Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2447

5.12.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/2447 DER KOMMISSION

vom 4. Dezember 2025

mit Durchführungsbestimmungen zur Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates im Hinblick auf die technischen Spezifikationen, Maßnahmen und sonstigen Anforderungen für die Einrichtung und Nutzung des dezentralen IT-Systems für die sichere Verarbeitung und Übermittlung von Informationen

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates vom 14. November 2018 betreffend die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) und zur Ersetzung und Aufhebung des Beschlusses 2002/187/JI des Rates ([1]), insbesondere Artikel 22a Absatz 3 und Artikel 22b Absatz 1 Buchstaben a, b, c und d,

in Erwägung nachstehender Gründe:

(1) In der Verordnung (EU) 2018/1727 wird der Rahmen für die neue interne digitale Infrastruktur von Eurojust und die Einrichtung eines dezentralen sicheren digitalen Kommunikationssystems zwischen den zuständigen nationalen Behörden der Mitgliedstaaten und Eurojust festgelegt.

(2) Die sichere digitale Kommunikation soll über das dezentrale IT-System erfolgen. Zur Einrichtung des dezentralen IT-Systems müssen technische Spezifikationen festgelegt werden, in denen die Methoden der Kommunikation und die Kommunikationsprotokolle, technische Maßnahmen zur Gewährleistung von Mindeststandards für die Informationssicherheit und die Sicherheit sowie Mindestverfügbarkeitsvorgaben für die Umsetzung dieses Systems festgelegt werden.

(3) Nach Artikel 22a Absatz 1 der Verordnung (EU) 2018/1727 soll sich das dezentrale IT-System aus den IT-Systemen der Mitgliedstaaten und von Eurojust sowie aus den interoperablen e-CODEX-Zugangspunkten zusammensetzen, über die diese IT-Systeme miteinander vernetzt sind. Die in der vorliegenden Verordnung festgelegten technischen Spezifikationen und sonstigen Anforderungen des dezentralen IT-Systems sollten diesem Rahmen Rechnung tragen.

(4) Die Zugangspunkte des dezentralen IT-Systems sollten auf autorisierten e-CODEX-Zugangspunkten gemäß Artikel 3 Nummer 3 der Verordnung (EU) 2022/850 des Europäischen Parlaments und des Rates ([2]) beruhen.

(5) Das dezentrale IT-System wird in einem größeren, auf e-CODEX basierenden dezentralen IT-System (JUDEX) implementiert. Daher muss ein wirksamer Informationsaustausch über horizontale Entwicklungen gewährleistet werden.

(6) Gemäß Artikel 22a Absatz 4 der Verordnung (EU) 2018/1727 können die Mitgliedstaaten und Eurojust beschließen, anstelle eines nationalen IT-Systems die von der Kommission entwickelte Referenzimplementierungssoftware als Back-End-System zu verwenden. Damit die Interoperabilität gewährleistet ist, sollten für die nationalen IT-Systeme und die Referenzimplementierungssoftware dieselben technischen Spezifikationen und Anforderungen gelten.

(7) Daten über terroristische Straftaten und schwere organisierte Kriminalität sollten strukturiert übermittelt werden, um die Qualität und Relevanz der Informationen zu verbessern und sicherzustellen, dass die Informationen effizienter in das Fallbearbeitungssystem von Eurojust integriert und besser mit bereits in diesem System gespeicherten Informationen abgeglichen werden können. Für Fingerabdruckdaten und Lichtbilder, die Eurojust zur Identifizierung von Personen, die Gegenstand von Strafverfahren im Zusammenhang mit terroristischen Straftaten sind, übermittelt werden können, sollten das Format und die technischen Standards für die Übermittlung festgelegt werden.

([1]) ABl. L 295 vom 21.11.2018, S. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

([2]) Verordnung (EU) 2022/850 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über ein EDV-System für den grenzüberschreitenden elektronischen Datenaustausch im Bereich der justiziellen Zusammenarbeit in Zivil- und Strafsachen (e-CODEX-System) und zur Änderung der Verordnung (EU) 2018/1726 (ABl. L 150 vom 1.6.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust erleichtert und unterstützt die Ausstellung und Erledigung von Ersuchen um justizielle Zusammenarbeit, darunter Ersuchen und Entscheidungen auf der Grundlage von Rechtsinstrumenten, die dem Grundsatz der gegenseitigen Anerkennung Wirkung verleihen. Die zuständigen nationalen Behörden sollten Eurojust über das dezentrale IT-System um Unterstützung und Koordinierung ersuchen können.

(9) Zur Gewährleistung von Effizienz und Kohärenz ist es wichtig, dass die gemäß der Verordnung (EU) 2018/1727 festzulegenden technischen Spezifikationen mit den technischen Spezifikationen gemäß den Verordnungen (EU) 2023/2844 ([3]), (EU) 2023/1543 ([4]) und (EU) 2024/3011 ([5]) des Europäischen Parlaments und des Rates sowie mit künftigen Digitalisierungsmaßnahmen, die für das Mandat von Eurojust zur Unterstützung der zuständigen nationalen Behörden relevant sind, vereinbar sind.

(10) Jede andere Kommunikation zwischen Eurojust und den zuständigen nationalen Behörden, wie die Übermittlung von Informationen über die Ergebnisse der Verarbeitung von Informationen, einschließlich des Bestehens von Verbindungen zu Fällen, die bereits im Fallbearbeitungssystem gemäß Artikel 22 der Verordnung (EU) 2018/1727 gespeichert sind, wenn Eurojust aus eigener Initiative handelt, oder von Informationen, die Eurojust zum Zwecke der Sicherung, Analyse und Speicherung von Beweismitteln im Zusammenhang mit Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen und damit zusammenhängenden Straftaten gemäß Artikel 4 Absatz 1 Buchstabe j der genannten Verordnung übermittelt werden, sollte ebenfalls über das dezentrale IT-System ermöglicht werden.

(11) Um sicherzustellen, dass diese Verordnung den operativen Erfordernissen von Eurojust genügt, wurde Eurojust gemäß Artikel 22a Absatz 3 der Verordnung (EU) 2018/1727 konsultiert.

(12) Nach Artikel 4 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts hat Irland mit Schreiben vom 9. September 2019 seinen Wunsch mitgeteilt, die Verordnung (EU) 2018/1727 anzunehmen und durch sie gebunden zu sein. Mit dem Beschluss (EU) 2019/2006 der Kommission ([6]) wurde eine solche Beteiligung bestätigt. Mit der Verordnung (EU) 2023/2131 des Europäischen Parlaments und des Rates ([7]) wurde die Verordnung (EU) 2018/1727 geändert, um die Einrichtung sicherer digitaler Kommunikationskanäle zwischen Eurojust und den zuständigen nationalen Behörden zu ermöglichen, und sie bildet die Rechtsgrundlage für die vorliegende Verordnung. In Fällen, in denen Irland nicht mitgeteilt hat, dass es sich an der Annahme und Anwendung der Verordnung (EU) 2023/2131 beteiligen möchte und nicht mitgeteilt hat, dass es die genannte Verordnung annimmt und durch diese gebunden ist, ist Irland gemäß den Artikeln 1 und 2 und Artikel 4a Absatz 1 des Protokolls Nr. 21 weder durch die Verordnung (EU) 2023/2131 gebunden noch zu ihrer Anwendung verpflichtet. Daher beteiligt sich Irland nicht an der Annahme der genannten Verordnung.

(13) Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks hat sich Dänemark nicht an der Annahme der Verordnung (EU) 2018/1727 beteiligt. Dänemark ist daher weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.

([3]) Verordnung (EU) 2023/2844 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über die Digitalisierung der justiziellen Zusammenarbeit und des Zugangs zur Justiz in grenzüberschreitenden Zivil-, Handels- und Strafsachen und zur Änderung bestimmter Rechtsakte im Bereich der justiziellen Zusammenarbeit (ABl. L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Verordnung (EU) 2024/3011 des Europäischen Parlaments und des Rates vom 27. November 2024 zur Verwirklichung des Einheitlichen Europäischen Luftraums (ABl. L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Beschluss (EU) 2019/2006 der Kommission vom 29. November 2019 über die Beteiligung Irlands an der Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates betreffend die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) (ABl. L 310 vom 2.12.2019, S. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Verordnung (EU) 2023/2131 des Europäischen Parlaments und des Rates vom 4. Oktober 2023 zur Änderung der Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates sowie des Beschlusses 2005/671/JI des Rates im Hinblick auf digitalen Informationsaustausch in Terrorismusfällen (ABl. L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([8]) angehört und hat am 21. Oktober 2025 eine Stellungnahme abgegeben.

(15) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 22c der Verordnung (EU) 2018/1727 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Technische Spezifikationen des dezentralen IT-Systems

Die in Artikel 22b Absatz 1 Buchstabe a, b, c und d der Verordnung (EU) 2018/1727 genannten technischen Spezifikationen, Maßnahmen und Zielvorgaben des dezentralen IT-Systems sind in Anhang I der vorliegenden Verordnung festgelegt.

Artikel 2

Digitale Verfahrensstandards

Die digitalen Verfahrensstandards für die elektronische Kommunikation über das dezentrale IT-System gemäß Artikel 22a Absatz 3 der Verordnung (EU) 2018/1727 sind in Anhang II der vorliegenden Verordnung festgelegt.

Artikel 3

Technische Spezifikationen für die Übermittlung von Fingerabdrücken und Lichtbildern

Die technischen Spezifikationen und das Format für die Übermittlung von Fingerabdrücken und Lichtbildern gemäß Artikel 22a Absatz 3 der Verordnung (EU) 2018/1727 sind in Anhang III der vorliegenden Verordnung festgelegt.

Artikel 4

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß den Verträgen unmittelbar in den Mitgliedstaaten.

Brüssel, den 4. Dezember 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

([8]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANHANG I

TECHNISCHE SPEZIFIKATIONEN, MAßNAHMEN UND ZIELVORGABEN DES DEZENTRALEN IT-SYSTEMS

1. Einleitung und Geltungsbereich

Dieser Anhang enthält die technischen Spezifikationen, Maßnahmen und Zielvorgaben des dezentralen IT-Systems für den Informationsaustausch gemäß Verordnung (EU) 2018/1727.

Durch seinen dezentralen Charakter ermöglicht das IT-System einen direkten und sicheren Datenaustausch zwischen den zuständigen nationalen Behörden und Eurojust.

2. Begriffsbestimmungen

Für die Zwecke dieses Anhangs gelten folgende Begriffsbestimmungen:

2.1. „Hypertext Transfer Protocol Secure“ (Sicheres Hypertext-Übertragungsprotokoll) oder „HTTPS“ steht für verschlüsselte Kommunikation und gesicherte Verbindungswege;

2.2. „Nichtabstreitbarkeit der Herkunft“ steht für die Maßnahmen, mit denen die Integrität und die Herkunft der Daten unter anderem durch digitale Zertifikate, Public-Key-Infrastruktur, elektronische Signaturen und elektronische Siegel nachgewiesen wird;

2.3. „Nichtabstreitbarkeit des Erhalts“ steht für die Maßnahmen, mit denen der Ersteller unter anderem durch digitale Zertifikate, Public-Key-Infrastruktur, elektronische Signaturen und elektronische Siegel den Nachweis erhält, dass der vorgesehene Empfänger die Daten erhalten hat;

2.4. „SOAP“ (Simple Object Access Protocol) im Sinne der Standards des World Wide Web Consortium steht für ein Nachrichtenprotokoll für den Austausch strukturierter Informationen über Webdienste in Computernetzen;

2.5. „REST“ (Representational State Transfer) ist ein Architekturstil für die Entwicklung vernetzter Anwendungen, der sich auf ein zustandsloses Client-Server-Kommunikationsmodell stützt und Standardmethoden für Operationen mit Ressourcen verwendet, die in der Regel in strukturierten Formaten dargestellt werden;

2.6. „Webdienst“ steht für ein Software-System, das die interoperable Maschinen-zu-Maschinen-Interaktion über ein Netzwerk unterstützt und über eine Schnittstelle verfügt, die in einem maschinenlesbaren Format beschrieben ist;

2.7. „Datenaustausch“ steht für den Austausch von Nachrichten und Schriftstücken über das dezentrale IT-System;

2.8. „e-CODEX“ steht für das e-CODEX-System gemäß Artikel 3 Nummer 1 der Verordnung (EU) 2022/850;

2.9. „EU-Kernvokabular zur E-Justiz“ steht für das EU-Kernvokabular zur E-Justiz im Sinne von Nummer 4 des Anhangs der Verordnung (EU) 2022/850;

2.10. „ebMS“ steht für den ebXML-Messaging-Dienst, ein im Rahmen des OASIS-Rahmenwerks entwickeltes Nachrichtenprotokoll, das einen sicheren, zuverlässigen und interoperablen Austausch elektronischer Geschäftsunterlagen über SOAP ermöglicht. Es unterstützt die Business-to-Business-Integration über verschiedene Systeme hinweg;

2.11. „AS4“ steht für „Applicability Statement Nr. 4“, einen OASIS-Standard, der ebMS 3.0 profiliert; er vereinfacht die sichere und interoperable Kommunikation zwischen Unternehmen durch die Verwendung offener Standards wie SOAP und WS-Security;

2.12. „Vorgabe für die Wiederherstellungszeit“ steht für die Dauer, die für die Wiederherstellung des Betriebs nach einem Vorfall höchstens tolerierbar ist;

2.13. „Vorgabe für den Wiederherstellungspunkt“ steht für den maximal zulässigen Umfang des Datenverlusts bei einem Ausfall.

3. **Methoden der elektronischen Kommunikation**

3.1. Für den Austausch von Nachrichten und Schriftstücken nutzt das dezentrale IT-System dienstbasierte Methoden der Kommunikation wie etwa Webdienste oder andere wiederverwendbare Komponenten und Softwarelösungen.

3.2. Insbesondere muss das dezentrale IT-System die Kommunikation über e-CODEX-Zugangspunkte gemäß Artikel 5 Absatz 2 der Verordnung (EU) 2022/850 umfassen. Um einen wirksamen und interoperablen grenzüberschreitenden Datenaustausch zu gewährleisten, muss das dezentrale IT-System die Kommunikation über das e-CODEX-System unterstützen.

4. **Kommunikationsprotokolle**

4.1. Das dezentrale IT-System verwendet sichere Internetprotokolle für

a) die Kommunikation innerhalb des dezentralen IT-Systems zwischen den zuständigen Behörden und Eurojust,

b) die Kommunikation mit der zuständigen Behörde/der Gerichtsdatenbank gemäß Nummer 7.1.

4.2. Für die Definition und Übermittlung strukturierter Daten und Metadaten stützen sich die Komponenten des dezentralen IT-Systems auf umfassende und allgemein anerkannte Industrienormen und -protokolle wie SOAP und REST.

4.3. Für die Transport- und Nachrichtenprotokolle beruht das dezentrale IT-System auf sicheren Standardprotokollen, wie z. B.:

a) einem AS4-Profil für den grenzüberschreitenden Datenaustausch, um eine sichere und zuverlässige Nachrichtenübermittlung mit Verschlüsselung und Nichtabstreitbarkeit zu gewährleisten,

b) HTTPS/RESTful APIs für Kommunikation, die JSON- und XML-Formate unterstützt,

c) SOAP für hochzuverlässige Interaktionen, einschließlich WS-Security zur Authentifizierung und Verschlüsselung.

4.4. Für die Zwecke eines nahtlosen und interoperablen Datenaustauschs müssen die vom dezentralen IT-System verwendeten Kommunikationsprotokolle den einschlägigen Interoperabilitätsstandards entsprechen.

4.5. Bei den XML-Schemata werden gegebenenfalls einschlägige Standards oder Vokabulare verwendet, die für die ordnungsgemäße Validierung der im Schema festgelegten Elemente und Typen erforderlich sind. Diese Standards oder Vokabulare können Folgendes umfassen:

a) das EU-Kernvokabular zur E-Justiz,

b) unqualifizierte Datentypen,

c) eine Codeliste für die Sprachencodes der Europäischen Union.

4.6. Für die Sicherheits- und Authentifizierungsprotokolle stützt sich das dezentrale IT-System auf standardisierte Protokolle wie:

a) TLS (Transport Layer Security) für die verschlüsselte und authentifizierte Kommunikation über Netze, mit Unterstützung der gegenseitigen Authentifizierung über digitale X.509-Zertifikate,

b) OAuth/OpenID Connect (OIDC) für die sichere Authentifizierung und Autorisierung,

c) PKI (Public Key Infrastructure) und digitale Signaturen für den sicheren Schlüsselaustausch und die Überprüfung der Nachrichtenintegrität unter Verwendung digitaler Zertifikate (X.509), die von vertrauenswürdigen Zertifizierungsstellen (CA) ausgestellt werden.

5. **Vorgaben für die Informationssicherheit und entsprechende technische Maßnahmen**

5.1. Die technischen Maßnahmen zur Einhaltung von IT-Mindestsicherheitsstandards für den Informationsaustausch über das dezentrale IT-System müssen Folgendes umfassen:

a) Maßnahmen zur Gewährleistung der Vertraulichkeit der Informationen, z. B. durch Nutzung sicherer Kommunikationskanäle,

b) Maßnahmen zur Gewährleistung der Integrität der Daten im Ruhezustand und bei der Datenübermittlung,

c) Maßnahmen zur Gewährleistung der Nichtabstreitbarkeit der Herkunft durch den Absender der Informationen innerhalb des dezentralen IT-Systems sowie der Nichtabstreitbarkeit des Erhalts der Informationen,

d) Maßnahmen, die die Protokollierung von sicherheitsrelevanten Ereignissen im Einklang mit anerkannten internationalen Empfehlungen für IT-Sicherheitsstandards gewährleisten ([1]);

e) Maßnahmen zur Gewährleistung der Authentifizierung und Autorisierung der Nutzer und Maßnahmen zur Überprüfung der Identität der mit dem dezentralen IT-System verbundenen Systeme.

5.2. Die Komponenten des dezentralen IT-Systems gewährleisten eine sichere Kommunikation und Datenübertragung durch Verschlüsselung, Public-Key-Infrastruktur mit digitalen Zertifikaten für die Authentifizierung und den sicheren Schlüsselaustausch sowie sichere Nachrichtenübermittlungsprotokolle wie AS4 (ebMS), RESTful APIs und SOAP, um die Vertraulichkeit und Integrität der Nachrichten zu wahren.

5.3. Wird TLS im Rahmen des dezentralen IT-Systems eingesetzt, so ist die letzte stabile Version des Protokolls oder, falls dies nicht möglich ist, eine Version ohne bekannte Sicherheitslücken zu verwenden. Es sind nur Schlüssellängen zulässig, die ein angemessenes Maß an kryptografischer Sicherheit gewährleisten, und es dürfen keine als unsicher oder veraltet bekannten Cipher Suites verwendet werden.

5.4. Soweit möglich, werden digitale PKI-Zertifikate, die für die Zwecke des dezentralen IT-Systems verwendet werden, von Zertifizierungsstellen ausgestellt, die gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([2]) als qualifizierte Vertrauensdiensteanbieter anerkannt sind. Es werden Maßnahmen ergriffen, um sicherzustellen, dass solche Zertifikate ausschließlich für ihre vorgesehenen Zwecke, auf dem erforderlichen Vertrauensniveau und im Einklang mit den geltenden Anforderungen der Verordnung (EU) Nr. 910/2014 verwendet werden.

5.5. Die Komponenten des dezentralen IT-Systems werden nach dem Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen entwickelt, und es werden geeignete administrative, organisatorische und technische Maßnahmen ergriffen, um ein hohes Maß an Cybersicherheit zu gewährleisten.

5.6. Die Kommission konzipiert, entwickelt und pflegt die Referenzimplementierungssoftware im Einklang mit den in der Verordnung (EU) 2018/1725 festgelegten Datenschutzanforderungen und -grundsätzen. Die von der Kommission bereitgestellte Referenzimplementierungssoftware ermöglicht es den Mitgliedstaaten, ihren Verpflichtungen gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([3]) bzw. der Richtlinie (EU) 2016/680 nachzukommen.

([1]) Unbeschadet der Protokollierung zu Sicherheitszwecken müssen die von den Komponenten des dezentralen IT-Systems eingesetzten Protokollierungsmechanismen gegebenenfalls die Einhaltung der Anforderungen des Artikels 88 der Verordnung (EU) 2018/1725 und gegebenenfalls des Artikels 25 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj) gewährleisten.

([2]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Mitgliedstaaten, die ein anderes nationales Back-End-System als die Referenzimplementierungssoftware verwenden, ergreifen die erforderlichen Maßnahmen, um sicherzustellen, dass dieses andere Back-End-System den Anforderungen der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 entspricht.

5.8. Eurojust ergreift die erforderlichen Maßnahmen, um sicherzustellen, dass sein Back-End-System oder eine von Eurojust verwendete Referenzimplementierungssoftware den Anforderungen der Verordnungen (EU) 2018/1725 und (EU) 2018/1727 entspricht.

5.9. Die Mitgliedstaaten und Eurojust richten für die IT-Systeme, die Teil des dezentralen IT-Systems sind und in ihre Zuständigkeit fallen, gemäß ihren diesbezüglichen Regelwerken robuste Mechanismen für die Entdeckung von Bedrohungen und die Reaktion auf Vorfälle ein, um die rechtzeitige Erkennung und Eindämmung sowie die Wiederherstellung des Betriebs bei Sicherheitsvorfällen sicherzustellen.

6. **Mindestverfügbarkeitsvorgaben**

6.1. Eurojust und die Mitgliedstaaten stellen sicher, dass die Komponenten des dezentralen IT-Systems, für die sie zuständig sind, täglich rund um die Uhr verfügbar sind, wobei die angestrebte technische Verfügbarkeitsquote bei mindestens 98 % jährlich liegt, planmäßige Wartungsarbeiten ausgenommen.

6.2. Die Kommission sorgt dafür, dass die Gerichtsdatenbank täglich rund um die Uhr zur Verfügung steht, wobei die angestrebte technische Verfügbarkeitsquote bei über 99 % jährlich liegt, planmäßige Wartungsarbeiten ausgenommen.

6.3. Soweit möglich, werden Wartungsarbeiten an Arbeitstagen zwischen 20 Uhr und 7 Uhr MEZ geplant.

6.4. Die Mitgliedstaaten unterrichten die Kommission, Eurojust und die anderen Mitgliedstaaten über Wartungstätigkeiten wie folgt:

a) 5 Arbeitstage vor Wartungsarbeiten, die eine Nichtverfügbarkeit von bis zu 4 Stunden zur Folge haben können,

b) 10 Arbeitstage vor Wartungsarbeiten, die eine Nichtverfügbarkeit von 4 bis 12 Stunden zur Folge haben können,

c) 30 Arbeitstage vor Wartungsarbeiten, die eine Nichtverfügbarkeit von über 12 Stunden zur Folge haben können.

6.5. Verfügen die Mitgliedstaaten über feste Zeitfenster für die regelmäßige Wartung, so unterrichten sie die Kommission, Eurojust und die anderen Mitgliedstaaten über die Uhrzeit und die Tage, an denen solche festen Zeitfenster geplant sind. Sollten Komponenten des dezentralen IT-Systems, für die die Mitgliedstaaten zuständig sind, während eines solchen festen Zeitfensters nicht verfügbar sein, so können die Mitgliedstaaten abweichend von den Verpflichtungen in Satz 1 beschließen, die Kommission nicht in jedem Fall darüber zu unterrichten.

6.6. Im Falle eines unerwarteten technischen Ausfalls einer Komponente des dezentralen IT-Systems, für die die Mitgliedstaaten zuständig sind, unterrichten die Mitgliedstaaten die Kommission und die anderen Mitgliedstaaten unverzüglich und, sofern bekannt, über den voraussichtlichen Zeitraum bis zur Wiederherstellung.

6.7. Eurojust unterrichtet die Kommission und die Mitgliedstaaten über Wartungstätigkeiten wie folgt:

a) 5 Arbeitstage vor Wartungsarbeiten, die eine Nichtverfügbarkeit von bis zu 4 Stunden zur Folge haben können,

b) 10 Arbeitstage vor Wartungsarbeiten, die eine Nichtverfügbarkeit von 4 bis 12 Stunden zur Folge haben können,

c) 30 Arbeitstage vor Wartungsarbeiten, die eine Nichtverfügbarkeit von über 12 Stunden zur Folge haben können.

6.8. Verfügt Eurojust über feste Zeitfenster für die regelmäßige Wartung, so unterrichtet Eurojust die Kommission und die Mitgliedstaaten über die Uhrzeit und die Tage, an denen solche festen Zeitfenster geplant sind. Sollten Komponenten des dezentralen IT-Systems, für die Eurojust zuständig ist, während eines solchen festen Zeitfensters nicht verfügbar sein, so kann Eurojust abweichend von den Verpflichtungen in Satz 1 beschließen, die Kommission nicht in jedem Fall darüber zu unterrichten.

6.9. Im Falle eines unerwarteten technischen Ausfalls einer Komponente des dezentralen IT-Systems, für die Eurojust zuständig ist, unterrichtet Eurojust die Kommission und die Mitgliedstaaten unverzüglich über den Ausfall und, falls bekannt, über den voraussichtlichen Zeitraum bis zur Wiederherstellung.

6.10. Im Falle eines unerwarteten technischen Ausfalls der Datenbank der zuständigen Behörden/Gerichtsdatenbank unterrichtet die Kommission Eurojust und die Mitgliedstaaten umgehend über den Ausfall und, sofern bekannt, über den voraussichtlichen Zeitraum bis zur Wiederherstellung.

6.11. Im Falle einer Unterbrechung des Dienstes sorgen die Mitgliedstaaten und Eurojust für eine rasche Wiederherstellung des Dienstes und einen minimalen Datenverlust gemäß den Vorgaben für die Wiederherstellungszeit und den Wiederherstellungspunkt.

6.12. Die Mitgliedstaaten und Eurojust ergreifen geeignete Maßnahmen, um die vorstehend genannten Verfügbarkeitsvorgaben zu erfüllen, und legen Verfahren für eine wirksame Reaktion auf Vorfälle fest.

7. **Datenbank der zuständigen Behörden/Gerichtsdatenbank (Court database, CDB)**

7.1. Gemäß Artikel 22a der Verordnung (EU) 2018/1727 ermöglicht das dezentrale IT-System die elektronische Kommunikation zwischen den zuständigen nationalen Behörden und Eurojust. Angesichts der Verpflichtungen zum Informationsaustausch zwischen den zuständigen nationalen Behörden und Eurojust gemäß den Artikeln 21, 21a und 22, aber auch der Rolle von Eurojust bei der Erleichterung und Unterstützung der Ausstellung und Erledigung von Rechtshilfeersuchen oder Ersuchen um gegenseitige Anerkennung gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2018/1727 müssen die beteiligten zuständigen Behörden bei der Nutzung des dezentralen IT-Systems klar erkennbar sein. Daher ist es von wesentlicher Bedeutung, für die Zwecke des dezentralen IT-Systems eine amtliche Datenbank mit Angaben zu diesen Behörden einzurichten.

7.2. Die CDB enthält folgende Informationen in strukturierter Form:

a) für die Zwecke von Artikel 8 Absätze 1, 3 und 4, Artikel 21, Artikel 21a und Artikel 22 der Verordnung (EU) 2018/1727 Informationen über die zuständigen nationalen Behörden, einschließlich der nationalen Anlaufstellen gemäß Artikel 20 der genannten Verordnung, sowie über die nationalen Mitglieder gemäß Artikel 7 ([4]) der genannten Verordnung,

b) gegebenenfalls Informationen, die zur Bestimmung der geografischen oder wesentlichen Zuständigkeitsbereiche der zuständigen Behörden erforderlich sind, oder andere relevante Kriterien, die für die Feststellung ihrer Zuständigkeit erforderlich sind,

c) Informationen, die für die ordnungsgemäße technische Weiterleitung von Nachrichten innerhalb des dezentralen IT-Systems erforderlich sind.

7.3. Die Kommission ist für die Entwicklung, die Pflege, den Betrieb und den Support der CDB zuständig.

7.4. Die CDB ermöglicht es den Mitgliedstaaten und Eurojust, Informationen zu aktualisieren, und den am dezentralen IT-System beteiligten zuständigen nationalen Behörden und nationalen Mitgliedern, programmgesteuert auf diese Informationen zuzugreifen und sie abzurufen.

7.5. Der Zugang zur CDB ist über ein gemeinsames Kommunikationsprotokoll möglich, unabhängig davon, ob die an das dezentrale IT-System angeschlossenen zuständigen Behörden ein nationales Back-End-System betreiben, und von einer Bereitstellung der Referenzimplementierungssoftware.

7.6. Die Mitgliedstaaten stellen sicher, dass die Informationen über ihre zuständigen Behörden in der CDB gemäß Nummer 7.2 vollständig, genau und auf dem neuesten Stand sind.

([4]) Dies gilt unbeschadet der Übertragung von Befugnissen vom nationalen Mitglied auf seinen Stellvertreter, sonstiges Personal am nationalen Verbindungsbüro oder ermächtigte Bedienstete von Eurojust.

ANHANG II

DIGITALE VERFAHRENSSTANDARDS

In Artikel 3 Absatz 9 der Verordnung (EU) 2022/850 sind digitale Verfahrensstandards als technische Spezifikationen für Geschäftsprozessmodelle und Datenschemata festgelegt, mit denen die elektronische Struktur der im Rahmen des e-CODEX-Systems ausgetauschten Daten bestimmt wird.

Dieser Anhang enthält die technischen Spezifikationen für Geschäftsprozessmodelle und die technischen Spezifikationen der Datenschemata.

1. **Technische Spezifikationen für die Geschäftsprozessmodelle gemäß Verordnung (EU) 2018/1727**

Die technischen Spezifikationen für Geschäftsprozessmodelle sind in den Nummern 1.1 bis 1.5 dargelegt. Darin werden die wichtigsten Aspekte definiert, die für die elektronische Kommunikation für die Zwecke der Verordnung (EU) 2018/1727 über das dezentrale IT-System erforderlich sind.

Das dezentrale IT-System ermöglicht den Informationsaustausch nur zwischen den zuständigen nationalen Behörden eines Mitgliedstaats und dem nationalen Mitglied aus diesem Mitgliedstaat.

1.1. *Informationsaustausch im Zusammenhang mit dem Europäischen Justiziellen Terrorismusregister (CTR) Artikel 21a der Verordnung (EU) 2018/1727*

1.1.1. Modell Übermittlung von CTR-Daten:

Die zuständige nationale Behörde übermittelt dem nationalen Mitglied für das CTR Daten über Terrorismusverfahren.

1.1.2. Modell Erhalt von CTR-Daten:

Das nationale Mitglied erhält die CTR-Daten.

1.1.3. Modell Ersuchen um Zustimmung:

Das nationale Mitglied ersucht um die Zustimmung seiner zuständigen nationalen Behörde.

1.1.4. Modell Erhalt Zustimmungsersuchen:

Die zuständige nationale Behörde erhält das Zustimmungsersuchen.

1.1.5. Modell Antwort auf Zustimmungsersuchen senden:

Die zuständige nationale Behörde sendet eine Antwort auf das Zustimmungsersuchen.

1.1.6. Modell Antwort auf Zustimmungsersuchen erhalten:

Das nationale Mitglied erhält die Antwort auf das Zustimmungsersuchen.

1.1.7. Modell Informationen über Verbindungen:

Das nationale Mitglied informiert die zuständige nationale Behörde über die Verbindung mit einem anderen Fall.

1.1.8. Modell Aktualisierung von CTR-Daten:

Die zuständige nationale Behörde übermittelt Daten, die aktualisiert oder gelöscht werden müssen, an ihr jeweiliges nationales Mitglied.

1.1.9. Modell Erhalt aktualisierter CTR-Daten:

Das nationale Mitglied erhält die CTR-Daten, die aktualisiert oder gelöscht werden müssen.

1.2. *Informationsaustausch im Zusammenhang mit schwerer Kriminalität Artikel 21 der Verordnung (EU) 2018/1727*

1.2.1. Modell Übermittlung von Daten über grenzüberschreitende schwere Kriminalität:

Die zuständige nationale Behörde übermittelt Eurojust Daten über grenzüberschreitende schwere Kriminalität.

1.2.2. Modell Erhalt von Daten über grenzüberschreitende schwere Kriminalität:

Das nationale Mitglied erhält die Daten über grenzüberschreitende schwere Kriminalität.

1.2.3. Modell Ersuchen um Zustimmung:

Das nationale Mitglied ersucht um die Zustimmung seiner zuständigen nationalen Behörde.

1.2.4. Modell Erhalt Zustimmungsersuchen:

Die zuständige nationale Behörde erhält das Zustimmungsersuchen.

1.2.5. Modell Antwort auf Zustimmungsersuchen senden:

Die zuständige nationale Behörde sendet eine Antwort auf das Zustimmungsersuchen.

1.2.6. Modell Antwort auf Zustimmungsersuchen erhalten:

Das nationale Mitglied erhält die Antwort auf das Zustimmungsersuchen.

1.2.7. Modell Informationen über Verbindungen:

Das nationale Mitglied informiert die zuständige nationale Behörde über die Verbindung zu einem anderen Fall.

1.2.8. Modell Aktualisierung von Daten über grenzüberschreitende schwere Kriminalität:

Die zuständige nationale Behörde übermittelt Daten, die aktualisiert oder gelöscht werden müssen, an ihr jeweiliges nationales Mitglied.

1.2.9. Modell Erhalt von Daten über schwere grenzüberschreitende Kriminalität:

Das nationale Mitglied erhält die Daten über grenzüberschreitende schwere Kriminalität, die aktualisiert oder gelöscht werden müssen.

1.3. *Austausch allgemeiner Informationen*

1.3.1. Modell Versand von Informationen:

Das nationale Mitglied sendet Informationen an die zuständige nationale Behörde und umgekehrt.

1.3.2. Modell Erhalt von Informationen:

Die zuständige nationale Behörde bzw. das nationale Mitglied erhält die Informationen.

1.3.3. Modell Antwort auf Informationen:

Die zuständige nationale Behörde antwortet auf die vom nationalen Mitglied erhaltenen Informationen und umgekehrt.

1.3.4. Modell Erhalt von Antworten:

Das nationale Mitglied erhält die Antwort von der zuständigen nationalen Behörde.

1.3.5. Modell Versand von Informationen:

Die zuständige nationale Behörde sendet dem nationalen Mitglied Informationen.

1.3.6. Modell Erhalt von Informationen:

Das nationale Mitglied erhält die Informationen.

1.3.7. Modell Antwort auf Informationen:

Das nationale Mitglied antwortet auf die von der zuständigen nationalen Behörde erhaltenen Informationen.

1.3.8. Modell Erhalt von Antworten:

Die zuständige nationale Behörde erhält die Antwort des nationalen Mitglieds.

1.4. *Unterstützung der Ausstellung oder Erledigung gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2018/1727*

Hinweis: Umfassen die in Nummer 1.5 beschriebenen Modelle für Erleichterung und Unterstützung den Austausch gesetzlicher Formblätter, die durch Rechtsakte der Union im Bereich der justiziellen Zusammenarbeit in Strafsachen festgelegt wurden, so verwenden die Modelle, soweit verfügbar, die einschlägigen Darstellungen strukturierter Daten und XML-Schemata, die für diese Rechtsakte entwickelt wurden, z. B. die für die Zwecke der Durchführung der Verordnung (EU) 2023/2844 oder anderer einschlägiger Instrumente festgelegt wurden.

1.5. *Modell Ersuchen um Erleichterung oder Unterstützung:*

1.5.1. Modell Übermittlung von Ersuchen um Erleichterung oder Unterstützung:

Die zuständige nationale Behörde übermittelt ein Ersuchen um Erleichterung oder Unterstützung an ihr jeweiliges nationales Mitglied.

1.5.2. Modell Erhalt von Ersuchen um Erleichterung oder Unterstützung:

Das nationale Mitglied erhält das Ersuchen um Erleichterung oder Unterstützung und leitet es an das nationale Mitglied des ersuchten Mitgliedstaats außerhalb von JUDEX weiter.

1.5.3. Modell Weiterleitung des Ersuchens um Erleichterung oder Unterstützung an die zuständige nationalen Behörde:

Das nationale Mitglied des ersuchten Mitgliedstaats sendet das Ersuchen an seine jeweils zuständige nationale Behörde.

1.5.4. Modell Erhalt von Ersuchen um Erleichterung oder Unterstützung:

Die zuständige nationale Behörde erhält das Ersuchen um Erleichterung oder Unterstützung.

1.5.5. Modell Versand einer Antwort auf ein Ersuchen um Erleichterung oder Unterstützung:

Die zuständige nationale Behörde sendet dem nationalen Mitglied des ersuchten Mitgliedstaats eine Antwort auf das oder Informationen zu dem Ersuchen.

1.5.6. Modell Erhalt einer Antwort auf ein Ersuchen um Erleichterung oder Unterstützung:

Das nationale Mitglied erhält von der zuständigen nationalen Behörde die Antwort auf oder Informationen über das Ersuchen um Erleichterung oder Unterstützung und übermittelt sie dem nationalen Mitglied des ersuchenden Mitgliedstaats außerhalb von JUDEX.

1.5.7. Modell Beantwortung eines Ersuchens um Erleichterung oder Unterstützung:

Das nationale Mitglied des ersuchenden Mitgliedstaats beantwortet die Informationen von der zuständigen nationalen Behörde über das Ersuchen um Erleichterung oder Unterstützung oder leitet diese Informationen weiter.

1.5.8. Modell Erhalt von Antworten:

Die zuständige nationale Behörde erhält die Antwort oder die Informationen über das Ersuchen um Erleichterung oder Unterstützung.

2. **Technische Spezifikationen für Datenschemata**

Die technischen Spezifikationen, die als Grundlage für die Entwicklung von XML-Schemadefinitionen (XSD) für die Digitalisierung der Verordnung (EU) 2018/1727 dienen sollen, sind in den Nummern 2.1 und 2.2 dieses Anhangs aufgeführt. In diesen Spezifikationen werden die Schlüsselelemente und alle sonstigen Informationen für eine umfassende Beschreibung zur Erstellung dieser Schemata festgelegt.

Die Beschreibung soll allgemein gehalten werden, damit die erstellten XSD geändert und erweitert werden können, ohne dass wesentliche Änderungen dieser Spezifikationen erforderlich sind.

Die Spezifikationen gelten für die vorgeschriebene Form der Schemata im Anhang der Verordnung (EU) 2018/1727, für vordefinierte Nachrichten und für Freitextnachrichten, die im Rahmen der genannten Verordnung ausgetauscht werden.

2.1. *Allgemeine Erwägungen*

Für alle vorzulegenden Schemata gelten folgende Bestimmungen:

2.1.1. Versionsverwaltung

Es ist ein Versionsattribut aufzunehmen, das das Schemaversionsmanagement erleichtert und es ermöglicht, das Schema in künftigen Iterationen entsprechend den betrieblichen Anforderungen zu aktualisieren. Das Versionsattribut gibt an, ob die neue Version abwärtskompatibel ist, wenn neue Funktionen oder Verbesserungen eingeführt werden.

2.1.2. Schemaerklärung und Metadaten

— Gegebenenfalls verwendet das Schema einschlägige Normen oder Vokabulare, die von e-CODEX zur Gewährleistung der Interoperabilität verlangt werden und die für die ordnungsgemäße Validierung der in diesem Schema definierten Elemente und Typen erforderlich sind. Dazu können zählen:

  — das EU-Kernvokabular zur E-Justiz,

  — unqualifizierte Datentypen,

  — eine Codeliste für die Sprachencodes der Europäischen Union.

— Gegebenenfalls kann das XML-Schema auch die einschlägigen ETSI-Standards befolgen, um deren Definitionen zu verwenden.

2.1.3. Anmerkungen und Dokumentation

— **Anmerkungen**: Jedes Element des Schemas muss in der Regel mit Anmerkungen versehen sein. Die Anmerkungen liefern vom Menschen lesbare Informationen über das Element, wobei oft der Zweck oder die Verwendung des Elements klar und prägnant definiert wird.

2.1.4. Nutzung und Anpassungsfähigkeit

Das Schema muss den unter den Buchstaben a bis d festgelegten Regeln entsprechen:

a) **Modulare Struktur**: Jeder Abschnitt ist mit spezifischen Funktionen zu konzipieren und kann unabhängig wiederverwendet oder angepasst werden. Dies soll die Anpassung des Schemas an verschiedene Anwendungsfälle erleichtern.

b) **Erweiterbarkeit**: Das Schema ist so zu gestalten, dass die Aufnahme neuer Elemente oder Attribute unterstützt wird, wenn in Zukunft zusätzliche Informationen benötigt werden. Dies muss dadurch erreicht werden, dass optionale Elemente und Sequenzen verwendet werden, die erweitert werden können, ohne bestehende Implementierungen unbrauchbar zu machen.

c) **Anpassbare Struktur**: Das Schema ist so zu gestalten, dass bei Bedarf die Hinzufügung oder Änderung von Elementen oder Datentypen möglich ist. Das Schema muss so strukturiert sein, dass Änderungen der Anforderungen ohne größere Neugestaltungen möglich sind.

d) **Fakultative Elemente**: Elemente innerhalb eines Schemas können als fakultativ gekennzeichnet werden, d. h. sie können je nach den spezifischen Umständen aufgenommen oder weggelassen werden.

Das Schema ist so zu gestalten, dass die Erfassung strukturierter Daten für spezifische Ersuchen möglich ist.

2.1.5. Änderungen

Wesentliche Merkmale des Schemas müssen Flexibilität, Modularität und einfache Anpassung sein. Komplexe Typen und optionale Elemente sind so in das Design aufzunehmen, dass sie für unterschiedliche Szenarien geeignet und gleichzeitig leicht zu ändern und zu erweitern sind.

2.2. *Austausch strukturierter Daten*

Die in den Nummern 2.2.1 und 2.2.2 genannten strukturierten Daten werden gemäß Artikel 22a Absatz 3 der Verordnung (EU) 2018/1727 bereitgestellt. Das Schema muss auch die Kennzeichnung von Datensätzen ermöglichen, die bei künftigen Aktualisierungen gelöscht werden sollen.

2.2.1. Daten des Europäischen Justiziellen Terrorismusregisters

Die folgenden technischen Spezifikationen für das Datenschema legen einen strukturierten Rahmen für die Erstellung des Schemas im XML-Format fest.

a) Abschnitt der obersten Ebene

Dieser Abschnitt der obersten Ebene entspricht den Angaben in Anhang III der Verordnung (EU) 2018/1727 für das Europäische Justizielle Terrorismusregister (CTR).

b) Struktur der Nachricht

Die Struktur der CTR-Daten besteht aus einer Abfolge von Elementen und umfasst mindestens Folgendes:

i) Angaben zur Identifizierung natürlicher Personen:

— Nachname (Familienname),

— Vorname(n),

— gegebenenfalls Aliasnamen,

— Geburtsdatum,

— Geburtsort (Gemeinde und Staat),

— Staatsangehörigkeit(en),

— Ausweisdokument (Art und Nummer des Dokuments),

— Geschlecht,

— Wohnsitz

ii) Angaben zur Identifizierung juristischer Personen:

— Name des Unternehmens,

— Rechtsform,

— Ort des Hauptsitzes

iii) Angaben zur Identifizierung sowohl natürlicher als auch juristischer Personen:

— Telefonnummern,

— E-Mail-Adressen,

— Angaben zu Konten bei Banken oder anderen Finanzinstitutionen,

— Stand des Verfahrens

iv) Informationen über die Straftat:

— Informationen zu juristischen Personen, die an der Vorbereitung oder Begehung einer terroristischen Straftat beteiligt sind,

— rechtliche Einstufung der Straftat nach dem nationalen Recht,

— Form schwerer Kriminalität gemäß der Liste in Anhang I,

— gegebenenfalls Zugehörigkeit zu einer terroristischen Vereinigung,

— Art des Terrorismus, z. B. dschihadistischer, separatistischer, linksradikaler oder rechtsradikaler Terrorismus,

— kurze Zusammenfassung des Falls

v) Informationen zum nationalen Verfahren:

— Stand des Verfahrens,

— zuständige Staatsanwaltschaft,

— Aktenzeichen,

— Tag der Einleitung des förmlichen Justizverfahrens,

— Verbindungen mit anderen einschlägigen Fällen

vi) Feld für zusätzliche Informationen (Freitext)

vii) Code der Vorabgenehmigung

2.2.2. Nach Artikel 21 der Verordnung (EU) 2018/1727 übermittelte Daten

a) Artikel 21 Absatz 4 der Verordnung (EU) 2018/1727 zur Einsetzung gemeinsamer Ermittlungsgruppen (im Folgenden „GEG“)

i) Abschnitt der obersten Ebene

Dieser Abschnitt der obersten Ebene entspricht den Informationen gemäß Artikel 21 Absatz 4 der Verordnung (EU) 2018/1727 über die Bildung gemeinsamer Ermittlungsgruppen.

ii) Struktur der Nachricht

Die Datenstruktur besteht aus einer Abfolge von Elementen und umfasst mindestens Folgendes:

— Für das Strafverfahren zuständige nationale Justizbehörde

— Nationales Aktenzeichen des Strafverfahrens

— Stand des Strafverfahrens

— Untersuchte Straftaten

— Andere an dem Fall beteiligte Länder

— Der Fall wurde bereits von Eurojust unterstützt?

— Wenn ja, Eurojust-Fallkennung?

— Wenn nein, handelt es sich um ein Unterstützungsersuchen?

— Von Europol unterstützter Fall?

— Wenn ja, operative Taskforce („OTF“) und/oder Netzanwendung für sicheren Datenaustausch („SIENA“)?

— GEG-Vereinbarung:

— Betroffene Staaten

— GEG-Parteien (für die Ermittlungen zuständige nationale Behörden)

— Nationales Aktenzeichen des Strafverfahrens, mit dem die GEG befasst ist

— Datum der Unterzeichnung

— Dauer

— Untersuchte Straftaten

— Kurze Zusammenfassung des Falls

— Hauptverdächtige in den von der GEG behandelten Strafverfahren (Vor- und Nachname, Geburtsdatum und -ort sowie gegebenenfalls andere relevante und notwendige Datenkategorien gemäß Anhang II)

— Ergebnisse der Arbeit der GEG:

— Schwierigkeiten/Verzögerungen in Bezug auf:

— Bildung der GEG

— Anforderung/Austausch von Beweismitteln innerhalb der GEG

— Einigung auf/Umsetzung einer gemeinsamen Strafverfolgungsstrategie

— Zulässigkeit/Unzulässigkeit/Bewertung von Beweismitteln der GEG in nationalen Verfahren

— Ergebnis von Gerichtsverfahren (erfolgreiche/erfolglose Strafverfolgungsmaßnahmen und Verurteilungen/Freisprüche)

iii) Code der Vorabgenehmigung

b) Artikel 21 Absatz 5 der Verordnung (EU) 2018/1727, schwere komplexe Fälle

i) Abschnitt der obersten Ebene

Dieser Abschnitt der obersten Ebene entspricht den Angaben nach Artikel 21 Absatz 5 der Eurojust-Verordnung, d. h. schwere komplexe Fälle.

ii) Struktur der Nachricht

Die Datenstruktur besteht aus einer Abfolge von Elementen und umfasst mindestens Folgendes:

— Für das Strafverfahren zuständige nationale Justizbehörde

— Nationales Aktenzeichen des Strafverfahrens

— Stand des Strafverfahrens

— Untersuchte Straftaten

— Andere an dem Fall beteiligte Länder

— Der Fall wurde bereits von Eurojust unterstützt?

— Wenn ja, Eurojust-Fallkennung?

— Wenn nein, handelt es sich um ein Unterstützungsersuchen?

— Von Europol unterstützter Fall?

— Wenn ja, operative Taskforce und/oder SIENA?

— Einschlägige Form der schweren Kriminalität

— Beteiligung einer organisierten kriminellen Gruppe

— Mafia-Typ

— Transnationale organisierte kriminelle Gruppe

— Auswirkungen auf EU-Ebene

— Hauptverdächtige im Strafverfahren (Vor- und Nachname, Geburtsdatum und -ort sowie gegebenenfalls andere relevante und notwendige Datenkategorien gemäß Anhang II)

— Kurze Zusammenfassung des Falls

— Andere beteiligte Länder

— Länder, mit denen bereits eine Zusammenarbeit besteht

— Zuständige Behörden in einem anderen Land

— Eingesetzte Instrumente der justiziellen Zusammenarbeit

— Anzahl der gestellten/eingegangenen Ersuchen

— Vorliegen verbundener Ermittlungen

— Länder, mit denen eine Zusammenarbeit aufgenommen werden soll/möglicherweise betroffene Länder

— Art der erforderlichen Zusammenarbeit (z. B. Auslieferung, Beweiserhebung, sonstige Zusammenarbeit)

— Vorliegen verbundener Ermittlungen

iii) Code der Vorabgenehmigung

c) Artikel 21 Absatz 6 Buchstabe a der Verordnung (EU) 2018/1727, Kompetenzkonflikte

i) Abschnitt der obersten Ebene

Dieser Abschnitt der obersten Ebene entspricht den Informationen gemäß Artikel 21 Absatz 6 Buchstabe a der Verordnung (EU) 2018/1727, (Kompetenzkonflikte).

ii) Struktur der Nachricht

Die Datenstruktur besteht aus einer Abfolge von Elementen und umfasst mindestens Folgendes:

— Für das Strafverfahren zuständige nationale Justizbehörde

— Nationales Aktenzeichen des Strafverfahrens

— Stand des Strafverfahrens (z. B. Ermittlung, Strafverfolgung, Gerichtsverfahren)

— Untersuchte Straftaten

— Andere an dem Fall beteiligte Länder

— Der Fall wurde bereits von Eurojust unterstützt?

— Wenn ja, Eurojust-Fallkennung?

— Wenn nein, handelt es sich um ein Unterstützungsersuchen?

— Von Europol unterstützter Fall?

— Wenn ja, operative Taskforce und/oder SIENA?

— Andere beteiligte Länder

— Zuständige nationale Behörden des anderen Landes, sofern bekannt

— Nationales Aktenzeichen des Strafverfahrens im anderen Land

— Verfahrensstadium in einem anderen Land, sofern bekannt

— Positiver oder negativer Konflikt

— Tatsächlicher oder potenzieller Konflikt

— Bereits durchgeführte Koordinierungsmaßnahmen (z. B. Konsultationen gemäß dem Rahmenbeschluss 2009/948/JI ([1]))

— Kurze Zusammenfassung des Falls

— Gemeinsame Hauptverdächtige (Vor- und Nachname, Geburtsdatum und -ort sowie gegebenenfalls andere relevante und notwendige Datenkategorien gemäß Anhang II)

iii) Code der Vorabgenehmigung

d) Artikel 21 Absatz 6 Buchstabe b, kontrollierte Lieferungen

i) Abschnitt der obersten Ebene

Dieser Abschnitt der obersten Ebene entspricht den Informationen gemäß Artikel 21 Absatz 6 Buchstabe b der Verordnung (EU) 2018/1727: Kontrollierte Lieferungen

ii) Struktur der Nachricht

Die Struktur für die Daten besteht aus einer Abfolge von Elementen und umfasst mindestens Folgendes:

— Für das Strafverfahren zuständige nationale Justizbehörde

— Nationales Aktenzeichen des Strafverfahrens

— Stand des Strafverfahrens (z. B. Ermittlung, Strafverfolgung, Gerichtsverfahren)

— Untersuchte Straftaten

— Andere an dem Fall beteiligte Länder

— Der Fall wurde bereits von Eurojust unterstützt?

— Wenn ja, Eurojust-Fallkennung?

— Wenn nein, handelt es sich um ein Unterstützungsersuchen?

— Von Europol unterstützter Fall?

— Wenn ja, operative Taskforce und/oder SIENA?

— Andere beteiligte Länder

— Herkunftsland/Transitland/Bestimmungsland

— Zuständige nationale Behörden in anderen Ländern

— Vorliegen verbundener Ermittlungen in anderen Ländern

([1]) Rahmenbeschluss 2009/948/JI des Rates vom 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren (ABl. L 328 vom 15.12.2009, S. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Art der gelieferten Waren (z. B. Drogen und Art/Geld/Waffen/Zigaretten/sonstige)

— Status der kontrollierten Lieferung (z. B. geplant, im Gange, ausgeführt)

— Ergebnis der kontrollierten Lieferung, sofern bereits erfolgt

— Angewandter Rechtsakt der justiziellen Zusammenarbeit

— Gemeinsame Hauptverdächtige (Vor- und Nachname, Geburtsdatum und -ort sowie gegebenenfalls andere relevante und notwendige Datenkategorien gemäß Anhang II)

iii) Code der Vorabgenehmigung

e) Artikel 21 Absatz 6 Buchstabe c der Verordnung (EU) 2018/1727, wiederholte Probleme mit Instrumenten der justiziellen Zusammenarbeit

i) Abschnitt der obersten Ebene

Dieser Abschnitt der obersten Ebene entspricht den Informationen gemäß Artikel 21 Absatz 6 Buchstabe c der Verordnung (EU) 2018/1727: Wiederholte Probleme mit Instrumenten der justiziellen Zusammenarbeit.

ii) Struktur der Nachricht

Die Datenstruktur besteht aus einer Abfolge von Elementen und umfasst mindestens Folgendes:

— Für das Strafverfahren zuständige nationale Justizbehörde

— Nationales Aktenzeichen des Strafverfahrens

— Stand des Strafverfahrens (z. B. Ermittlung, Strafverfolgung, Gerichtsverfahren)

— Untersuchte Straftaten

— Andere an dem Fall beteiligte Länder

— Der Fall wurde bereits von Eurojust unterstützt?

— Wenn ja, Eurojust-Fallkennung?

— Wenn nein, handelt es sich um ein Unterstützungsersuchen?

— Von Europol unterstützter Fall?

— Wenn ja, operative Taskforce und/oder SIENA?

— Andere beteiligte Länder

— Zuständige nationale Behörden, sofern bekannt

— Als Anordnungs- oder Vollstreckungsbehörde handelnd

— Instrument der justiziellen Zusammenarbeit (z. B. Europäischer Haftbefehl, Europäische Ermittlungsanordnung, Sicherstellung und Einziehung)

— Konkretes Ersuchen (d. h. welche Ermittlungsmaßnahme, welche Art von Sicherstellung, Europäischer Haftbefehl zur Vollstreckung einer Strafe oder zur Strafverfolgung)

— Ablehnung oder wiederholte Schwierigkeiten

— Bei Ablehnung: Welcher spezifische Grund wurde geltend gemacht?

— Kurze Beschreibung des Problems

— Ggf. andere nationale Behörden, die vom selben Problem betroffen sind

iii) Code der Vorabgenehmigung

2.3. *Codes für die Vorabgenehmigung*

Beim Datenaustausch mit Eurojust über JUDEX geben die zuständigen nationalen Behörden mittels Codes für die Vorabgenehmigung die weitere Bearbeitung, den Zugang und die Übermittlung von Daten nach Identifizierung einer Verbindung an. Die Codes für die Vorabgenehmigung geben an, ob und in welchem Umfang Informationen im Zusammenhang mit der Verbindung an andere zuständige nationale Behörden, andere Agenturen und Einrichtungen der Union, Drittländer oder internationale Organisationen weitergegeben werden dürfen.

2.4. *Vordefinierte Nachrichten*

Vordefinierte Nachrichten sind Darstellungen von Informationsaustauschen gemäß der Verordnung (EU) 2018/1727, für die der Rechtsakt jedoch keine spezifische Form vorsieht. Ihre Art und Anzahl werden im Rahmen der geschäftlichen und technischen Analyse festgelegt.

Die XLM-Schemadefinitionen (XSD) für vordefinierte Nachrichten sind so zu gestalten, dass Kohärenz, Struktur und Übereinstimmung mit den Geschäftsanforderungen gewährleistet sind.

Für diese Schemata gilt Folgendes:

a) Der Abschnitt der obersten Ebene in diesem Schema ist entsprechend dem jeweils definierten Nachrichtentyp zu benennen,

b) innerhalb dieser Struktur sind die für den spezifischen Nachrichtentyp erforderlichen Felder hinzuzufügen und zu definieren, um eine ordnungsgemäße Darstellung der Datenelemente zu gewährleisten.

2.5. *Freitextnachrichten*

Freitextnachrichten sind Darstellungen des Austauschs, die unstrukturierte oder teilweise strukturierte Inhalte ermöglichen, Flexibilität bieten und gleichzeitig den rechtlichen und geschäftlichen Anforderungen entsprechen. Die XSD für Freitextnachrichten sind so zu gestalten, dass Kohärenz und eine ordnungsgemäße Formatierung gewährleistet sind.

Für diese Schemata gilt Folgendes:

a) Der Abschnitt der obersten Ebene in diesem Schema ist entsprechend dem jeweils definierten Freitextnachrichtentyp zu benennen,

b) im Schema muss die erforderliche Struktur für die Freitextnachricht festgelegt sein, wobei erforderlichenfalls eine angemessene Anordnung der Elemente möglich sein muss,

c) innerhalb dieser Struktur sind die für die Art des spezifischen Freitextnachrichtentyps erforderlichen Felder hinzuzufügen und zu definieren, um eine ordnungsgemäße Darstellung des Datenelements zu gewährleisten.

ANHANG III

TECHNISCHE SPEZIFIKATIONEN FÜR FINGERABDRÜCKE UND LICHTBILDER

Den über das dezentrale IT-System ausgetauschten Nachrichten können gemäß den technischen Spezifikationen der Nummern 1 und 2 Anlagen beigefügt werden, einschließlich Dateien des Nationalen Instituts für Normen und Technologie (NIST), die Fingerabdrücke und Lichtbilder enthalten.

1. **Fingerabdrücke**

Fingerabdrücke, die Eurojust zum Zwecke der zuverlässigen Identifizierung von Personen, die Gegenstand von Strafverfahren im Zusammenhang mit terroristischen Straftaten sind, übermittelt werden können, müssen folgende Bedingungen erfüllen:

a) Die Fingerabdrücke werden in einer Datei mit digitalen Fingerabdruckbildern (NIST-Fingerabdruckdatei) bereitgestellt und gemäß dem Standard ANSI/NIST-ITL 1-2011, aktualisierte Version 2015 (oder neuere Version) übermittelt,

b) die NIST-Fingerabdruckdatei besteht aus bis zu zehn individuellen Fingerabdrücken; gerollt, flach oder in Kombination,

c) bei allen Fingerabdrücken ist gekennzeichnet, um welchen Finger es sich handelt,

d) die Fingerabdrücke werden durch Live-Scans oder mit Tinte auf Papier erfasst, sofern die mit Tinte auf Papier erfassten Fingerabdrücke in der erforderlichen Auflösung und mit der gleichen Qualität gescannt wurden,

e) die NIST-Fingerabdruckdatei ermöglicht die Aufnahme ergänzender Informationen wie die Bedingungen der Registrierung von Fingerabdrücken und die Methode für die Erfassung einzelner Fingerabdruckbilder,

f) die Fingerabdrücke besitzen eine Nennauflösung von 500 oder 1 000 ppi ([1]) (zulässige Abweichung +/– 10 ppi) mit 256 Graustufen,

g) der zu verwendende Kompressionsalgorithmus für Fingerabdruckbilder entspricht den Empfehlungen des National Institute of Standards and Technology (NIST). Fingerabdruckdaten mit einer Auflösung von 500 ppi werden mit dem WSQ-Algorithmus (ISO/IEC 19794-5:2005) komprimiert. Fingerabdruckdaten mit einer Auflösung von 1 000 ppi werden mit dem Bildkompressionsstandard JPEG 2000 (ISO/IEC 15444-1) und dem Kodierungssystem komprimiert. Die Zielkompressionsrate beträgt 15:1.

2. **Lichtbilder**

Die Lichtbilder, die Eurojust zum Zwecke der zuverlässigen Identifizierung von Personen, gegen die ein Strafverfahren im Zusammenhang mit terroristischen Straftaten anhängig ist, übermittelt werden können, müssen folgende Bedingungen erfüllen:

a) Nur ein Gesichtsbild wird in einer Fotodatei (der NIST-Fotodatei) bereitgestellt und gemäß dem ANSI/NIST-ITL 1-2011 Update 2015 oder einer neueren Version übermittelt.

b) Die Fotos sind entweder in Graustufen, Farbe oder Nahinfrarot.

c) Die Qualität der Fotos richtet sich nach den Anforderungen von ISO/IEC 19794-5:2011 Frontalaufnahme oder neueren Versionen.

d) Die NIST-Fotodatei ermöglicht die Aufnahme ergänzender Informationen, einschließlich des Datums, an dem das Bild aufgenommen wurde.

([1]) Pixel pro Zoll.

e) Die Fotos im Porträtmodus weisen eine Auflösung von mindestens 600 Pixel mal 800 Pixel und eine maximale Auflösung von 1 200 Pixel mal 1 600 Pixel auf.

f) Das Gesicht nimmt einen Raum innerhalb des Lichtbildes ein, der mindestens 120 Pixel zwischen der Mitte der Augen gewährleistet.

g) Der verwendete Algorithmus zur Komprimierung der Lichtbilder entspricht den Empfehlungen des National Institute of Standards and Technology (NIST). Lichtbilder werden nur einmal mit dem Bildkompressionsstandard JPG (ISO/IEC 10918) oder JPEG 2000 (ISO/IEC 15444) und dem Kodierungssystem mit einem maximal zulässigen Bildkompressionsverhältnis von 20:1 komprimiert.