copy of a request for information or a copy of information is sent to Europol pursuant to paragraph 1 of this Article, the purposes of the processing of the information and any possible restrictions to that processing pursuant to Article 19 of Regulation (EU) 2016/794 are duly communicated to Europol. Member States shall ensure that information initially obtained from another Member State or a third country is sent to Europol pursuant to paragraph 1 of this Article only where that other Member State or that third country has given its consent.

### 第 13 条 安全な通信経路

#### Article 13 Secure communication channel

1. 構成国は、第 II 章もしくは第 III 章の下においてまたは第 12 条の下において、当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関が、情報を求める要請書を送付するため、そのような要請により情報を提供するため、または、当該単一連絡部局もしくは当該職務権限のある法執行機関の自発により情報を提供するため、Europol の安全な情報交換ネットワークアプリケーション(SIENA)を使用することを確保する。

Member States shall ensure that their Single Point of Contact or their competent law enforcement authorities use Europol's Secure Information Exchange Network Application (SIENA) to send requests for information, to provide information pursuant to such requests or to provide information on its or their own initiative under Chapter II or III or under Article 12.

2. 構成国は、第 II 章もしくは第 III 章の下においてまたは第 12 条の下において、以下の 1 または複数の場合に該当するときは、当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関が、情報を求める要請書を送付するため、そのような要請により情報を提供するため、または、当該単一連絡部局もしくは当該職務権限のある法執行機関の自発により情報を提供するために SIENA を使用しないことを認め得る:
  - (a) Interpol の通信経路を介する場合を含め、その情報の交換が、第三国もしくは国際機関の関与を要求する場合、または、後の段階において、そのような関与が要求されると信ずる客観的な理由が存在する場合;
  - (b) 情報を求める要請の緊急性が、別の通信経路の一時的な使用を要求する場合;
  - (c) 予想外の技術上または運用上のインシデントが、当該構成国の単一連絡部局または当該構成国の職務権限のある法執行機関による情報の交換のための SIENA の使用を妨げている場合。

Member States may permit their Single Point of Contact or their competent law enforcement authorities not to use SIENA to send requests for information, to provide information pursuant to such requests or to provide information on its or their own initiative under Chapter II or III or under Article 12 in one or more of the following cases:

- (a) the exchange of information requires the involvement of third countries or international organisations or there are objective reasons to believe that such involvement will be required at a later stage, including through the Interpol communication channel;
  - (b) the urgency of the request for information requires the temporary use of another communication channel;
  - (c) an unexpected technical or operational incident prevents their Single Point of Contact or their competent law enforcement authorities from using SIENA to exchange the information.
3. 構成国は、当該構成国の単一連絡部局、及び、この指令の下にある情報の交換に関与すること



があり得る当該構成国の全ての職務権限のある法執行機関が、それが適切なときは、モバイル機器を介する場合を含め、SIENA と直接に接続されることを確保する。

Member States shall ensure that their Single Point of Contact, and all their competent law enforcement authorities that might be involved in the exchange of information under this Directive, are directly connected to SIENA, including, where appropriate, through mobile devices.

## 第 V 章 構成国間における情報の交換のための単一連絡部局

### Chapter V Single Point of Contact for the Exchange of Information between Member States

#### 第 14 条 単一連絡部局の設置または指定及び職務と能力

#### Article 14 Establishment or designation and tasks and capabilities of Single Points of Contact

1. 各構成国は、単一連絡部局を設置または指定する。単一連絡部局は、この指令の下にある情報の交換を調整すること及び容易にすることに関する職責を負う拠点法主体となる。

Each Member State shall establish or designate a Single Point of Contact. The Single Point of Contact shall be the central entity responsible for coordinating and facilitating the exchange of information under this Directive.

2. 構成国は、当該構成国の単一連絡部局が、少なくとも以下の全ての職務を遂行するための資源を具備し、かつ、その権限をもつことを確保する：
  - (a) 第 11 条第 2 項により通知された言語により、第 4 条に従って提出された情報を求める要請書を受理すること及び評価すること；
  - (b) 関連する職務権限のある法執行機関に対して情報を求める要請書を転送すること、及び、それが必要なときは、当該職務権限のある法執行機関の間において、そのような要請の処理及びそのような要請による情報の提供を調整すること；
  - (c) 別の構成国の単一連絡部局に対し、または、それが適用可能なときは、別の構成国の職務権限のある法執行機関に対し、情報を提供するため、情報の分析及び構成を調整すること；
  - (d) 要請に応じて、または、当該単一連絡部局の自発により、第 5 条及び第 7 条に従って、別の構成国に対し、情報を提供すること；
  - (e) 第 6 条に従って情報を提供することを拒否すること、及び、それが必要なときは、第 6 条第 3 項に従って、明確化または特定を要請すること；
  - (f) 第 4 条に従って、別の構成国の単一連絡部局に対し、情報を求める要請書を送付すること、及び、それが必要なときは、第 6 条第 3 項に従って、明確化または特定を提供すること。

Member States shall ensure that their Single Point of Contact is equipped and empowered to carry out at least all of the following tasks:

- (a) receiving and evaluating requests for information submitted in accordance with Article 4 in the languages notified pursuant to Article 11(2);
- (b) channelling requests for information to the relevant competent law enforcement authorities and, where necessary, coordinating among them the processing of such requests and the provision of information pursuant to such requests;
- (c) coordinating the analysis and structuring of information with a view to providing it to the Single Points of Contact and, where applicable, to the competent law enforcement authorities of other Member States;

- (d) providing, on request or on its own initiative, information to other Member States in accordance with Articles 5 and 7;
  - (e) refusing to provide information in accordance with Article 6 and, where necessary, requesting clarification or specifications in accordance with Article 6(3);
  - (f) sending requests for information to the Single Points of Contact of other Member States in accordance with Article 4 and, where necessary, providing clarification or specifications in accordance with Article 6(3).
3. 構成国は、以下のことを確保する:
- (a) 当該構成国の単一連絡部局が:
    - (i) この指令の下にある当該単一連絡部局の職務を遂行するために必要な範囲内において、当該構成国の職務権限のある法執行機関にとって利用可能な全ての情報に対するアクセスをもつこと;
    - (ii) 週 7 日間、日 24 時間体制で当該単一連絡部局の職務を遂行すること;
    - (iii) それが適用可能なときは、第 5 条第 1 項に定める期限内の場合を含め、この指令に従って適切で、実効的かつ迅速な態様で当該単一連絡部局の職務を遂行するために必要となる、資格をもつ職員、適切な運用ツール、技術上の資源及び資金、インフラ、並びに、翻訳のためのものを含め、能力の提供を受けること;
  - (b) 第 9 条に従って、国内法の下で要求される法務上の許可を与えることの職務権限をもつ法務当局が、週 7 日間、日 24 時間体制で、要求に応じて、単一連絡部局にとって利用可能であること。

Member States shall ensure that:

- (a) their Single Point of Contact:
    - (i) has access to all information available to their competent law enforcement authorities, in so far as necessary to carry out its tasks under this Directive;
    - (ii) carries out its tasks 24 hours a day, 7 days a week;
    - (iii) is provided with qualified staff, appropriate operational tools, technical and financial resources, infrastructure, and capabilities, including for translation, necessary to carry out its tasks in an adequate, effective and rapid manner in accordance with this Directive, including, where applicable, within the time limits set out in Article 5(1);
  - (b) the judicial authorities competent to grant the judicial authorisations required under national law in accordance with Article 9 are available on call to the Single Point of Contact 24 hours a day, 7 days a week.
4. 構成国は、欧州委員会に対し、当該構成国の単一連絡部局の設置または指定から 1 か月以内に、通知する。当該構成国は、当該構成国の単一連絡部局に関して変更が存在するときは、欧州委員会に対し、連絡する。

Member States shall notify the Commission within one month of the establishment or designation of their

Single Point of Contact. They shall inform the Commission where there are changes as regards their Single Point of Contact.

欧州委員会は、EU 官報上において、当該通知及び同通知のアップデートを公表する。

The Commission shall publish those notifications, and any updates thereto, in the *Official Journal of the European Union*.

## 第 15 条 組織、構成及び訓練

### Article 15 Organisation, composition and training

1. 構成国は、当該構成国の単一連絡部局が、効率的かつ実効的な態様でこの指令の下にある当該単一連絡部局の職務を遂行できるような態様で、当該構成国の単一連絡部局の組織及び構成を決定する。

Member States shall determine the organisation and the composition of their Single Point of Contact in such a manner that it can carry out its tasks under this Directive in an efficient and effective manner.

2. 構成国は、そのようなユニットまたは事務局を設置または指定するための関連法律または国際協定によって関係する構成国が拘束されている範囲内において、少なくとも以下のユニットまたは事務局を含め、この指令の下における情報の適切かつ迅速な交換のためにその関与が必要な当該構成国の職務権限のある法執行機関の職員によって当該構成国の単一連絡部局が構成されることを確保する:
  - (a) 規則(EU) 2016/794 の第 7 条によって設置された Europol 国内ユニット;
  - (b) 規則(EU) 2018/1862 の第 7 条第 2 項によって設置された SIRENE 事務局;
  - (c) 国際刑事警察機構—Interpol の憲章の第 32 条によって設置された Interpol の国内中央事務局。

Member States shall ensure that their Single Point of Contact is composed of staff from their competent law enforcement authorities whose involvement is necessary for the adequate and rapid exchange of information under this Directive, including at least the following in so far as the Member State concerned is bound by the relevant law or international agreement to establish or designate such units or bureaux:

- (a) the Europol national unit established by Article 7 of Regulation (EU) 2016/794;
  - (b) the SIRENE Bureau established by Article 7(2) of Regulation (EU) 2018/1862;
  - (c) the Interpol National Central Bureau established by Article 32 of the Constitution of the International Criminal Police Organisation – Interpol.
3. 構成国は、当該構成国の単一連絡部局の職員が、この指令の下にある当該職員の機能を果たすための適切な資格をもつことを確保する。その目的のために、構成国は、当該構成国の単一

連絡部部局の職員に対し、とりわけ以下の事項と関連する適切かつ定期的な訓練へのアクセスを提供する:

- (a) 単一連絡部局内で使用されるデータ処理ツールの使用、とりわけ、SIENA 及び事件管理システムの使用;
- (b) とりわけ、指令(EU) 2016/680 を含め、個人データの保護に関し、この指令及び規則(EU) 2016/794 を含め、法執行機関の間における国境を越える協力に関し、並びに、機密情報の取扱いに関し、この指令の下における単一連絡部局の活動と関連する欧州連合法及び国内法の適用;
- (c) 第 11 条により、関係する構成国によって作成されるリストの中に含まれている言語の使用。

Member States shall ensure that the staff of their Single Point of Contact are adequately qualified in order to carry out their functions under this Directive. To that end, Member States shall provide the staff of their Single Point of Contact with access to adequate and regular training, in particular as regards the following:

- (a) the use of data processing tools used within the Single Point of Contact, in particular SIENA and the case management system;
- (b) the application of Union and national law relevant for the activities of the Single Point of Contact under this Directive, in particular on the protection of personal data, including Directive (EU) 2016/680, on cross-border cooperation between law enforcement authorities, including this Directive and Regulation (EU) 2016/794, and on the handling of confidential information;
- (c) the use of the languages included in the list established by the Member State concerned pursuant to Article 11.

## 第 16 条 事件管理システム

### Article 16 Case management system

1. 構成国は、当該構成国の単一連絡部局が、この指令の下にある単一連絡部局の職務を単一連絡部局が遂行できるようにするリポジトリとして、単一の電子的な事件管理システムを配置及び運用することを確保する。事件管理システムは、少なくとも、以下の機能及び能力の全てをもつものとする:
  - (a) 第 5 条及び第 8 条に示す情報を求める要請の受領と送付、並びに、それ以外の、第 6 条第 2 項及び第 3 項にそれぞれ示す情報を求める要請の拒否に関する情報、及び、明確化または特定の提供を求める要請及びその提供を含め、別の構成国の単一連絡部局との間の、及び、それが適用可能なときは、別の構成国の職務権限のある法執行機関との間の、そのような要請と関連する通信を記録すること;
  - (b) 第 14 条第 2 項(b)による単一連絡部局と職務権限のある法執行機関との間の通信を記録すること;
  - (c) 第 5 条、第 7 条及び第 8 条に従い、別の構成国の単一連絡部局に対する、及び、それが適用可能なときは、別の構成国の職務権限のある法執行機関に対する情報の提供を記録すること;

- (d) 第 5 条及び第 8 条に示す、受領する情報を求める要請と、第 5 条第 3 項第 2 副項及び第 7 条第 3 項第 2 副項に従って提供された情報を含め、単一連絡部局にとって利用可能な情報、及び、事件管理システム内に記録されたその他の関連情報とを照合すること;
- (e) とりわけ、第 5 条に定める要請された情報の提供の期限を尊重するという観点から、第 4 条に示す情報を求める要請の受領への適切かつ迅速な事後対応を確保すること;
- (f) SIENA と相互運用性があること、とりわけ、SIENA を介する受領の通信が事件管理システムの中に直接に記録され得ること、及び、SIENA を介する送付の通信が事件管理システムから直接に送信され得ることを確保すること;
- (g) 評価及び監視の目的のために、とりわけ、第 18 条の目的のために、この指令の下にある情報の交換に関する統計を生成すること;
- (h) 指令(EU) 2016/680 の第 25 条に従い、説明責任の目的及びサイバーセキュリティの目的のために、事件管理システムの中に収録されている情報と関係するアクセス及びそれ以外の処理業務の遂行の履歴(ログ)を記録すること。

Member States shall ensure that their Single Point of Contact deploys and operates a single electronic case management system as the repository that allows the Single Point of Contact to carry out its tasks under this Directive. The case management system shall have at least all of the following functions and capabilities:

- (a) recording incoming and outgoing requests for information as referred to in Articles 5 and 8 and any other communications relating to such requests with Single Points of Contact and, where applicable, the competent law enforcement authorities of other Member States, including information about refusals of requests for information and requests for and the provision of clarification or specifications as referred to in Article 6(2) and (3) respectively;
- (b) recording communications between the Single Point of Contact and the competent law enforcement authorities, pursuant to Article 14(2), point (b);
- (c) recording provisions of information to the Single Point of Contact and, where applicable, to the competent law enforcement authorities of other Member States in accordance with Articles 5, 7 and 8;
- (d) cross-checking incoming requests for information as referred to in Articles 5 and 8 against information available to the Single Point of Contact, including information provided in accordance with Article 5(3), second subparagraph, and Article 7(3), second subparagraph, and other relevant information recorded in the case management system;
- (e) ensuring adequate and rapid follow-up to incoming requests for information as referred to in Article 4, in particular with a view to respecting the time limits for the provision of the requested information set out in Article 5;
- (f) be interoperable with SIENA, ensuring, in particular, that incoming communications through SIENA can be directly recorded in, and that outgoing communications through SIENA can be directly sent from, the case management system;
- (g) generating statistics in respect of exchanges of information under this Directive for evaluation and monitoring purposes, in particular for the purposes of Article 18;

(h) logging access and other processing operations in relation to the information contained in the case management system, for accountability and cybersecurity purposes, in accordance with Article 25 of Directive (EU) 2016/680.

2. 構成国は、事件管理システムと関連する全てのサイバーセキュリティ上のリスク、とりわけ、事件管理システムのアーキテクチャ、統治及び管理と関連するリスクが、慎重かつ実効的な態様で管理及び対処されること、そして、無権限のアクセス及び濫用に抗する適切な安全確保が定められることを確保する。

Member States shall ensure that all cybersecurity risks relating to the case management system, in particular as regards its architecture, governance and control, are managed and addressed in a prudent and effective manner and that adequate safeguards against unauthorised access and abuse are provided for.

3. 構成国は、この指令の下において単一連絡部局に割当てられた職務を遂行するために単一連絡部局によって必要かつ比例的な範囲内に限り、事件管理システムが個人データを収録すること、そして、事件管理システムに収録された個人データが、その後、不可逆的に消去されることを確保する。

Member States shall ensure that the case management system contains personal data only for as long as it is necessary and proportionate for the Single Point of Contact to carry out the tasks assigned to it under this Directive and that the personal data contained therein are subsequently irrevocably deleted.

4. 構成国は、当該構成国の単一連絡部局が、最初は情報の交換が完了した後 6 か月以内に、かつ、その後は定期的に、第 3 項の遵守を見直すことを確保する。

Member States shall ensure that their Single Point of Contact reviews, for the first time at the latest six months after an exchange of information has concluded and subsequently on a regular basis, compliance with paragraph 3.

## 第 17 条 単一連絡部局間の協力

### Article 17 Cooperation between Single Points of Contact

1. 構成国は、この指令の目的のための当該構成国の単一連絡部局と職務権限のある法執行機関との間の実務上の協力を推進する。

Member States shall encourage practical cooperation between their Single Points of Contact and competent law enforcement authorities for the purposes of this Directive.

2. 構成国は、単一連絡部局の長が、単一連絡部局職の間の協力の質を評価するため、困難が生じ

た際において、必要な技術上の措置または組織上の措置を討議するため、そして、それが要求されるときは、手順を明確化するため、少なくとも年 1 回、会合することを確保する。

Member States shall ensure that the Heads of the Single Points of Contact meet at least once a year to assess the quality of the cooperation between their services, to discuss necessary technical or organisational measures in the event of any difficulties and to clarify procedures where required.



## 第VI章 最終規定

### Chapter VI Final Provisions

#### 第18条 統計

##### Article 18 Statistics

1. 毎年 3 月 1 日までに、各構成国は、欧州委員会に対し、この指令の下において別の構成国との間において前暦年の間に行われた情報の交換に関する統計を提供する。

By 1 March of each year, each Member State shall provide the Commission with statistics on the exchanges of information with other Member States under this Directive which took place during the previous calendar year.

2. 各構成国は、第 1 項に示す統計が、ミニマムのものとして、以下の事項を包摂することを確保する：
  - (a) 当該構成国の単一連絡部局から、及び、それが関連するときは、当該構成国の職務権限のある法執行機関から提出された情報を求める要請の数；
  - (b) 緊急の要請と緊急ではない要請とに仕分けし、かつ、要請元構成国毎に仕分けした、当該構成国の単一連絡部局及び当該構成国の職務権限のある法執行機関が受けた情報を求める要請の数、並びに、その要請に対して当該構成国の単一連絡部局及び当該構成国の職務権限のある法執行機関が回答した情報を求める要請の数；
  - (c) 要請元構成国毎に仕分けし、かつ、拒否の根拠毎に仕分けした、第 6 条により拒否された情報を求める要請の数；
  - (d) 関係する情報を求める要請書を提出した構成国毎に仕分けした、第 5 条第 2 項に従って法務上の許可を得るために必要だったことを理由として第 5 条第 1 項に定める期限の適用の免除が存在した案件の数。

Each Member State shall ensure that the statistics referred to in paragraph 1 cover, as a minimum:

- (a) the number of requests for information submitted by their Single Point of Contact and, where relevant, by their competent law enforcement authorities;
- (b) the number of requests for information that their Single Point of Contact and their competent law enforcement authorities received and the number of requests for information to which they replied, broken down by urgent and non-urgent requests and by requesting Member State;
- (c) the number of requests for information refused pursuant to Article 6, broken down by requesting Member State and by ground for refusal;
- (d) the number of cases in which there was a deviation from the time limits set out in Article 5(1) because it was necessary to obtain a judicial authorisation in accordance with Article 5(2), broken down by the Member States that submitted the requests for information concerned.

3. 欧州委員会は、第 2 項の下で構成国から提出されたミニマムの統計をとりまとめ、かつ、欧州議会及び理事会に対し、それを利用できるようにする。

The Commission shall compile the minimum statistics provided by Member States under paragraph 2 and make them available to the European Parliament and to the Council.

## 第 19 条 報告

### Article 19 Reporting

1. 欧州委員会は、2026 年 6 月 12 日までに、及び、2027 年 6 月 12 日以降は 5 年毎に、欧州議会及び理事会に対し、この指令の実装を評価し、かつ、各構成国がこの指令をどのように実装したのかに関する詳細情報を含む報告書を提出する。当該報告書をとりまとめる際、欧州委員会は、職務権限のある法執行機関がどれだけ効率的に情報を交換したか、情報を求める要請が拒否された根拠、とりわけ、要請がこの指令の目的の適用範囲外にある場合、並びに、データ保護に関する条項及び Europol に対する情報の提供に関する条項の遵守に対して特に注意を払う。

The Commission shall, by 12 June 2026 and every five years after 12 June 2027, submit a report to the European Parliament and to the Council assessing the implementation of this Directive and containing detailed information on how each Member State has implemented this Directive. In compiling that report, the Commission shall pay particular attention to how efficiently competent law enforcement authorities exchanged information, the grounds for which requests for information were refused, in particular where requests fall outside the scope of the objectives of this Directive, and the compliance with provisions on data protection and the provision of information to Europol.

2. 欧州委員会は、2027 年 6 月 12 日までに、及び、その後は 5 年毎に、欧州議会及び理事会に対し、この指令の実効性、とりわけ、法執行の協力、第 14 条第 3 項(a)(iii)に定める義務及び個人データの保護に対するこの指令の影響を評価する報告書を提出する。欧州委員会は、それが適用可能なときは、この指令の実効的な実装を阻害する実務上の障害を含め、構成国から提供された情報及びこの指令の国内法化及び実装と関連するその他の関連情報を考慮に入れる。同評価を基礎として、欧州委員会は、それが適切なときは、立法提案を含め、適切な事後対応の活動に関して判断する。

The Commission shall, by 12 June 2027 and every five years thereafter, submit a report to the European Parliament and to the Council assessing the effectiveness of this Directive, in particular its impact on law enforcement cooperation, the obligations laid down in Article 14(3), point (a)(iii), and the protection of personal data. The Commission shall take into account the information provided by Member States and any other relevant information related to the transposition and implementation of this Directive, including, where applicable, practical obstacles that hamper its effective implementation. On the basis of that assessment, the Commission shall decide on appropriate follow-up actions, including, where appropriate,

a legislative proposal.

## 第 20 条 シェンゲン協定実装条約の改正

### Article 20 Amendments to the Convention implementing the Schengen Agreement

2024 年 12 月 12 日から、シェンゲン協定実装条約の第 39 条及び第 46 条の枠組み決定 2006/960/JHA によって置き換えられなかった部分は、当該条項がこの指令の適用範囲内にある情報の交換と関連する範囲内において、この指令によって置き換えられる。

From 12 December 2024, the parts of Articles 39 and 46 of the Convention implementing the Schengen Agreement that have not been replaced by Framework Decision 2006/960/JHA are replaced by this Directive in so far as those Articles relate to the exchange of information falling within the scope of this Directive.

## 第 21 条 廃止

### Article 21 Repeal

枠組み決定 2006/960/JHA は、2024 年 12 月 12 日から廃止される。

Framework Decision 2006/960/JHA is repealed from 12 December 2024.

廃止される枠組み決定に対する参照は、この指令への参照として解釈され、かつ、別紙の新旧対照表に従って読み替えられる。

References to the repealed Framework Decision shall be construed as references to this Directive and shall be read in accordance with the correlation table in the Annex.

## 第 22 条 国内法化

### Article 22 Transposition

1. 2024 年 12 月 12 日までに、構成国は、この指令を遵守するために必要となる法律、規則及び行政条項を発効させる。当該構成国は、欧州委員会に対し、直ちに、当該法律、規則及び行政条項を連絡する。

Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 12 December 2024. They shall immediately inform the Commission thereof.

第 1 副項の特例により、構成国は、2027 年 6 月 12 日までに、第 13 条を遵守するために必要となる法律、規則及び行政条項を発効させる。当該構成国は、欧州委員会に対し、直ちに、当該法律、規則及び行政条項を連絡する。

By way of derogation from the first subparagraph, Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with Article 13 by 12 June 2027. They shall immediately inform the Commission thereof.

構成国が第 1 副項に及び第 2 副項に示す措置を採択する際、当該措置は、この指令に対する参照を含めるものとし、または、当該措置の公示の際にそのような参照を添えるものとする。そのような参照を行う手法は、構成国によって定められる。

When Member States adopt the measures referred to in the first and second subparagraphs, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. 構成国は、欧州委員会に対し、この指令の適用のある分野において当該構成国が採択する国内法の主要な措置の正文を通知する。

Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

## 第 23 条 発効

### Article 23 Entry into force

この指令は、EU 官報上のその公示の 20 日後に発効する。

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

## 第 24 条 発出

### Article 24 Addressees

この指令は、諸条約に従い、構成国に対して発出される。

This Directive is addressed to the Member States in accordance with the Treaties.

ストラスブールにおいて, 2023 年 5 月 10 日に行われた。

Done at Strasbourg, 10 May 2023.

欧州議会として  
For the European Parliament

議長 R. METSOLA  
The President The President

理事会として  
For the Council

議長 J. ROSWALL  
The President J. ROSWALL

別 紙  
新旧対照表

CORRELATION TABLE

理事会枠組み決定 2006/960/JHA Council Framework Decision 2006/960/JHA	この指令 This Directive
第 1 条	第 1 条
第 2 条	第 2 条
第 3 条	第 3 条及び第 9 条
第 4 条	第 5 条
第 5 条	第 4 条
第 6 条	第 11 条, 第 12 条及び第 13 条
第 7 条	第 7 条及び第 8 条
第 8 条	第 10 条
第 9 条	第 3 条
第 10 条	第 6 条
第 11 条	第 21 条
第 12 条	第 19 条
第 13 条	第 22 条



2024 Printed in Japan

ISSN 2432-6089

法と情報雑誌 第9巻第1号 (通巻第55号) (第1分冊)

The Law and Information Magazine vol.9 no.1 (consecutive no.55) part 1

2024年1月1日発行

発行者 夏井高人

発行所 法と情報研究会 (代表 夏井高人)

東京都千代田区神田駿河台1-1

学校法人明治大学研究棟

(非売品)