Amtsblatt
der Europäischen Union

DE
Reihe L

2025/1550

29.7.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/1550 DER KOMMISSION

vom 28. Juli 2025

mit technischen Spezifikationen und sonstigen Anforderungen des dezentralen IT-Systems nach der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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 ([1]), insbesondere auf Artikel 25 Absatz 1 Buchstaben a, b, c und d,

in Erwägung nachstehender Gründe:

(1) Zur Einrichtung des dezentralen IT-Systems nach der Verordnung (EU) 2023/1543 müssen technische Spezifikationen, Maßnahmen und Zielvorgaben für die Umsetzung dieses Systems festgelegt und angenommen werden.

(2) Nach der Verordnung (EU) 2023/1543 sollte sich das dezentrale IT-System aus den IT-Systemen der Mitgliedstaaten und der Einrichtungen und sonstigen Stellen der Union sowie aus interoperablen e-CODEX-Zugangspunkten zusammensetzen, über die diese IT-Systeme miteinander vernetzt sind. Die technischen Spezifikationen und sonstigen Anforderungen des dezentralen IT-Systems sollten diesem Rahmen Rechnung tragen.

(3) Nach der Verordnung (EU) 2023/1543 sollten die Zugangspunkte des dezentralen IT-Systems auf autorisierten e-CODEX-Zugangspunkten nach Artikel 3 Nummer 3 der Verordnung (EU) 2022/850 des Europäischen Parlaments und des Rates ([2]) beruhen.

(4) Die Mitgliedstaaten können anstelle eines nationalen IT-Systems die von der Kommission entwickelte Referenzimplementierungssoftware als Back-End-System einsetzen. Damit die Interoperabilität gewährleistet ist, sollten für die nationalen IT-Systeme und die Referenzimplementierungssoftware dieselben technischen Spezifikationen und Anforderungen gelten, die in dieser Verordnung festgelegt sind.

(5) Um potenziellen technischen Problemen im Zusammenhang mit der Kapazität und Zuverlässigkeit des dezentralen IT-Systems entgegenzuwirken, muss eine Obergrenze für das Volumen der über dieses System übermittelten elektronischen Beweismittel festgelegt werden. Nach der Inbetriebnahme des Systems sollten die Häufigkeit und das Volumen der Übermittlungen überwacht und die Obergrenze gegebenenfalls angepasst werden, um die Effizienz des Systems zu maximieren.

(6) Damit das zentrale IT-System hochgradig interoperabel und effizienter wird, sollte vorgeschrieben werden, dass die entsprechenden ETSI-Normen befolgt werden. Künftige Entwicklungen sollten überwacht werden, und erforderlichenfalls sollte die Aufnahme zusätzlicher ETSI-Normen in Erwägung gezogen werden.

(7) Irland ist durch die Verordnung (EU) 2023/1543 gebunden und beteiligt sich daher an der Annahme dieser Verordnung.

(8) 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 ist Dänemark weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.

([1]) ABl. L 191 vom 28.7.2023, S. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/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).

(9) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([3]) angehört und hat am 25. Juni 2025 eine Stellungnahme abgegeben.

(10) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 26 der Verordnung (EU) 2023/1543 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Technische Spezifikationen des dezentralen IT-Systems

Die in Artikel 25 Absatz 1 der Verordnung (EU) 2023/1543 genannten technischen Spezifikationen, Anforderungen, Maßnahmen und Zielvorgaben des dezentralen IT-Systems für die Kommunikation im Sinne des Artikels 19 der genannten Verordnung sind im Anhang der vorliegenden Verordnung festgelegt.

Artikel 2

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 28. Juli 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

([3]) 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

TECHNISCHE SPEZIFIKATIONEN DES DEZENTRALEN IT-SYSTEMS

(nach Artikel 1)

1. Einleitung und Geltungsbereich

Dieser Anhang enthält die technischen Spezifikationen, Maßnahmen und Zielvorgaben des dezentralen IT-System für die Verfahren gemäß Verordnung (EU) 2023/1543.

Gemäß Verordnung (EU) 2023/1543, insbesondere Artikel 19, soll das dezentrale IT-System die schriftliche Kommunikation zwischen zuständigen Behörden und benannten Niederlassungen oder Vertretern, zwischen zuständigen Behörden sowie zwischen zuständigen Behörden und den zuständigen Einrichtungen oder sonstigen Stellen der Union ermöglichen.

2. 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“ im Sinne der Standards des World Wide Web Consortium steht für ein Nachrichtenprotokoll für den Austausch strukturierter Informationen über Webdienste in Computernetzen;

2.5. „Representational State Transfer“ („REST“) 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, Formularen, Schriftstücken und elektronischen Beweismitteln über das dezentrale IT-System;

2.8. „API“ steht für eine Anwendungsprogrammierschnittstelle, die auf einem gemeinsamen Datenaustauschstandard beruht und Diensteanbietern, die individuelle IT-Lösungen für den Austausch von Informationen und Daten im Zusammenhang mit Ersuchen um elektronische Beweismittel nutzen, den automatisierten Zugang zu den dezentralen IT-Systemen ermöglicht;

2.9. „webbasierte Schnittstelle“ steht für eine über HTTPS im Internet verfügbare Benutzerschnittstelle, die es Diensteanbietern ermöglicht, manuell auf das dezentrale IT-System zuzugreifen, um sicher mit den Behörden zu kommunizieren und Daten im Zusammenhang mit Ersuchen um elektronische Beweismittel auszutauschen, ohne eine eigene spezielle Infrastruktur einrichten zu müssen;

2.10. „ETSI-Standards“ stehen für technische Spezifikationen und Normen, die vom Europäischen Institut für Telekommunikationsnormen (ETSI) entwickelt wurden, um die Interoperabilität, Sicherheit und Effizienz der Informations- und Kommunikationstechnologien zu gewährleisten; sie bieten Frameworks, Protokolle und bewährte Verfahren für ein breites Spektrum von Technologien, darunter Mobilfunknetze, Funkkommunikation, Cybersicherheit und Internetinfrastruktur;

2.11. „Hash-Wert“ steht für einen Ergebniswert fester Länge, der von einer kryptografischen Hash-Funktion erzeugt wird, wenn sie auf eine Eingangsnachricht beliebiger Länge angewandt wird; eine kryptografische Hash-Funktion ist so konzipiert, dass sie grundlegende Sicherheitseigenschaften, darunter eine Urbildresistenz (preimage resistance), eine schwache Kollisionsresistenz (second preimage resistance) und eine starke Kollisionsresistenz (collision resistance), besitzt und damit gut gegen Inversion und Kollisionsangriffe geschützt ist;

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

2.13. „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;

2.14. „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 und die systemübergreifende B2B-Integration unterstützt;

2.15. „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;

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

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

3. **Methoden der elektronischen Kommunikation**

3.1. Für die Zwecke der schriftlichen Kommunikation zwischen den zuständigen Behörden der Mitgliedstaaten, zwischen den zuständigen Behörden und den benannten Niederlassungen oder Vertretern von Diensteanbietern sowie zwischen den zuständigen Behörden und den Einrichtungen oder sonstigen Stellen der Union verwendet das dezentrale IT-System dienstbasierte Kommunikationsmethoden wie Webdienste oder andere wiederverwendbare Komponenten und Softwarelösungen zum Datenaustausch. Insbesondere wird die Kommunikation über die e-CODEX-Zugangspunkte gemäß Artikel 5 Absatz 2 der Verordnung (EU) 2022/850 erfolgen. Um einen wirksamen und interoperablen grenzüberschreitenden Datenaustausch zu gewährleisten, muss das dezentrale IT-System die Kommunikation über das e-CODEX-System unterstützen.

3.2. Angesichts des voraussichtlich hohen Volumens elektronischer Beweismittel, die gemäß Artikel 19 Absätze 1 und 4 der Verordnung (EU) 2023/1543 auf eine Europäische Herausgabeanordnung hin über das dezentrale IT-System übermittelt werden sollen, was zu technischen Kapazitätsengpässen mit negativen Folgen für das dezentrale IT-System führen könnte, werden über dieses System nur elektronische Beweismittel übermittelt, die die Obergrenze von 25 Megabyte (25 600 Kilobyte) nicht überschreiten. Die Übermittlung elektronischer Beweismittel, die diese Obergrenze überschreiten, erfolgt gemäß Artikel 19 Absatz 5 der genannten Verordnung.

3.3. Erfolgt gemäß Artikel 19 Absatz 6 der Verordnung (EU) 2023/1543 eine Übermittlung mit alternativen Mitteln, weil das dezentrale IT-System aus einem der in Artikel 19 Absatz 5 genannten Gründe nicht genutzt werden kann,

3.3.1. erfasst der Ersteller der Übermittlung, sofern diese die schriftliche Kommunikation zwischen zuständigen Behörden und Diensteanbietern, einschließlich des Austauschs von Formularen, im Sinne des Artikels 19 Absatz 1 der Verordnung (EU) 2023/1543 betrifft, die Übermittlung in seinem nationalen IT-System, das Teil des dezentralen IT-Systems ist; die erfassten Informationen umfassen mindestens eine Fallnummer oder ein Aktenzeichen, das Datum und die Uhrzeit der Übermittlung, den Absender und den Empfänger sowie den Namen und die Größe der Datei;

3.3.2. erfasst der Ersteller der Übermittlung, sofern diese die schriftliche Kommunikation zwischen zuständigen Behörden, einschließlich des Austauschs von Formularen, oder die schriftliche Kommunikation mit den zuständigen Einrichtungen oder sonstigen Stellen der Union im Sinne des Artikels 19 Absatz 4 der Verordnung (EU) 2023/1543 betrifft, die Übermittlung im dezentralen IT-System, und zwar in seinem nationalen IT-System oder gegebenenfalls in einem von einer zuständigen Einrichtung oder sonstigen Stelle der Union betriebenen IT-System; die erfassten Informationen umfassen mindestens eine Fallnummer oder ein Aktenzeichen, das Datum und die Uhrzeit der Übermittlung, den Absender und den Empfänger sowie den Namen und die Größe der Datei;

3.3.3. gilt, sofern elektronische Beweismittel aufgrund einer Europäischen Herausgabeanordnung über alternative Kommunikationsmittel zwischen Diensteanbietern und den zuständigen Behörden des Anordnungsstaats ([1]) übermittelt wurden oder elektronische Beweismittel im Rahmen des Vollstreckungsverfahrens gemäß Artikel 16 Absatz 9 der Verordnung (EU) 2023/1543 über alternative Mittel von der Vollstreckungsbehörde an die zuständigen Behörden des Anordnungsstaats übermittelt werden, für den Ersteller Folgendes:

a) Er erfasst folgende Informationen in einem Verzeichnis und übermittelt es der Behörde, der die elektronischen Beweismittel übermittelt oder zur Verfügung gestellt wurden:

(1) Angaben zum Absender und zum Empfänger;

(2) Metadaten, die die bereitgestellten elektronischen Beweismittel mit einer bestimmten Europäischen Herausgabe- oder Sicherungsanordnung verknüpfen;

(3) Datum und Uhrzeit der Übermittlung oder Angabe, wann die elektronischen Beweismittel dem Empfänger zur Verfügung gestellt wurden;

(4) Angaben zu den Übermittlungswegen (z. B. Aufzeichnung der sicheren Verbindung, über die die elektronischen Beweismittel bereitgestellt wurden, Nachweis des Empfangs oder der Zustellung durch Postdienste usw. ([2]));

(5) den oder die vollständigen Dateinamen der elektronischen Beweismittel, die dem vorgesehenen Empfänger im Anordnungsstaat übermittelt oder auf andere Weise zur Verfügung gestellt wurden;

(6) die Datengröße der elektronischen Beweismittel, die dem vorgesehenen Empfänger im Anordnungsstaat übermittelt oder auf andere Weise zur Verfügung gestellt wurden;

(7) mindestens einen Hash-Wert der übermittelten oder bereitgestellten Daten und Angaben zum verwendeten Hash-Algorithmus; der oder die für die Berechnung dieses Hash-Werts verwendeten Hash-Algorithmen müssen kryptografisch stark und gängig sein und dürfen keine öffentlich bekannt gegebenen Schwächen wie Kollisionen aufweisen (z. B. SHA-512, SHA3-512, BLAKE2 oder RIPEMD-160, aber je nach technologischer Entwicklung möglicherweise auch ein stärkerer).

b) Gegebenenfalls gibt er in dem unter Buchstabe a genannten Verzeichnis das Datum und die Uhrzeit an, bis zu der die elektronischen Beweismittel zugänglich bleiben. Diese Frist gibt der zuständigen Behörde des Anordnungsstaats einen angemessenen Zeitrahmen für die Abrufung der elektronischen Beweismittel, der mindestens 10 Kalendertage und höchstens 45 Kalendertage ab dem Zeitpunkt der Bereitstellung der elektronischen Beweismittel beträgt. Auf Antrag der zuständigen Behörde des Anordnungsstaats kann die vom Ersteller angegebene Frist im Einzelfall verlängert werden.

c) Er kann alle zusätzlichen Informationen oder Bemerkungen, die für den Fall relevant sind, in dem Verzeichnis gemäß vorstehendem Buchstaben a erfassen und der Behörde, der die elektronischen Beweismittel übermittelt oder zur Verfügung gestellt wurden, übermitteln.

3.4. Gemäß Artikel 28 der Verordnung (EU) 2023/1543 muss die Referenzimplementierungssoftware die in Artikel 28 Absatz 2 genannten Statistiken sowohl in strukturierten (z. B. XML) als auch unstrukturierten Datenformaten (z. B. PDF) programmgesteuert erheben, übermitteln oder anderweitig zugänglich machen. Gemäß Artikel 28 Absatz 3 der Verordnung (EU) 2023/1543 können von den Mitgliedstaaten betriebene nationale Portale ([3]), die dafür technisch ausgerüstet sind, diese Statistiken der Kommission auch über ein automatisiertes Verfahren übermitteln oder bereitstellen. Die Kommission gibt Leitlinien zur Datenstruktur und zur Methode für die Erhebung und Übermittlung dieser Statistiken heraus.

([1]) Zur Klarstellung sei darauf hingewiesen, dass Bezugnahmen auf zuständige nationale Behörden so zu verstehen sind, dass sie entsprechend auch für die nationalen Mitglieder von Eurojust, die Europäischen Staatsanwälte und die Delegierten Europäischen Staatsanwälte gelten, sofern diese befugt sind, dieselben Aufgaben nach Unionsrecht und nationalem Recht wahrzunehmen.

([2]) Es ist zu beachten, dass die Übermittlung über solche alternativen Kommunikationsmittel gemäß Artikel 19 Absatz 5 den Erfordernissen einer raschen, sicheren und zuverlässigen Übermittlung genügen muss, die es dem Empfänger ermöglicht, die Echtheit festzustellen.

([3]) Unter nationalen Portalen sind die nationalen IT-Systeme zu verstehen, die Teil des dezentralen IT-Systems im Sinne von Artikel 3 Nummer 21 der Verordnung (EU) 2023/1543 sind.

4. **Kommunikationsprotokolle**

4.1. Das dezentrale IT-System verwendet sichere Internetprotokolle für

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

b) die Kommunikation innerhalb des dezentralen IT-Systems zwischen den zuständigen Behörden und den Einrichtungen und sonstigen Stellen der Union,

c) die Kommunikation zwischen zuständigen Behörden und Diensteanbietern über eine API und die webbasierte Schnittstelle und

d) die Kommunikation mit der Gerichtsdatenbank.

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, insbesondere auf diejenigen, auf die europäische Normungsorganisationen wie ETSI verweisen.

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 für elektronische Beweismittel werden gegebenenfalls einschlägige Standards oder Vokabulare verwendet, die für die ordnungsgemäße Validierung der in diesem Schema festgelegten Elemente und Typen erforderlich sind, beispielsweise:

a) das EU-Kernvokabular zur E-Justiz;

b) unqualifizierte Datentypen;

c) eine Codeliste für die Sprachencodes der Europäischen Union.

Gegebenenfalls können die XML-Schemata auch die einschlägigen ETSI-Standards befolgen, um deren Definitionen zu verwenden.

4.6. Die Kommission legt die Spezifikationen für die gemeinsame API fest, die die Vollstreckungsstaaten den Diensteanbietern für den Zugang zum dezentralen IT-System zur Verfügung stellen müssen. Diese API beruht auf ETSI TS 104 144 („Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers“), soweit das möglich und sinnvoll ist.

4.7. 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) Public-Key-Infrastruktur 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 (Nachrichten, Formulare, Dokumente und elektronische Beweismittel) im Ruhezustand und bei der Übertragung;

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 zur Sicherstellung der Verfügbarkeit, indem der kontinuierliche Zugang zu Diensten und Daten sichergestellt und Störungen aufgrund von Cyberangriffen oder Ausfällen verhindert werden;

e) Maßnahmen zur Gewährleistung der Protokollierung sicherheitsrelevanter Ereignisse im Einklang mit den anerkannten internationalen Empfehlungen für IT-Sicherheitsstandards;

f) 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. 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.

5.4. 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 ([4]) bzw. der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ([5]) nachzukommen.

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

5.6. Eurojust und die Europäische Staatsanwaltschaft ergreifen bezüglich ihrer Beteiligung am dezentralen IT-System die erforderlichen Maßnahmen, um sicherzustellen, dass ihre jeweiligen IT-Systeme den Anforderungen der Verordnung (EU) 2018/1725 und ihrer Gründungsrechtsakte entsprechen.

5.7. Die Mitgliedstaaten, Eurojust und die Europäische Staatsanwaltschaft 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. **Verschlüsselung elektronischer Beweismittel** ([6])

6.1. Unbeschadet der Sicherheitsmaßnahmen des dezentralen IT-Systems können die zuständigen Behörden beim Erlass einer Europäischen Herausgabeanordnung zusätzlich ein spezielles öffentliches X.509-Zertifikat für die asymmetrische Verschlüsselung elektronischer Beweismittel bereitstellen.

([4]) 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).

([5]) 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).

([6]) Der Klarheit halber sei ergänzt, dass sich der Begriff „elektronische Beweismittel“ auf den Begriffsumfang nach Artikel 3 Nummer 8 der Verordnung (EU) 2023/1543 beschränkt.

6.2. Der Erlass, die Verwaltung, die Überprüfung und alle damit zusammenhängenden Aspekte der unter Nummer 6.1 genannten Zertifikate sowie die entsprechende Public-Key-Infrastruktur fallen in die alleinige Zuständigkeit des Anordnungsstaats.

6.3. Unbeschadet künftiger technologischer Entwicklungen unterstützen die öffentlichen Zertifikate branchenübliche Verschlüsselungsalgorithmen wie RSA (Rivest-Shamir-Adleman) oder ECDH (Elliptic Curve Diffie-Hellman) für ECC (Elliptic Curve Cryptography).

6.4. Die öffentlichen Zertifikate enthalten die passende „keyUsage"-Erweiterung, etwa „keyEncipherment" oder „dataEncipherment" für RSA-basierte Zertifikate und „keyAgreement" für ECC-basierte Zertifikate. Die Zertifikate werden im Format PEM (Privacy-Enhanced Mail) oder DER (Distinguished Encoding Rules) bereitgestellt.

6.5. Hat die Anordnungsbehörde ein öffentliches X.509-Zertifikat bereitgestellt und übermittelt ein Diensteanbieter elektronische Beweismittel aufgrund einer Europäischen Herausgabeanordnung, so verschlüsselt der Anbieter die elektronischen Beweismittel vor der Übermittlung dieser Daten über das dezentrale IT-System mithilfe des entsprechenden vom Anordnungsstaat bereitgestellten öffentlichen X.509-Zertifikats.

6.6. Wenn die Anordnungsbehörde ein öffentliches X.509-Zertifikat bereitgestellt hat, die Übermittlung elektronischer Beweismittel in verschlüsselter Form jedoch aus technischen oder anderen gerechtfertigten Gründen und unbeschadet der Bestimmung in Artikel 19 Absatz 5 der Verordnung (EU) 2023/1543 nicht möglich ist, kann der Diensteanbieter die Daten ohne Inhaltsverschlüsselung übermitteln. In diesem Fall legt der Diensteanbieter der Anordnungsbehörde eine Erklärung mit den Gründen vor.

7. **Mindestverfügbarkeitsvorgaben**

7.1. Die Mitgliedstaaten, Eurojust und die Europäische Staatsanwaltschaft 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.

7.2. 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.

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

7.4. Die Mitgliedstaaten, Eurojust und die Europäische Staatsanwaltschaft unterrichten die Kommission 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;

7.5. Verfügen die Mitgliedstaaten, Eurojust oder die Europäische Staatsanwaltschaft über feste Zeitfenster für die regelmäßige Wartung, so unterrichten sie die Kommission und die Teilnehmer des dezentralen IT-Systems über die Uhrzeit und die Tage, an denen solche festen Zeitfenster geplant sind. Sollten Komponenten des dezentralen IT-Systems, für die die Mitgliedstaaten, Eurojust oder die Europäische Staatsanwaltschaft zuständig sind, während eines solchen festen Zeitfensters nicht verfügbar sein, so können diese ungeachtet der Verpflichtungen unter Nummer 7.4 beschließen, die Kommission nicht in jedem Fall darüber zu unterrichten.

7.6. Im Falle eines unerwarteten technischen Ausfalls der Komponenten des dezentralen IT-Systems, für die die Mitgliedstaaten, Eurojust oder die Europäische Staatsanwaltschaft zuständig sind, unterrichten sie die Kommission und die Teilnehmer des dezentralen IT-Systems umgehend über diesen Ausfall und, sofern bekannt, über den voraussichtlichen Zeitraum bis zur Wiederherstellung.

7.7. Im Falle von Wartungstätigkeiten oder eines unerwarteten technischen Versagens von Komponenten innerhalb des dezentralen IT-Systems, für die ein Mitgliedstaat zuständig ist, die sich nachteilig auf die Verfügbarkeit der API und/oder der webbasierten Schnittstelle für Diensteanbieter auswirken, stellt der betreffende Mitgliedstaat diese Informationen unverzüglich auf einer Website zur Verfügung und/oder übermittelt sie unverzüglich den in seinem Hoheitsgebiet tätigen Diensteanbietern.

7.8. Im Falle eines unerwarteten technischen Ausfalls der Gerichtsdatenbank unterrichtet die Kommission die Mitgliedstaaten, Eurojust und die Europäische Staatsanwaltschaft umgehend darüber, dass die Datenbank nicht verfügbar ist und, sofern bekannt, über den voraussichtlichen Zeitraum bis zur Wiederherstellung.

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

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

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

8.1. Hinsichtlich Artikel 19 der Verordnung (EU) 2023/1543 ist es für das Funktionieren des dezentralen IT-Systems unerlässlich, eine amtliche Datenbank mit den Diensteanbietern und zuständigen Behörden einzurichten.

8.2. Die amtliche Datenbank der zuständigen Behörden enthält folgende Informationen in strukturierter Form:

a) für die Zwecke des Artikels 19 der Verordnung (EU) 2023/1543 Informationen über die zuständigen Behörden, die gemäß Artikel 31 Absatz 1 Buchstaben a bis c mitgeteilt wurden, auch in Bezug auf

(1) die nationalen Mitglieder von Eurojust einschließlich der Angabe, ob sie nach nationalem Recht zum Erlass von Europäischen Herausgabeanordnungen und Europäischen Sicherungsanordnungen gemäß Artikel 8 Absätze 3 und 4 der Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates ([7]) befugt sind;

(2) die Delegierten Europäischen Staatsanwälte und die Europäischen Staatsanwälte, die von den Mitgliedstaaten gemäß Artikel 105 Absatz 3 der Verordnung (EU) 2017/1939 des Rates ([8]) als zuständige Anordnungsbehörde im Sinne der Verordnung (EU) 2023/1543 notifiziert wurden;

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

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

8.2.1. Die unter Nummer 8.2 Buchstabe c genannten Informationen umfassen Folgendes:

a) Informationen über den Mitgliedstaat, in dem die benannte Niederlassung des Diensteanbieters niedergelassen ist oder in dem sein gesetzlicher Vertreter ansässig ist:

(1) Mitgliedstaat

(2) zentrale Behörde

([7]) 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 (ABl. L 295 vom 21.11.2018, S. 138).

([8]) Verordnung (EU) 2017/1939 des Rates vom 12. Oktober 2017 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA) (ABl. L 283 vom 31.10.2017, S. 1).

b) Informationen über den Diensteanbieter:

(1) Name

(2) Anschrift/Sitz

(3) Registriernummer

(4) Rechtsform

(5) Telefonnummer

(6) E-Mail-Adresse

c) Informationen über die benannte Niederlassung/den Vertreter:

(1) Art des Rechtsträgers (Benannte Niederlassung/Vertreter)

(2) Name

(3) Anschrift/Sitz

(4) Telefonnummer

(5) E-Mail-Adresse

(6) allgemeine Kontaktperson/Kontaktstelle

(7) von dem Diensteanbieter/der benannten Niederlassung/dem Vertreter akzeptierte Amtssprache(n)

(8) in der Union angebotene Dienstleistungen gemäß Artikel 2 Nummer 1 der Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates ([9])

(9) Art der EU-Rechtsinstrumente, für die die benannte Niederlassung/der Vertreter benannt wird (in Situationen, in denen die Mitgliedstaaten nicht an allen einschlägigen EU-Rechtsinstrumenten beteiligt sind)

(10) räumlicher Geltungsbereich der Benennung/Ernennung

d) Authentifizierung der Informationen:

(1) Name des Bevollmächtigten

(2) Stellenbezeichnung

(3) Anschrift

(4) Telefonnummer

(5) E-Mail-Adresse

(6) Datum

8.2.2. Soweit verfügbar, können die unter Nummer 8.2 Buchstabe c genannten Informationen Folgendes umfassen:

a) Informationen über den Diensteanbieter:

(1) Ansprechpartner für Anfragen zu den Mitteilungen (falls nicht mit dem Unterzeichner identisch)

(2) Webseite

b) Arten der verfügbaren Daten:

(1) für jede betroffene Dienstleistung:

— Arten der verfügbaren Daten

— Datenkategorie

— Identifikatoren

— Zeitraum der Datenverfügbarkeit

([9]) Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren (ABl. L 191 vom 28.7.2023, S. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

(2) zusätzliche Informationen über die Daten

(3) zusätzliche Informationen über die Dienstleistung (z. B. Unterverträge)

c) Informationen über die benannte Niederlassung/den Vertreter:

(1) andere Diensteanbieter, für die diese benannte Niederlassung oder dieser Vertreter benannt wurde

(2) Kontaktdaten für technische Hilfe

(3) Notfallkontakt

d) technische Angaben:

(1) Name der technischen Kontaktstelle

(2) Telefonnummer der technischen Kontaktstelle

(3) E-Mail-Adresse der technischen Kontaktstelle

(4) API-URL für dynamische Abfragen zu den Arten der Daten

(5) Art der Verbindung mit dem nationalen IT-System:

— webbasierte Schnittstelle

— API

— Push-API-URL

8.3. Hinsichtlich der operativen Erfordernisse des dezentralen IT-Systems gilt Folgendes:

a) Die Kommission ist für die Entwicklung, die Pflege, den Betrieb und den Support der amtlichen Datenbank zuständig.

b) Die Kommission ermöglicht den Zugriff auf die amtliche Datenbank über eine API, die den zuständigen Behörden, Eurojust und der Europäischen Staatsanwaltschaft für die Zwecke ihrer Teilnahme am dezentralen IT-System zur Verfügung gestellt wird.

c) Die Mitgliedstaaten stellen sicher, dass die Informationen über ihre zuständigen Behörden gemäß Nummer 8.2 Buchstaben a und b in der amtlichen Datenbank vollständig und genau sind und auf dem neuesten Stand gehalten werden.

d) Die amtliche Datenbank ermöglicht es den Mitgliedstaaten, Informationen über ihre Diensteanbieter bereitzustellen und zu aktualisieren, und den am dezentralen IT-System beteiligten Behörden, programmgesteuert auf diese Informationen zuzugreifen und sie abzurufen.

e) Die Mitgliedstaaten und Diensteanbieter stellen sicher, dass die unter Punkt 8.2 Buchstabe c genannten Informationen in der amtlichen Datenbank vollständig und genau sind und auf dem neuesten Stand gehalten werden.