II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) 2022/1463 DER KOMMISSION

vom 5. August 2022

zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 ([1]), insbesondere auf Artikel 14 Absatz 9,

in Erwägung nachstehender Gründe:

(1) Gemäß Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 ist die Kommission verpflichtet, in Zusammenarbeit mit den Mitgliedstaaten ein technisches System für den grenzüberschreitenden automatisierten Austausch von Nachweisen einzurichten, das für die in Anhang II der genannten Verordnung aufgeführten Online-Verfahren und die in den Richtlinien 2005/36/EG ([2]), 2006/123/EG ([3]), 2014/24/EU ([4]) und 2014/25/EU ([5]) des Europäischen Parlaments und des Rates vorgesehenen Verfahren erforderlich ist.

(2) In den in dieser Verordnung enthaltenen technischen und operativen Spezifikationen des technischen Systems zur einmaligen Erfassung („once-only" technical system; im Folgenden OOTS) sollten die Hauptkomponenten der Architektur des OOTS festgelegt und die technischen und operativen Aufgaben und Verantwortlichkeiten der Kommission, der Mitgliedstaaten, der Nachweise anfordernden Behörden, der Nachweislieferanten und der intermediären Plattformen festgelegt werden. Darüber hinaus sollte im Rahmen dieser Spezifikationen ein Protokollsystem zur Überwachung des Austauschs eingerichtet und die Verantwortung für die Wartung, den Betrieb und die Sicherheit des OOTS abgegrenzt werden.

(3) Um die Einrichtung des OOTS bis zu dem in der Verordnung (EU) 2018/1724 festgelegten Datum zu ermöglichen, ist vorgesehen, diese Verordnung um detailliertere, nicht verbindliche technische Entwurfsdokumente zu ergänzen, die von der Kommission in Zusammenarbeit mit den Mitgliedstaaten im Rahmen der Koordinierungsgruppe für das Zugangstor und im Einklang mit den Leitlinien der Kommission für die Umsetzung des Arbeitsprogramms der Verordnung über das einheitliche digitale Zugangstor 2021-2022 einvernehmlich erstellt werden. Wird dies jedoch aufgrund neuer technischer Entwicklungen oder aufgrund von Debatten oder Meinungsverschiedenheiten innerhalb der Koordinierungsgruppe für das Zugangstor als notwendig erachtet — insbesondere im Hinblick auf die

([1]) ABl. L 295 vom 21.11.2018, S. 1.

([2]) Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. L 255 vom 30.9.2005, S. 22).

([3]) Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (ABl. L 376 vom 27.12.2006, S. 36).

([4]) Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

([5]) Richtlinie 2014/25/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die Vergabe von Aufträgen durch Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste und zur Aufhebung der Richtlinie 2004/17/EG (ABl. L 94 vom 28.3.2014, S. 243).

Fertigstellung der technischen Entwurfsdokumente und wichtige Konzeptionsentscheidungen —, oder ergibt sich die Notwendigkeit, bestimmte Elemente der technischen Entwurfsdokumente verbindlich zu gestalten, so ist es möglich, die in dieser Verordnung festgelegten technischen und operativen Spezifikationen gemäß dem in Artikel 37 Absatz 2 der Verordnung (EU) 2018/1724 genannten Prüfverfahren zu ergänzen bzw. zu ändern.

(4) Um die Kosten und den Zeitaufwand für die Einrichtung des OOTS zu verringern, sollte die Architektur des OOTS so weit wie möglich auf wiederverwendbaren Lösungen beruhen, neutral in Bezug auf die Implementierungstechnologie sein und mit verschiedenen nationalen Lösungen kompatibel sein. Das OOTS sollte beispielsweise in der Lage sein, die bestehenden Verfahrensportale, Datendienste oder intermediären Plattformen auf nationaler Ebene — auch auf zentraler, regionaler und lokaler Ebene —, die für die nationale Nutzung eingerichtet wurden, zu nutzen. Die von der Kommission entwickelten Komponenten sollten im Rahmen einer offenen Softwarelizenz veröffentlicht werden, durch die die Wiederverwendung und die Zusammenarbeit gefördert werden.

(5) Eine solche wiederverwendbare Lösung, die auf Unionsebene entwickelt wurde, ist das System der eIDAS-Knoten, das in der Durchführungsverordnung (EU) 2015/1501 der Kommission ([6]) festgelegt wurde und durch die Kommunikation mit anderen Knoten des eIDAS-Netzes die Beantragung und die Bereitstellung einer grenzüberschreitenden Authentifizierung eines Nutzers verarbeiten kann. Die eIDAS-Knoten sollten es Nachweise anfordernden Behörden und gegebenenfalls Nachweislieferanten erleichtern, Nutzer zu identifizieren, die den Austausch von Nachweisen über das OOTS anfordern, damit die Nachweislieferanten die Identifizierungsdaten mit ihren bestehenden Datensätzen abgleichen können.

(6) Das OOTS sollte auf der bereits geleisteten Arbeit aufbauen und Synergien mit anderen bestehenden Systemen für den Austausch von Nachweisen oder Informationen zwischen Behörden, die für die in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 genannten Verfahren relevant sind, nutzen, darunter auch Systeme, die nicht unter Artikel 14 Absatz 10 der genannten Verordnung fallen. Zum Beispiel sollte das OOTS in Bezug auf Fahrzeug- und Führerscheinregisterdaten bereits entwickelten Datenmodellen Rechnung tragen und, soweit machbar, technische Brücken schaffen, um die Verknüpfung der zuständigen Behörden, die bereits andere bestehende Netze (RESPER ([7]) oder EUCARIS ([8])) nutzen, mit dem OOTS für die Bereitstellung von Nachweisen in den vom OOTS abgedeckten Verfahren zu erleichtern. Ein ähnlicher Ansatz sollte in Bezug auf andere Systeme verfolgt werden, unter anderem in Bezug auf: die Emrex-Nutzergruppe (Emrex User Group; EUG) ([9]) im Bildungswesen, den elektronischen Austausch von Sozialversicherungsdaten (Electronic Exchange of Social Security Information; EESSI) gemäß der Verordnung (EG) Nr. 987/2009 des Europäischen Parlaments und des Rates ([10]) im Bereich der sozialen Sicherheit, das Europäische Strafregisterinformationssystem, das durch den Beschluss 2009/316/JI des Rates ([11]) eingerichtet wurde, und eCertis ([12]), das bei öffentlichen Ausschreibungsverfahren eingesetzt wird. Die Zusammenarbeit zwischen diesen Systemen und dem OOTS sollte von Fall zu Fall festgelegt werden.

(7) Zum Zweck der grenzüberschreitenden Authentifizierung eines Nutzers sollte die Architektur des OOTS der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([13]) Rechnung tragen. Am 3. Juni 2021 nahm die Kommission eine Empfehlung für ein gemeinsames Instrumentarium der Union für ein koordiniertes Konzept für einen Rahmen für die europäische digitale Identität ([14]) an. Mit dieser Empfehlung wird ein strukturierter Prozess für die Zusammenarbeit zwischen den Mitgliedstaaten, der Kommission und gegebenenfalls dem Privatsektor geschaffen, die an den technischen Aspekten des Rahmens für die europäische digitale Identität

([6]) Durchführungsverordnung (EU) 2015/1501 der Kommission vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (ABl. L 235 vom 9.9.2015, S. 1).

([7]) EU-Führerscheinnetz, das auf der Grundlage von Artikel 15 der Richtlinie 2006/126/EG des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Führerschein (ABl. L 403 vom 30.12.2006, S. 18) eingerichtet wurde.

([8]) Vertrag über ein Europäisches Fahrzeug- und Führerscheininformationssystem (EUCARIS), angenommen in Luxemburg am 29. Juni 2000.

([9]) Die Emrex-Nutzergruppe (EUG) ist ein unabhängiges, internationales Netz, in dem verschiedene Akteure vereint sind, die an der Verbesserung der Übertragbarkeit von Studierendendaten beteiligt sind. Weitere Informationen sind abrufbar unter https://emrex.eu/.

([10]) Verordnung (EG) Nr. 987/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 zur Festlegung der Modalitäten für die Durchführung der Verordnung (EG) Nr. 883/2004 über die Koordinierung der Systeme der sozialen Sicherheit (ABl. L 284 vom 30.10.2009, S. 1).

([11]) Beschluss 2009/316/JI des Rates vom 6. April 2009 zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2009/315/JI (ABl. L 93 vom 7.4.2009, S. 33).

([12]) https://ec.europa.eu/tools/ecertis/#/homePage

([13]) 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).

([14]) Eine vertrauenswürdige und sichere europäische eID — Empfehlung |Gestaltung der digitalen Zukunft Europas (europa.eu).

mitwirken. Um für die notwendige Abstimmung zwischen diesem Prozess und dem OOTS zu sorgen, sollte die Kommission insbesondere über die Kontaktgruppe für Synergien und Interoperabilität (Synergies and Interoperability Contact Group) eine angemessene Koordinierung zwischen dem durch den Durchführungsbeschluss (EU) 2015/296 der Kommission ([15]) eingerichteten Kooperationsnetz und der Koordinierungsgruppe für das Zugangstor sicherstellen.

(8) Zur Gewährleistung der Sicherheit der grenzüberschreitenden Dienste für die Zustellung elektronischer Dokumente für die Zwecke des OOTS sollten die Mitgliedstaaten dafür Sorge tragen, dass diese Dienste den Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben gemäß Artikel 44 der Verordnung (EU) Nr. 910/2014 genügen. Zu diesem Zweck ist es angezeigt, im Rahmen des OOTS eDelivery-Zugangspunkte zu verwenden, um ein Netz von Knotenpunkten für den sicheren digitalen Datenaustausch zu schaffen. Die elektronische Zustellung (eDelivery) ermöglicht nicht nur eine sichere grenzüberschreitende Zustellung, sondern bietet auch Funktionen für Metadatendienste, die künftige Versionen des OOTS mit einer größeren Anzahl von sicheren Knoten für den Datenaustausch unterstützen können. Innerhalb dieses Rahmens sollten die Mitgliedstaaten die Möglichkeit haben, die Anbieter ihrer eDelivery-Software auszuwählen.

(9) Damit die Anwendung dieser Verordnung flexibel ist, sollten die Mitgliedstaaten entscheiden können, ob sie einen oder mehrere eDelivery-Zugangspunkte als Teil des OOTS einrichten möchten. Ein Mitgliedstaat sollte daher in der Lage sein, einen einzigen Zugangspunkt einzurichten, der alle mit dem OOTS zusammenhängenden eDelivery-Mitteilungen an die Nachweise anfordernden Behörden oder Nachweislieferanten über eine intermediäre Plattform verwaltet, oder alternativ mehrere Zugangspunkte auf einer beliebigen hierarchischen Ebene oder für bestimmte Bereiche, Sektoren oder geografische Ebenen seiner öffentlichen Verwaltungen einzurichten.

(10) Nach dem Unionsrecht, einschließlich der Richtlinien 2005/36/EG, 2006/123/EG, 2014/24/EU und 2014/25/EU sowie der Verordnung (EU) 2018/1724, müssen bestimmte Verwaltungsverfahren den Nutzern online zur Verfügung gestellt werden. Da diese Verfahren und die erforderlichen Nachweise im Unionsrecht nicht harmonisiert sind, sollten gemeinsame Dienste eingerichtet werden, um den grenzüberschreitenden Austausch der für diese Verfahren erforderlichen Nachweise über das OOTS zu ermöglichen.

(11) Gibt es keine vereinbarten Nachweisarten, die in der gesamten Union harmonisiert sind und die alle Mitgliedstaaten vorlegen können, sollte ein Nachweisdienst dabei helfen, zu bestimmen, welche Nachweisarten für ein bestimmtes Verfahren akzeptiert werden können.

(12) Der Nachweisdienst sollte auf den von den Mitgliedstaaten zur Verfügung gestellten Regelinhalten beruhen und einen Online-Mechanismus bereitstellen, mit dem die Mitgliedstaaten ihre Informationsanforderungen und Nachweisartensätze abfragen können. Der Nachweisdienst sollte die Mitgliedstaaten in die Lage versetzen, Informationen über die Vorschriften für bestimmte Nachweisarten zu verwalten und auszutauschen.

(13) In Fällen, in denen die Interoperabilität zwischen dem Verfahrensportal und den Datendiensten und den gemeinsamen Diensten erforderlich ist, sollte dies durch eine technische Entwurfsdokumentation unterstützt werden.

(14) In dieser Verordnung sollte festgelegt werden, wann strukturierte und unstrukturierte Nachweise, die für die in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 aufgeführten Verfahren erforderlich sind, als rechtmäßig in einem elektronischen Format ausgestellt gelten, das einen automatischen Austausch ermöglicht. Unstrukturierte Nachweise, die in einem elektronischen Format ausgestellt wurden, können über das OOTS ausgetauscht werden, wenn sie um die Metadatenelemente des allgemeinen Metadatenmodells des OOTS ergänzt werden, das in dem in Artikel 7 Absatz 1 dieser Verordnung genannten semantischen Datenspeicher enthalten ist. Strukturierte Nachweise können über das OOTS ausgetauscht werden, wenn sie um die Metadatenelemente des in Artikel 7 Absatz 1 dieser Verordnung genannten allgemeinen Metadatenmodells des OOTS ergänzt werden und entweder dem Datenmodell des OOTS für die betreffende Nachweisart gemäß Artikel 7 Absatz 2 dieser Verordnung entsprechen oder von einer vom Menschen lesbaren Fassung begleitet werden.

([15]) Durchführungsbeschluss (EU) 2015/296 der Kommission vom 24. Februar 2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung gemäß Artikel 12 Absatz 7 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (ABl. L 53 vom 25.2.2015, S. 14).

(15) Die Mitgliedstaaten sollten frei entscheiden können, wann sie Nachweise in ein elektronisches Format umwandeln, sodass ihr automatischer Austausch über das OOTS möglich ist. Da der Nutzen des OOTS für seine Nutzer jedoch erhöht werden soll und die Verwendung von Datenmodellen und Metadatenschemata sowohl für unstrukturierte als auch für strukturierte Formate allgemein nachdrücklich empfohlen wird, sollte die Kommission die Mitgliedstaaten bei ihren Bemühungen, auf dieses Ziel hinzuarbeiten, unterstützen.

(16) Um Überschneidungen zu vermeiden, Synergien sicherzustellen und den Nutzern Wahlmöglichkeiten zu bieten, sollten die Entwicklung von Datenmodellen des OOTS für strukturierte Nachweisarten und die Standardisierung von Anwendungsfällen für die Bereitstellung von Berechtigungsnachweisen gemäß dem strukturierten Prozess, der in der Empfehlung (EU) 2021/946 der Kommission vom 3. Juni 2021 für ein gemeinsames Instrumentarium der Union für ein koordiniertes Konzept für einen Rahmen für die europäische digitale Identität ([16]) vorgesehen ist, in enger Zusammenarbeit und Abstimmung untereinander erfolgen, soweit es sich um Nachweise handelt, die unter Artikel 14 der Verordnung (EU) 2018/1724 fallen; hierzu gehört auch die Ermittlung gemeinsamer Anwendungsfälle. Die Angleichung der Datenmodelle des technischen Systems (OOTS) und der standardisierten Anwendungsfälle im Rahmen der oben genannten Empfehlung der Kommission sollte es den Nutzern ermöglichen, sich auf alternative Mittel für die Lieferung der unter Artikel 14 der Verordnung (EU) 2018/1724 fallenden Nachweise zu stützen, entweder unabhängig vom OOTS oder in Kombination mit diesem. Wenn Änderungen an den Datenmodellen oder an Metadatenschemata für die im semantischen Datenspeicher enthaltenen Nachweise vorgenommen werden, sollten die Mitgliedstaaten ab der Annahme einer Aktualisierung zwölf Monate Zeit haben, um etwaige Änderungen auf die betreffenden Nachweise anzuwenden.

(17) Um die Menge der ausgetauschten Daten zu verringern, könnte bei strukturierten Nachweisen, wenn nur eine Teilmenge der Daten in der Nachweisanfrage angefordert wird, der Nachweislieferant oder gegebenenfalls eine intermediäre Plattform die automatische Filterung der Daten und, falls für die Übermittlung erforderlich, die Umwandlung der Daten im Namen des verantwortlichen Datenverantwortlichen ermöglichen, sodass nur die angeforderten Daten ausgetauscht werden.

(18) Verwalten die Mitgliedstaaten nationale Register und Dienste, die dieselbe oder eine gleichwertige Rolle wie das Verzeichnis der Datendienste oder der Nachweisdienst übernehmen, sollten sie nicht verpflichtet sein, ihre Arbeit durch Beiträge zu den entsprechenden gemeinsamen Diensten zu verdoppeln. In einem solchen Fall sollten sie jedoch sicherstellen, dass ihre nationalen Dienste auf eine Weise mit den gemeinsamen Diensten verbunden sind, dass sie von anderen Mitgliedstaaten genutzt werden können. Alternativ dazu sollten diese Mitgliedstaaten in der Lage sein, die entsprechenden Daten aus den nationalen Registern oder Diensten in das Verzeichnis der Datendienste oder den Nachweisdienst zu übertragen.

(19) In der Erklärung von Tallinn zu elektronischen Behördendiensten ([17]) von 2017 bekräftigten die Mitgliedstaaten ihre Entschlossenheit, bei der Vernetzung ihrer öffentlichen elektronischen Dienste Fortschritte zu erzielen und den Grundsatz der einmaligen Erfassung umzusetzen, um wirksame und sichere digitale öffentliche Dienste bereitzustellen, durch die das Leben der Bürgerinnen und Bürger sowie der Unternehmen erleichtert wird. Die Berliner Erklärung zur digitalen Gesellschaft und wertebasierten digitalen Verwaltung ([18]) von 2020 baut auf dem Grundsatz menschenzentrierter und benutzerfreundlicher Systeme auf und enthält weitere wichtige Grundsätze, auf denen digitale öffentliche Dienste beruhen sollten, darunter Vertrauen und Sicherheit bei der Interaktion mit digitalen Behörden sowie digitale Souveränität und Interoperabilität. Diese Verpflichtungen sollten mit dieser Verordnung umgesetzt werden, indem die Nutzer in den Mittelpunkt des Systems gestellt werden und vorgeschrieben wird, dass die Nutzer über das OOTS, seine Arbeitsschritte und die Folgen der Nutzung des Systems informiert werden müssen.

(20) Es muss ein geeignetes System vorhanden sein, das es den Nutzern ermöglicht, sich für die Zwecke des Austauschs von Nachweisen zu identifizieren. Der einzige Rahmen für die gegenseitige Anerkennung nationaler elektronischer Identifizierungsmittel auf Unionsebene ist in der Verordnung (EU) Nr. 910/2014 festgelegt. Elektronische Identifizierungsmittel, die im Rahmen von elektronischen Identifizierungssystemen ausgestellt werden und gemäß der genannten Verordnung notifiziert wurden, sollten daher von Nachweise anfordernden Behörden verwendet werden, um die Identität eines Nutzers zu authentifizieren, bevor der Nutzer ausdrücklich die Nutzung des OOTS beantragt. Wenn für die Identifizierung des betreffenden Nachweislieferanten die Bereitstellung von Merkmalen erforderlich ist, die über die obligatorischen Merkmale des im Anhang der Durchführungsverordnung (EU) 2015/1501 genannten Mindestdatensatzes hinausgehen, sollten diese zusätzlichen Merkmale auch vom Nutzer durch die Nachweise anfordernden Behörden angefordert und dem Nachweislieferanten oder der intermediären Plattform gegebenenfalls als Teil der Nachweisanfrage bereitgestellt werden.

([16]) ABl. L 210 vom 14.6.2021, S. 51.

([17]) Unterzeichnet am 6. Oktober 2017, abrufbar unter https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration.

([18]) Unterzeichnet am 8. Dezember 2020, abrufbar unter https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government.

(21) Einige der in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 aufgeführten Verfahren setzen voraus, dass Nachweise im Namen einer juristischen oder natürlichen Person angefordert werden können. So sind beispielsweise bestimmte Verfahren für Unternehmen relevant, weshalb Unternehmer die Möglichkeit haben sollten, den Austausch von Nachweisen entweder in ihrem eigenen Namen oder über einen Vertreter zu beantragen. Die Verordnung (EU) Nr. 910/2014 bietet einen vertrauenswürdigen Rechtsrahmen für elektronische Identifizierungsmittel, die für juristische Personen oder für natürliche Personen, die juristische Personen vertreten, ausgestellt werden. Für diese Vertretungsfälle gilt die gegenseitige Anerkennung nationaler elektronischer Identifizierungsmittel gemäß der genannten Verordnung. Diese Verordnung sollte sich daher auf die Verordnung (EU) Nr. 910/2014 und die auf ihrer Grundlage erlassenen Durchführungsrechtsakte stützen, wenn es um die Identifizierung von Nutzern in Vertretungsfällen geht. Die Koordinierungsgruppe für das Zugangstor und ihre Untergruppen sollten eng mit den gemäß der Verordnung (EU) Nr. 910/2014 eingerichteten Governance-Strukturen zusammenarbeiten, um zur Erarbeitung von Lösungen für Vertretungsbefugnisse und Mandate beizutragen. Da einige der vom OOTS abgedeckten Verfahren auf dem durch die Verordnung (EU) Nr. 910/2014 geschaffenen Rahmen beruhen, sollten die von den Vertretern angeforderten Nachweise auch über das OOTS bearbeitet werden können, sofern und soweit Lösungen dafür gefunden wurden.

(22) Damit der Zeitaufwand und die Kosten für die Einrichtung des OOTS begrenzt werden und die Mitgliedstaaten von den Erfahrungen der anderen Mitgliedstaaten bei der Einrichtung profitieren können, sollte die Kommission die Mitgliedstaaten unterstützen und die Zusammenarbeit zwischen ihnen in Bezug auf die Entwicklung von wiederverwendbaren technischen Lösungen und Komponenten, die für die Einrichtung nationaler Verfahrensportale, der Vorschaubereiche und der Datendienste genutzt werden können, fördern.

(23) Um dafür Sorge zu tragen, dass die Nutzer während der Nutzung des OOTS jederzeit die Kontrolle über ihre personenbezogenen Daten behalten, wie in der Verordnung (EU) 2018/1724 vorgesehen, sollte das OOTS die Nutzer in zwei Fällen in die Lage versetzen, ihre Entscheidung in Bezug auf diese Daten zu äußern. Erstens sollte sichergestellt werden, dass die Nutzer ausreichende Informationen erhalten, damit sie gemäß Artikel 14 Absatz 3 Buchstabe a und Artikel 14 Absatz 4 der Verordnung (EU) 2018/1724 in Kenntnis der Sachlage und ausdrücklich um die Verarbeitung ihrer Nachweisanfragen ersuchen können. Anschließend sollte gemäß Artikel 14 Absatz 3 Buchstabe f der Verordnung (EU) 2018/1724 sichergestellt werden, dass die auszutauschenden Nachweise in einem sicheren Vorschaubereich vorab eingesehen werden können, bevor der Nutzer entscheidet, ob er mit dem Austausch von Nachweisen fortfährt oder nicht, mit Ausnahme der in Artikel 14 Absatz 5 der genannten Verordnung genannten Fällen.

(24) Die Verantwortung für die Einrichtung des OOTS wird zwischen den Mitgliedstaaten und der Kommission aufgeteilt; die Koordinierungsgruppe für das Zugangstor sollte daher eine zentrale Rolle bei der Governance des Systems spielen. Angesichts des technischen Charakters ihrer Arbeit und zur Erleichterung der Umsetzung der technischen Entwurfsdokumentation in bestehenden nationalen Systemen sollte die Arbeit der Koordinierungsgruppe für das Zugangstor von Sachverständigen unterstützt und vorbereitet werden, die sich in einer oder mehreren Untergruppen zusammenfinden, die gemäß ihrer Geschäftsordnung eingesetzt werden. Die Funktionsweise einer solchen Governance des OOTS sollte in dem Bericht bewertet werden, den die Kommission dem Europäischen Parlament und dem Rat gemäß Artikel 36 der Verordnung (EU) 2018/1724 bis zum 12. Dezember 2022 vorgelegen muss.

(25) Um sicherzustellen, dass rasch auf mögliche Vorfälle und Ausfälle, die den Betrieb des OOTS beeinträchtigen könnten, reagiert werden kann, sollten die Mitgliedstaaten und die Kommission ein Netz von Kontaktstellen für die technische Unterstützung einrichten. Damit das OOTS ordnungsgemäß funktionieren kann, sollten diese Kontaktstellen für die technische Unterstützung über die erforderlichen Befugnisse sowie über ausreichende personelle und finanzielle Ressourcen verfügen, um ihre Aufgaben wahrnehmen zu können.

(26) Um eine wirksame Funktionsweise und Wartung des OOTS zu gewährleisten, sollten die Verantwortlichkeiten für die verschiedenen Komponenten klar verteilt sein. Die Kommission sollte als Eignerin und Betreiberin der gemeinsamen Dienste für deren Wartung, Hosting und Sicherheit verantwortlich sein. Jeder Mitgliedstaat sollte dafür verantwortlich sein, die Wartung und die Sicherheit der Komponenten des OOTS, die ihm gehören und für die er verantwortlich ist, z. B. eIDAS-Knoten, eDelivery-Zugangspunkte oder nationale Register, im Einklang mit den einschlägigen Rechtsvorschriften der Union und der Mitgliedstaaten sicherzustellen.

(27) Um einen angemessenen Schutz personenbezogener Daten gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([19]) zu gewährleisten, sollte die Rolle der Mitgliedstaaten, insbesondere der jeweils zuständigen Behörden in ihrer Eigenschaft als Nachweise anfordernde Behörde oder Nachweislieferant, und gegebenenfalls der intermediären Plattformen in Bezug auf die personenbezogenen Daten, die in den über das OOTS ausgetauschten Nachweisen enthalten sind, in dieser Verordnung festgelegt werden.

(28) Zum Schutz der gemeinsamen Dienste vor potenziellen Bedrohungen, die die Vertraulichkeit, Integrität oder Verfügbarkeit der Kommunikations- und Informationssysteme der Kommission beeinträchtigen, sollte der Beschluss (EU, Euratom) 2017/46 der Kommission ([20]) für diese Dienste gelten.

(29) Artikel 14 Absätze 1 bis 8 und 10 der Verordnung (EU) 2018/1724 gelten ab dem 12. Dezember 2023. Daher sollten die in der vorliegenden Verordnung festgelegten Anforderungen ebenfalls ab diesem Datum gelten.

(30) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([21]) angehört und hat am 6. Mai 2021 eine förmliche Stellungnahme ([22]) abgegeben.

(31) Die in der vorliegenden Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des Ausschusses für das einheitliche digitale Zugangstor —

HAT FOLGENDE VERORDNUNG ERLASSEN:

ABSCHNITT 1

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „technisches System zur einmaligen Erfassung“ bzw. „OOTS“ (once-only technical system) das technische System für den grenzüberschreitenden automatisierten Austausch von Nachweisen gemäß Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724;

2. „Nachweislieferant“ eine zuständige Behörde im Sinne des Artikels 14 Absatz 2 der Verordnung (EU) 2018/1724, die strukturierte oder unstrukturierte Nachweise rechtmäßig ausstellt;

3. „Nachweise anfordernde Behörde“ eine zuständige Behörde, die für eines oder mehrere der in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 genannten Verfahren verantwortlich ist;

4. „eDelivery-Zugangspunkt“ eine Kommunikationskomponente, die Teil des elektronischen Zustelldienstes eDelivery ist und auf technischen Spezifikationen und Normen beruht, einschließlich des AS4-Datenübermittlungsprotokolls und zusätzlicher Dienste, die im Rahmen der Fazilität „Connecting Europe“ entwickelt und im Rahmen des Programms „Digitales Europa“ fortgeführt wurden, soweit sich diese technischen Spezifikationen und Normen mit der Norm ISO 15000-2 decken;

([19]) 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).

([20]) Beschluss (EU, Euratom) 2017/46 der Kommission vom 10. Januar 2017 über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission (ABl. L 6 vom 11.1.2017, S. 40).

([21]) 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).

([22]) https://edps.europa.eu/data-protection/our-work/publications/comments/specifications-technical-system-cross-border_de

5. „eIDAS-Knoten“ einen Knoten im Sinne von Artikel 2 Nummer 1 der Durchführungsverordnung (EU) 2015/1501, der die technischen und operativen Anforderungen erfüllt, die in dieser Verordnung und auf deren Grundlage festgelegt sind;

6. „intermediäre Plattform“ eine technische Lösung, die je nach der Verwaltungsorganisation der Mitgliedstaaten, in denen die intermediäre Plattform tätig ist, in Erfüllung eigener Aufgaben oder im Namen anderer Behörden wie Nachweislieferanten oder Nachweise anfordernden Behörden tätig wird und über die Nachweislieferanten oder Nachweise anfordernde Behörden mit den in Artikel 4 Absatz 1 genannten gemeinsamen Diensten oder mit Nachweislieferanten oder Nachweise anfordernden Behörden aus anderen Mitgliedstaaten verbunden werden;

7. „Verzeichnis der Datendienste“ ein Register, das die Liste der Nachweislieferanten und der von ihnen herausgegebenen Nachweisarten zusammen mit den entsprechenden Begleitinformationen enthält;

8. „Nachweisdienst“ einen Dienst, der es einer Nachweise anfordernden Behörde ermöglicht, festzustellen, welche Nachweisart aus einem anderen Mitgliedstaat die Anforderungen an die Nachweise für die Zwecke eines nationalen Verfahrens erfüllt;

9. „elektronisches Identifizierungsmittel“ eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird;

10. „semantischer Datenspeicher“ ein Archiv semantischer Spezifikationen, die mit dem Nachweisdienst und dem Verzeichnis der Datendienste verknüpft sind und aus Definitionen von Namen, Datentypen und Datenelementen bestehen, die mit bestimmten Nachweisarten verbunden sind, um das gegenseitige Verständnis und die sprachenübergreifende Auslegung für Nachweislieferanten, Nachweise anfordernde Behörden und Nutzer beim Austausch von Nachweisen über das OOTS sicherzustellen;

11. „technische Entwurfsdokumentation“ eine Reihe detaillierter und unverbindlicher technischer Dokumente, die von der Kommission in Zusammenarbeit mit den Mitgliedstaaten im Rahmen der Koordinierungsgruppe für das Zugangstor gemäß Artikel 29 der Verordnung (EU) 2018/1724 oder etwaiger Untergruppen gemäß Artikel 19 dieser Verordnung erstellt werden und die unter anderem eine oberste Ebene der Architektur, Austauschprotokolle, Normen und Zusatzdienste umfassen, die die Kommission, die Mitgliedstaaten, die Nachweislieferanten, die Nachweise anfordernden Behörden, die intermediären Plattformen und andere betroffene Behörden bei der Einrichtung des OOTS im Einklang mit dieser Verordnung unterstützen;

12. „Datendienst“ einen technischen Dienst, über den ein Nachweislieferant die Nachweisanfrage bearbeitet und die Nachweise übermittelt;

13. „Datenmodell“ eine Abstraktion, in der Datenelemente organisiert werden und die ihre Beziehungen zueinander standardisiert und die Entitäten, ihre Merkmale und die Beziehungen zwischen diesen Entitäten spezifiziert;

14. „Vorschaubereich“ eine Funktion, die es dem Nutzer ermöglicht, die angeforderten Nachweise gemäß Artikel 15 Absatz 1 Buchstabe b Ziffer ii vorab einzusehen;

15. „strukturierter Nachweis“ alle Nachweise in elektronischem Format, die für die in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 genannten Verfahren erforderlich sind, die in vordefinierten Elementen oder Feldern organisiert sind, die eine bestimmte Bedeutung und ein bestimmtes technisches Format haben, das die Verarbeitung durch Softwaresysteme ermöglicht, und die durch die Metadatenelemente des in Artikel 7 Absatz 1 dieser Verordnung genannten allgemeinen Metadatenmodells des OOTS ergänzt werden und entweder dem in Artikel 7 Absatz 2 dieser Verordnung genannten Datenmodell des technischen Systems (OOTS) für die betreffende Nachweisart entsprechen oder von einer von Menschen lesbaren Version begleitet werden;

16. „unstrukturierter Nachweis“ Nachweise in elektronischem Format, die für die in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 genannten Verfahren erforderlich sind und die nicht in vordefinierten Elementen oder Feldern organisiert sind, die eine bestimmte Bedeutung und ein bestimmtes technisches Format haben, sondern durch die Metadatenelemente des allgemeinen Metadatenmodells des OOTS gemäß Artikel 7 Absatz 1 der vorliegenden Verordnung ergänzt werden;

17. „Nachweisart“ eine Kategorie von strukturierten oder unstrukturierten Nachweisen mit einem gemeinsamen Zweck oder einem gemeinsamen Inhalt;

18. „Vorfall“ eine Situation, in der das technische System (OOTS) die Leistung nicht erbringt, die Nachweise nicht übermittelt oder Nachweise übermittelt, die nicht angefordert wurden, oder in der die Nachweise während der Übermittlung verändert oder offengelegt wurden, sowie jede Verletzung der Sicherheit gemäß Artikel 29;

19. „Verfahrensportal“ eine Webseite oder eine mobile Anwendung, über die ein Nutzer Zugang zu einem Online-Verfahren im Sinne von Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 hat und es abschließen kann.

Artikel 2

Struktur des OOTS

Das OOTS besteht aus

a) den Verfahrensportalen von Nachweise anfordernden Behörden und den Datendiensten von Nachweislieferanten,

b) gegebenenfalls intermediären Plattformen,

c) dem in Artikel 15 Absatz 1 Buchstabe b Ziffer ii genannten Vorschaubereich,

d) den in Artikel 8 genannten nationalen Registern und Diensten, soweit erforderlich,

e) eIDAS-Knoten für die Nutzerauthentifizierung und den Identitätsabgleich,

f) eDelivery-Zugangspunkten,

g) den in Artikel 4 Absatz 1 genannten gemeinsamen Diensten,

h) den Integrationselementen und Schnittstellen, die erforderlich sind, um die in den Buchstaben a bis g genannten Komponenten zu verbinden.

ABSCHNITT 2

DIENSTE DES OOTS

Artikel 3

eIDAS-Knoten und eDelivery-Zugangspunkte

(1) Die Mitgliedstaaten tragen dafür Sorge, dass die Nachweise anfordernden Behörden entweder direkt oder über eine intermediäre Plattform mit einem eIDAS-Knoten verbunden sind, um die Nutzerauthentifizierung gemäß Artikel 11 zu ermöglichen.

(2) Die Mitgliedstaaten stellen sicher, dass eDelivery-Zugangspunkte in den Verfahrensportalen der Nachweise anfordernden Behörden, in den Datendiensten der Nachweislieferanten und auf den intermediären Plattformen installiert, konfiguriert und darin eingebunden sind.

(3) Die Mitgliedstaaten können die Anzahl der eDelivery-Zugangspunkte, die sie für das technische System (OOTS) verwenden, selbst bestimmen.

Artikel 4

Gemeinsame Dienste

(1) Die Kommission richtet in Zusammenarbeit mit den Mitgliedstaaten die folgenden Dienste des technischen Systems (OOTS) (im Folgenden „gemeinsame Dienste“) ein:

a) das Verzeichnis der Datendienste gemäß Artikel 5;

b) den Nachweisdienst gemäß Artikel 6;

c) den semantischen Datenspeicher gemäß Artikel 7.

(2) Die Mitgliedstaaten stellen die technische Verbindung zwischen den Verfahrensportalen der Nachweise anfordernden Behörden direkt oder über intermediäre Plattformen mit den gemeinsamen Diensten und die ordnungsgemäße Registrierung ihrer Datendienste in den gemeinsamen Diensten sicher. Bei der Implementierung dieser Verbindungen orientieren sich die Mitgliedstaaten an den Beschreibungen in der technischen Entwurfsdokumentation.

(3) Die Mitgliedstaaten stellen sicher, dass nur Nachweise anfordernde Behörden direkt oder über intermediäre Plattformen mit den gemeinsamen Diensten verbunden sind und dass nur Nachweise anfordernde Behörden und Nachweislieferanten das OOTS nutzen können. Die Mitgliedstaaten überprüfen in regelmäßigen Abständen das Funktionieren der Verbindungen zu den gemeinsamen Diensten.

Artikel 5

Verzeichnis der Datendienste

(1) Unbeschadet des Artikels 8 der vorliegenden Verordnung stellen die Mitgliedstaaten sicher, dass alle Nachweislieferanten und von ihnen ausgestellten Nachweisarten, die für die in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 genannten Online-Verfahren relevant sind, in das Verzeichnis der Datendienste aufgenommen werden.

(2) Die Kommission ist für die Entwicklung und Pflege von Schnittstellen verantwortlich, die es den in Artikel 28 der Verordnung (EU) 2018/1724 genannten nationalen Koordinatoren, den zuständigen Behörden, gegebenenfalls den intermediären Plattformen und der Kommission — jeweils im Rahmen ihrer Zuständigkeiten und der von der Kommission festgelegten Zugangsrechte — ermöglichen,

a) die im Verzeichnis der Datendienste enthaltenen Informationen zu registrieren, zu löschen und sonstige Aktualisierungen vorzunehmen,

b) die Zugriffsrechte der Personen zu verwalten, die berechtigt sind, Registrierungen und Änderungen an den registrierten Daten vorzunehmen.

Die Kommission trägt dafür Sorge, dass nationale Koordinatoren, zuständige Behörden und intermediäre Plattformen zwischen grafischen Anwenderschnittstellen für autorisierte Personen und Programmierschnittstellen für automatisches Hochladen wählen können.

(3) Die Mitgliedstaaten stellen sicher, dass jeder Nachweisart, die im Verzeichnis der Datendienste registriert ist, Folgendes beigefügt wird:

a) das Sicherheitsniveau der von den Mitgliedstaaten gemäß der Verordnung (EU) Nr. 910/2014 notifizierten elektronischen Identifizierungsmittel und

b) gegebenenfalls für den Austausch über das OOTS erforderliche zusätzliche Attribute, die zur Erleichterung der Identifizierung des jeweiligen Nachweislieferanten angegeben werden und die über die obligatorischen Merkmale des in der Durchführungsverordnung (EU) 2015/1501 festgelegten Mindestdatensatzes hinausgehen, die unter Verwendung der gemäß der Verordnung (EU) Nr. 910/2014 notifizierten elektronischen Identifizierungsmittel ausgetauscht werden.

(4) Im Verzeichnis der Datendienste wird klar zwischen den in Absatz 3 Buchstabe b dieses Artikels genannten zusätzlichen Merkmalen und den Merkmalen, die unter Verwendung der gemäß der Verordnung (EU) Nr. 910/2014 notifizierten elektronischen Identifizierungsmittel nach Artikel 13 Absatz 1 Buchstabe f dieser Verordnung ausgetauscht werden, unterschieden.

(5) Das in Absatz 3 Buchstabe a genannte Sicherheitsniveau, das für grenzüberschreitende Nutzer erforderlich ist, darf das für nicht grenzüberschreitende Nutzer erforderliche Sicherheitsniveau nicht überschreiten.

(6) Die Mitgliedstaaten sorgen dafür, dass die Informationen im Data Service Directory auf dem neuesten Stand gehalten werden.

Artikel 6

Nachweisdienst

(1) Der Nachweisdienst ermöglicht es den Nachweise anfordernden Behörden, festzustellen, welche in anderen Mitgliedstaaten ausgestellten Nachweisarten den Nachweisarten entsprechen, die im Rahmen der Verfahren, für die die Nachweise anfordernde Behörde zuständig ist, erforderlich sind.

(2) Die Mitgliedstaaten ergänzen über die in Artikel 5 Absatz 2 genannte Schnittstelle das Verzeichnis der Nachweisarten im Verzeichnis der Datendienste gemäß Artikel 5 Absatz 1 um die Sachverhalte oder die Einhaltung der von ihnen nachgewiesenen Verfahrensvorschriften, gegebenenfalls zusammen mit anderen Nachweisarten. Die Mitgliedstaaten sorgen dafür, dass diese Informationen richtig sind und auf dem neuesten Stand gehalten werden.

(3) Die Kommission ist für die Entwicklung und Pflege von Schnittstellen verantwortlich, die es den nationalen Koordinatoren, den zuständigen Behörden, gegebenenfalls den intermediären Plattformen und der Kommission — jeweils im Rahmen ihrer Zuständigkeiten und der von der Kommission festgelegten Zugangsrechte — ermöglichen,

a) die in Absatz 2 genannten Informationen hinzuzufügen, zu ändern oder zu aktualisieren und

b) die Zugriffsrechte der Personen zu verwalten, die berechtigt sind, Ergänzungen und Änderungen an den registrierten Information vorzunehmen.

Die Kommission trägt dafür Sorge, dass nationale Koordinatoren, zuständige Behörden und intermediäre Plattformen zwischen grafischen Anwenderschnittstellen für autorisierte Personen und Programmierschnittstellen für automatisches Hochladen wählen können.

(4) Die Kommission erleichtert die Zuordnung der in einem Mitgliedstaat ausgestellten Nachweise auf Sachverhalte oder die Einhaltung von Verfahrensvorschriften, die in einem Verfahren in einem anderen Mitgliedstaat nachgewiesen werden müssen, indem sie die Gespräche strukturiert und die Arbeit in der in Artikel 19 genannten zuständigen Untergruppe organisiert. Die Untergruppe legt eine formale domainspezifische Sprache fest, die nach Möglichkeit einer einschlägigen internationalen Norm zugeordnet werden kann, und schlägt diese Sprache der Koordinierungsgruppe für das Zugangstor gemäß Artikel 18 Buchstabe f vor.

Artikel 7

Semantischer Datenspeicher und Datenmodelle

(1) Der semantische Datenspeicher ermöglicht den Zugriff auf das allgemeine Metadatenmodell des OOTS, das so konzipiert ist, dass es Metadaten zur eindeutigen Identifizierung des Nachweises und des Nachweislieferanten anzeigt und das zusätzliche Felder zur Anzeige der in Artikel 13 Absatz 1 Buchstaben a, b und c genannten Metadaten enthält.

(2) Für die in der Koordinierungsgruppe für das Zugangstor vereinbarten strukturierten Nachweisarten enthält der semantische Datenspeicher ein Datenmodell des OOTS, das mindestens die folgenden Komponenten umfasst:

a) eine Darstellung dieses Datenmodells mit

   i) einem visuellen Diagramm des Datenmodells und

   ii) einer Beschreibung aller Entitäten des Datenmodells in Textform, bestehend aus einer Definition und der Liste der Merkmale der Entität, und für jedes Merkmal die erwartete Art (z. B. boolesch, Kennung, Datum), eine Definition, die Kardinalität und die optionale Verwendung einer Codeliste,

b) die Ausgabe in XML auf der Grundlage der XML-Schema-Definition (XSD) oder eines gleichwertigen Formats, ergänzt durch andere weitverbreitete Serialisierungsformate, sofern möglich,

c) Codelisten zur Gewährleistung der automatisierten Verarbeitung von Nachweisen, die in einem strukturierten Format verfügbar sind,

d) einen Mechanismus für die Umwandlung in ein für den Menschen lesbares Format, z. B. XSLT oder ein gleichwertiges Format.

(3) Für jede Art von Nachweis bietet der semantische Datenspeicher eine Versionskontrolle und ein Änderungsprotokoll, um die verschiedenen Versionen nachverfolgen zu können.

(4) Das Semantic Repository umfasst eine Methode für die Entwicklung neuer Datenmodelle des OOTS für über das OOTS ausgetauschte Nachweisarten, bestehend aus Beispielen und Lernmaterialien.

(5) Die Zeitpläne für Aktualisierungen und Anpassungen der allgemeinen Metadatenmodelle und der Datenmodelle des OOTS werden von den Mitgliedstaaten und der Kommission regelmäßig im Rahmen einer der Untergruppen der Koordinierungsgruppe für das Zugangstor gemäß Artikel 19 erörtert und von der Koordinierungsgruppe für das Zugangstor angenommen. Die Nachweislieferanten oder gegebenenfalls die intermediären Plattformen wenden diese Aktualisierungen und Anpassungen spätestens zwölf Monate nach ihrer Veröffentlichung im semantischen Datenspeicher an.

(6) Die Kommission stellt den Mitgliedstaaten ein IT-Tool zur Verfügung, mit dem sie die Übereinstimmung der Nachweise mit dem allgemeinen Metadatenmodell und den Datenmodellen des OOTS überprüfen können.

(7) Die Kommission veröffentlicht den semantischen Datenspeicher auf einer speziellen Website der Kommission.

Artikel 8

Nationale Register und Dienste

(1) Mitgliedstaaten, die über nationale Register oder Dienste verfügen, die dem Verzeichnis der Datendienste oder dem Nachweisdienst gleichwertig sind, können sich dafür entscheiden, die Nachweislieferanten, die Nachweisarten, die sie ausstellen, und die Sachverhalte oder die Einhaltung der von ihnen nachgewiesenen Verfahrensvorschriften, möglicherweise zusammen mit anderen Nachweisarten, sowie das Sicherheitsniveau der elektronischen Identifizierungsmittel, die für den Zugang zu den einzelnen Nachweisarten gemäß Artikel 5 und 6 erforderlich sind, nicht zu registrieren. In einem solchen Fall ergreifen sie stattdessen eine der folgenden Maßnahmen:

a) Sie gestatten es den anderen Mitgliedstaaten, in ihren nationalen Registern nach den in diesem Absatz genannten Informationen zu suchen;

b) sie übertragen die in diesem Absatz genannten Informationen aus den nationalen Registern oder Diensten in das Verzeichnis der Datendienste oder den Nachweisdienst.

(2) Bei der Umsetzung von Absatz 1 orientieren sich die Mitgliedstaaten an den Beschreibungen in der technischen Entwurfsdokumentation.

ABSCHNITT 3

NACHWEISE ANFORDERNDE BEHÖRDEN

Artikel 9

Erklärung für die Nutzer

(1) Die Nachweise anfordernden Behörden stellen sicher, dass ihre Verfahrensportale eine Erklärung des OOTS und von dessen Funktionen enthalten, einschließlich Informationen darüber, dass

a) die Nutzung des OOTS freiwillig ist;

b) die Nutzer die Möglichkeit haben, den Nachweis in dem Vorschaubereich gemäß Artikel 15 Absatz 1 Buchstabe b Ziffer ii vorab einzusehen und zu entscheiden, ob sie diesen für das Verfahren verwenden wollen oder nicht;

c) die Nutzer im eigenen Namen handeln oder sich von einer anderen juristischen oder natürlichen Person vertreten lassen können, sofern und soweit Lösungen für die Vertretung gemäß der Verordnung (EU) Nr. 910/2014 und den auf ihrer Grundlage erlassenen Durchführungsrechtsakten gefunden wurden.

Die in Unterabsatz 1 Buchstabe b dieses Absatzes genannten Informationen sind im Falle der in Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 genannten Verfahren nicht erforderlich.

(2) Die Verpflichtung zur Bereitstellung von Erläuterungen gemäß Absatz 1 dieses Artikels gilt unbeschadet der Verpflichtung, den betroffenen Personen die in den Artikeln 13 und 14 der Verordnung (EU) 2016/679 genannten Informationen zur Verfügung zu stellen.

Artikel 10

Auswahl der Nachweisart

(1) Die Nachweise anfordernden Behörden geben den Nutzern die Möglichkeit, die Nachweisarten, die auf der Grundlage der im Nachweisdienst registrierten Informationen den Arten entsprechen, die nach dem anwendbaren Recht in dem betreffenden Verfahren zulässig wären, mittels direkter Übermittlung anzufordern, sofern die Nachweislieferanten diese Nachweisarten über das OOTS gemäß Artikel 5 Absatz 1 zur Verfügung stellen.

(2) Können mehrere Nachweise angefordert werden, muss die Nachweise anfordernde Behörde sicherstellen, dass die Nutzer alle Nachweise, einen Teil davon oder eine bestimmte Nachweisart auswählen können.

Artikel 11

Nutzerauthentifizierung

(1) Die Nachweise anfordernden Behörden nutzen elektronische Identifizierungsmittel, die im Rahmen eines elektronischen Identifizierungssystems ausgestellt wurden, das gemäß der Verordnung (EU) Nr. 910/2014 notifiziert wurde, um die Nutzer zu authentifizieren, die entweder im eigenen Namen oder über einen Vertreter tätig werden, sofern und soweit Lösungen für die Vertretung gemäß der Verordnung (EU) Nr. 910/2014 und den auf ihrer Grundlage erlassenen Durchführungsrechtsakten gefunden wurden.

(2) Sobald der Nutzer die Nachweisart, die über das OOTS ausgetauscht werden soll, ausgewählt hat, informieren die Nachweise anfordernden Behörden die Nutzer

a) gegebenenfalls über die zusätzlichen Merkmale gemäß Artikel 5 Absatz 3 Buchstabe b dieser Verordnung, die sie bereitstellen müssen, und

b) darüber, dass sie zu den entsprechenden Nachweislieferanten oder gegebenenfalls zu einer oder mehreren intermediären Plattformen weitergeleitet werden, um die ausgewählten Nachweise vorab einzusehen.

(3) Ist die in Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 genannte Möglichkeit, den Nachweis vorab einzusehen, nicht erforderlich, so findet Absatz 2 Buchstabe b dieses Artikels keine Anwendung. In diesem Fall können die Nachweislieferanten oder gegebenenfalls die intermediären Plattformen die Nachweise anfordernde Behörde auffordern, den Nutzer zum Zwecke des Identitäts- und Nachweisabgleichs erneut zu identifizieren und zu authentifizieren. Der Nutzer kann sich dafür entscheiden, nicht weitergeleitet zu werden. In diesem Fall informiert die Nachweise anfordernde Behörde den Nutzer darüber, dass der vom Nachweislieferanten durchgeführte Identitäts- und Nachweisabgleich möglicherweise nicht zu einer Übereinstimmung im Sinne von Artikel 16 dieser Verordnung führt.

Artikel 12

Ausdrückliches Ersuchen

Die Nachweise anfordernde Behörde stellt dem Nutzer zusätzlich zu den in Artikel 9 genannten Informationen Folgendes zur Verfügung:

a) die Namen der Nachweise anfordernden Behörden,

b) die Nachweisarten oder Datenfelder, die ausgetauscht werden sollen.

Dieser Artikel gilt unbeschadet der Fälle, in denen die Nutzung des OOTS ohne ausdrückliches Ersuchen gemäß Artikel 14 Absatz 4 der Verordnung (EU) 2018/1724 zulässig ist.

Artikel 13

Nachweisanfrage

(1) Die Nachweise anfordernde Behörde stellt sicher, dass die Nachweisanfrage an den Nachweislieferanten oder gegebenenfalls die intermediäre Plattform übermittelt wird und die folgenden Informationen enthält:

a) die eindeutige Kennung der Anfrage,

b) die angeforderte Nachweisart,

c) das Datum und die Uhrzeit des ausdrücklichen Ersuchens,

d) die Angabe des Verfahrens, für das der Nachweis erforderlich ist,

e) den Namen und die Metadaten zur eindeutigen Identifizierung der Nachweise anfordernden Behörde und der intermediären Plattform, sofern zutreffend,

f) die Merkmale des Nutzers oder gegebenenfalls des Nutzers und des Vertreters, die unter Verwendung der in Artikel 11 Absatz 1 genannten elektronischen Identifizierungsmittel ausgetauscht werden,

g) das Sicherheitsniveau der vom Nutzer verwendeten elektronischen Identifizierungsmittel im Sinne der Verordnung (EU) Nr. 910/2014,

h) die in Artikel 5 Absatz 3 Buchstabe b genannten zusätzlichen Merkmale, die der Nutzer für die Zwecke der Anfrage bereitstellt,

i) die Kennung des im Verzeichnis der Datendienste eingetragenen Nachweislieferanten,

j) die Angabe, ob das ausdrückliche Ersuchen des Nutzers gemäß Artikel 14 Absatz 4 der Verordnung (EU) 2018/1724 erforderlich war,

k) die Angabe, ob die Möglichkeit, die Nachweise gemäß Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 vorab einzusehen, erforderlich war.

(2) Die Nachweise anfordernde Behörde unterscheidet klar zwischen den in Absatz 1 Buchstabe h genannten zusätzlichen Merkmalen und den in Absatz 1 Buchstabe f genannten Merkmalen.

Artikel 14

Weiterleitung des Nutzers an den Nachweislieferanten

(1) Unbeschadet der Verfahren nach Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 stellen die Nachweise anfordernden Behörden sicher, dass die Nutzer nach der Auswahl der über das OOTS auszutauschenden Nachweise im Verfahrensportal gemäß Artikel 10 dieser Verordnung und der Angabe ihres ausdrücklichen Ersuchens gemäß Artikel 12 dieser Verordnung zu den Nachweislieferanten oder gegebenenfalls zu einer oder mehreren intermediären Plattformen weitergeleitet werden, um von der Möglichkeit, die Nachweise vorab einzusehen, Gebrauch zu machen.

(2) In Bezug auf die in Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 genannten Verfahren können die Nutzer gemäß Artikel 11 Absatz 3 der vorliegenden Verordnung gegebenenfalls an die Nachweislieferanten oder eine oder mehrere intermediäre Plattformen weitergeleitet werden.

ABSCHNITT 4

NACHWEISLIEFERANT

Artikel 15

Rolle beim Austausch von Nachweisen

(1) Die Mitgliedstaaten stellen sicher, dass die Nachweislieferanten oder gegebenenfalls die intermediären Plattformen für den Austausch von Nachweisen über das OOTS Anwendungsdienste nutzen, die Folgendes leisten können:

a) Entgegennahme und Auswertung von Nachweisanfragen, die von einem eDelivery-Zugangspunkt übermittelt werden und die als Eingangsdaten für die Datendienste gelten;

b) vorbehaltlich einer erfolgreichen Identifizierung und Authentifizierung gemäß Artikel 16 dieser Verordnung:

   i) Abrufen von Nachweisen, die der Anfrage entsprechen;

   ii) Möglichkeit für die Nutzer — außer im Falle der in Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 genannten Verfahren —, anzugeben, welche dieser Nachweise sie im Vorschaubereich vorab einsehen möchten, und die auf diese Weise angegebenen Nachweise in einem Vorschaubereich einzusehen;

   iii) Möglichkeit für die Nutzer, anzugeben, welche der übereinstimmenden Nachweise gegebenenfalls an die Nachweise anfordernde Behörde zur Verwendung im Verfahren rückübermittelt werden sollen;

c) Rückübermittlung der Antworten auf die Nachweisanfrage an die Nachweise anfordernde Behörde über einen eDelivery-Zugangspunkt, vorbehaltlich der Entscheidung des Nutzers, den Nachweis in dem Verfahren zu verwenden, nachdem er die Möglichkeit hatte, diesen im Vorschaubereich einzusehen, außer im Falle der in Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 genannten Verfahren, von Fehlermeldungen, auch in der in Artikel 16 Absatz 3 Buchstabe a der vorliegenden Verordnung genannten Situation, oder von Berichten über Nachweise, die noch umgewandelt werden.

(2) Wird eine Antwort auf eine Nachweisanfrage rückübermittelt, so muss sie die angeforderten Nachweise und Folgendes enthalten:

a) Metadaten zur eindeutigen Identifizierung der Antwort auf eine Nachweisanfrage;

b) Metadaten zur eindeutigen Identifizierung der Nachweisanfrage;

c) Metadaten, die das Datum und die Uhrzeit angeben, zu der die Antwort erzeugt wurde;

d) Metadaten zur eindeutigen Identifizierung des Nachweises und des Nachweislieferanten;

e) eine von Menschen lesbare Fassung des Nachweises in Fällen, in denen strukturierte Nachweise nicht dem für die betreffende Nachweisart relevanten Datenmodell des OOTS entsprechen.

(3) Die Antwort auf eine Nachweisanfrage kann auch Metadaten enthalten, die die Sprache bzw. die Sprachen der angeforderten Nachweise eindeutig identifizieren.

(4) Wird eine Fehlermeldung rückübermittelt, so enthält diese Metadaten zur eindeutigen Identifizierung der Anfrage, des Datums und der Uhrzeit, zu der sie erstellt wurde, sowie eine Beschreibung des aufgetretenen Fehlers.

(5) Stehen noch keine Nachweise für den Austausch über das OOTS zur Verfügung, werden diese aber derzeit in strukturierte oder unstrukturierte Nachweise im Sinne von Artikel 1 Nummern 16 und 17 umgewandelt, wird ein Bericht nach Absatz 1 Buchstabe c des vorliegenden Artikels übermittelt. Dieser Bericht enthält Metadaten zur eindeutigen Identifizierung der Nachweisanfrage, des Datums und der Uhrzeit seiner Erstellung sowie die Meldung, dass die betreffenden Nachweise derzeit in strukturierte oder unstrukturierte Nachweise im Sinne von Artikel 1 Nummern 16 und 17 umgewandelt werden und in Zukunft für die Übermittlung durch das OOTS zur Verfügung stehen werden. Der Nachweislieferant gibt in seinem Bericht das voraussichtliche Datum und die Uhrzeit an, zu denen die Nachweise zur Verfügung stehen werden.

Artikel 16

Identitäts- und Nachweisabgleich

(1) Die Nachweislieferanten oder die intermediären Plattformen können gegebenenfalls verlangen, dass sich die Nutzer zum Zwecke des Identitäts- und Nachweisabgleichs erneut identifizieren und authentifizieren, auch durch die Bereitstellung zusätzlicher Attribute.

(2) Die Nachweislieferanten oder gegebenenfalls die intermediären Plattformen stellen sicher, dass Nachweise nur dann über das OOTS ausgetauscht werden, wenn die Identitätsattribute des Nutzers und gegebenenfalls des Vertreters, die unter Verwendung der in Artikel 11 Absatz 1 genannten elektronischen Identifizierungsmittel ausgetauscht wurden, sowie die in Artikel 11 Absatz 2 Buchstabe a genannten zusätzlichen Merkmale, die vom Nutzer zur Erleichterung der Identifizierung durch den jeweiligen Nachweislieferanten bereitgestellt wurden, mit den bei ihnen vorhandenen Merkmalen übereinstimmen.

(3) Führt der Identitäts- und Nachweisabgleich nicht zu einer Übereinstimmung oder führt der Identitätsabgleich zu zwei oder mehr Ergebnissen, so wird dem Nutzer oder gegebenenfalls dem Vertreter keine Vorschau auf die angeforderten Nachweise gewährt und die Nachweise werden nicht ausgetauscht. Sollte es keine Übereinstimmung geben,

a) wird der Nachweise anfordernden Behörde eine Fehlermeldung angezeigt;

b) erhält der Nutzer eine automatische Nachricht, in der erklärt wird, dass der Nachweis nicht zur Verfügung gestellt werden kann.

ABSCHNITT 5

PROTOKOLLSYSTEM DES OOTS

Artikel 17

Protokollsystem

(1) Für jede über das OOTS übermittelte Nachweisanfrage protokollieren die Nachweise anfordernde Behörde, die Nachweislieferanten oder gegebenenfalls die intermediären Plattformen die folgenden Elemente:

a) die Nachweisanfrage gemäß Artikel 13 Absatz 1,

b) die in der Antwort auf die Nachweisanfrage enthaltenen Informationen, mit Ausnahme der Nachweise selbst, oder den Fehlerbericht gemäß Artikel 15 Absatz 1 Buchstabe c und Artikel 16 Absatz 3 Buchstabe a,

c) die eDelivery-Ereignisdaten im Zusammenhang mit Folgendem:

i) den Nachweisanfragen;

ii) den Antworten auf eine Nachweisanfrage;

iii) den Fehlerberichten.

(2) Für jeden über das OOTS ausgetauschten Nachweis protokolliert der Nachweislieferant oder die intermediäre Plattform gegebenenfalls die Entscheidung des Nutzers nach der Vorschau des Nachweises, die Verwendung des Nachweises für das Verfahren zu genehmigen oder abzulehnen, oder gegebenenfalls die Tatsache, dass der Nutzer den Vorschaubereich oder das Verfahrensportal verlässt, ohne eine konkrete Entscheidung zu treffen.

(3) Die Kommission und — in den in Artikel 8 Absatz 1 Buchstabe a genannten Fällen — die betreffenden Mitgliedstaaten protokollieren alle Interaktionen mit den in Artikel 4 Absatz 1 genannten gemeinsamen Diensten.

(4) Unbeschadet längerer Aufbewahrungsfristen, die nach nationalem Recht für die in den Absätzen 1, 2 und 3 genannten Protokollen für die Zwecke des OOTS oder für andere Zwecke vorgeschrieben sind, bewahren die Kommission und die Nachweise anfordernden Behörden, die Nachweislieferanten oder gegebenenfalls die intermediären Plattformen diese Protokolle für einen Zeitraum von zwölf Monaten auf.

(5) Bei Verdacht auf Vorfälle und für die Zwecke von Prüfungen und stichprobenartigen Sicherheitskontrollen, die in ihrem jeweiligen Zuständigkeitsbereich gemäß Artikel 26 durchgeführt werden, gewähren die Nachweise anfordernden Behörden, die Nachweislieferanten und gegebenenfalls die intermediären Plattformen einander auf Ersuchen Zugang zu den in den Absätzen 1 und 2 des vorliegenden Artikels genannten Protokollen über das in Artikel 22 genannte Dashboard für technischen Support. Zu denselben Zwecken und in gleicher Weise stellen die Mitgliedstaaten und gegebenenfalls die Kommission den betreffenden Nachweise anfordernden Behörden, Nachweislieferanten und intermediären Plattformen die in Absatz 3 dieses Artikels genannten Protokolle zur Verfügung.

ABSCHNITT 6

GOVERNANCE DES OOTS

Artikel 18

Koordinierungsgruppe für das Zugangstor

Die Kommission ist in Zusammenarbeit mit den Mitgliedstaaten im Rahmen der mit Artikel 29 der Verordnung (EU) 2018/1724 eingesetzten Koordinierungsgruppe für das Zugangstor verpflichtet,

a) die Einrichtung und Inbetriebnahme des OOTS im Einklang mit Artikel 31 Absatz 3 dieser Verordnung zu beaufsichtigen;

b) Prioritäten für die Weiterentwicklung und Verbesserung des OOTS festzulegen;

c) einen voraussichtlichen Zeitplan für regelmäßige Aktualisierungen, die Pflege und die Anpassung der technischen Entwurfsdokumentation zu bestimmen;

d) Änderungen an der technischen Entwurfsdokumentation zu empfehlen;

e) eine Peerbegutachtung zur Förderung des Austauschs von Erfahrungen und bewährten Verfahren zwischen den Mitgliedstaaten bei der Anwendung dieser Verordnung durch die Mitgliedstaaten durchzuführen;

f) die von einer der Untergruppen, die im Einklang mit der Geschäftsordnung der Koordinierungsgruppe für das Zugangstor eingerichtet wurden, vorgelegten operativen Modalitäten zu genehmigen oder abzulehnen und erforderlichenfalls spezifische Anleitungen zu geben und ihre Arbeit zu überwachen.

Artikel 19

Untergruppen der Koordinierungsgruppe für das Zugangstor

(1) Um eine koordinierte Entwicklung und Funktionsweise des OOTS zu gewährleisten, erörtern die in Artikel 18 Buchstabe f genannten Untergruppen die operativen Modalitäten, die der Koordinierungsgruppe für das Zugangstor vorzulegen sind, und erarbeiten erforderlichenfalls Vorschläge zu den folgenden Bereichen:

a) Standardisierung von Datenmodellen des OOTS,

b) Zuordnung der Nachweise,

c) Überprüfung, Pflege und Auslegung der technischen Entwurfsdokumentation,

d) operative Governance, insbesondere operative Vereinbarungen und Dienstleistungsvereinbarungen,

e) Sicherheit des OOTS, einschließlich der Erstellung von Risikomanagementplänen für die Ermittlung von Risiken, die Bewertung ihrer möglichen Auswirkungen und die Planung geeigneter technischer und organisatorischer Maßnahmen im Falle von Vorfällen,

f) Erprobung und Einführung der Komponenten des OOTS, einschließlich der Interoperabilität zwischen den in Artikel 2 Buchstaben a bis f und h genannten nationalen Komponenten des OOTS und den in Artikel 4 Absatz 1 genannten gemeinsamen Diensten.

Zu den operativen Modalitäten gehören die Ausarbeitung und der Vorschlag von Normen, die für die Interoperabilität erforderlich sind, in den jeweiligen Bereichen der Untergruppen, wobei nach Möglichkeit internationale Normen zugrunde gelegt werden. Nach der Genehmigung durch die Koordinierungsgruppe für das Zugangstor werden diese Normen in die technische Entwurfsdokumentation aufgenommen.

(2) Die Untergruppen nehmen ihre Vorschläge für die operativen Modalitäten nach Möglichkeit im Konsens an. Stellt sich heraus, dass kein Konsens erzielt werden kann, so kann der Vorsitzende beschließen, dass ein Vorschlag der Untergruppe der Koordinierungsgruppe für das Zugangstor vorgelegt werden kann, wenn er von der einfachen Mehrheit der in der Sitzung anwesenden Mitglieder der Untergruppe unterstützt wird.

ABSCHNITT 7

TECHNISCHE UNTERSTÜTZUNG

Artikel 20

Zentrale Kontaktstelle der Kommission für technische Unterstützung

(1) Die Kommission benennt eine zentrale Kontaktstelle für technischen Support, die den Betrieb und die Wartung der in Artikel 4 Absatz 1 genannten gemeinsamen Dienste sicherstellt.

(2) Die zentrale Kontaktstelle für technische Unterstützung stellt die Verbindung zu anderen einschlägigen Kontaktstellen der Kommission her und koordiniert die Lösung von Problemen mit eDelivery-Zugangspunkten oder eIDAS-Knoten.

(3) Die Kommission stellt sicher, dass ihre zentrale Kontaktstelle für technische Unterstützung in einer Weise organisiert ist, die es ihr ermöglicht, ihre Aufgaben unter allen Umständen zu erfüllen und kurzfristig Maßnahmen zu ergreifen.

Artikel 21

Nationale zentrale Kontaktstelle für technische Unterstützung

(1) Jeder Mitgliedstaat benennt eine zentrale Kontaktstelle für technische Unterstützung, um den Betrieb und die Wartung der einschlägigen Komponenten des OOTS, für die der jeweilige Mitgliedstaat gemäß Abschnitt 9 zuständig ist, sicherzustellen.

(2) Die zentralen Kontaktstellen für technische Unterstützung

a) stellen den Nachweislieferanten und Nachweise anfordernden Behörden bei allen technischen Problemen im Zusammenhang mit dem Betrieb des OOTS Fachwissen und Beratung zur Verfügung und stellen erforderlichenfalls eine Verbindung zur Kontaktstelle für technische Unterstützung der Kommission und zu anderen Kontaktstellen für technische Unterstützung her;

b) untersuchen und beheben mögliche Ausfälle der eDelivery-Zugangspunkte, mögliche Sicherheitsverletzungen und andere Vorfälle;

c) unterrichten die Kontaktstellen für technische Unterstützung über alle Tätigkeiten, die zu einer Verletzung oder einer mutmaßlichen Verletzung der Sicherheit der elektronischen Systeme führen könnten.

(3) Werden von einem Nachweislieferanten Zweifel an der Rechtmäßigkeit einer oder mehrerer Nachweisanfragen geäußert, so ist die zentrale Kontaktstellen für technischen Support verpflichtet,

a) die Nachweisanfragen oder Stichproben von Nachweisanfragen, die in der Vergangenheit von derselben Nachweise anfordernden Behörde übermittelt wurden, zu überprüfen;

b) die vom Mitgliedstaat der Nachweise anfordernden Behörde benannte zentrale Kontaktstelle für technische Unterstützung über das in Artikel 22 genannte Dashboard für technische Unterstützung um die Übermittlung von Protokollen ausgewählter Austauschvorgänge gemäß Artikel 17 zu ersuchen;

c) den nationalen Koordinator auf das Problem aufmerksam zu machen, sofern es weiterhin besteht.

(4) Die Mitgliedstaaten stellen sicher, dass ihre jeweilige zentrale Kontaktstelle für technische Unterstützung in einer Weise organisiert ist, die es ihr ermöglicht, ihre Aufgaben unter allen Umständen zu erfüllen und kurzfristig Maßnahmen zu ergreifen.

Artikel 22

Dashboard für technische Unterstützung

(1) Die Kommission richtet ein Dashboard ein, um die Kommunikation zwischen allen Kontaktstellen für technische Unterstützung zu erleichtern.

(2) Die Mitgliedstaaten und die Kommission erfassen die Kontaktdaten der Kontaktstellen für technische Unterstützung im Dashboard und halten sie auf dem neuesten Stand.

(3) Die Kontaktstellen sind verpflichtet, über das Dashboard

a) jeden Vorfall, der als erheblich erachtet wird, zu melden;

b) alle vorübergehenden oder dauerhaften Maßnahmen, die nach Vorfällen ergriffen wurden, zu melden;

c) bei den zuständigen Kontaktstellen für technische Unterstützung die Protokolle ausgewählter Austauschvorgänge in den in Artikel 17 Absatz 5 genannten Fällen und bei Zweifeln hinsichtlich der Rechtmäßigkeit der Nachweisanfrage gemäß Artikel 21 Absatz 3 anzufordern;

d) im Falle von Vorfällen jede andere erforderliche Unterstützung anzufordern.

(4) Die nationalen Koordinatoren und der Vorsitzende der Koordinierungsgruppe für das Zugangstor haben Zugang zum Dashboard.

(5) Die Kommission und die nationalen Koordinatoren nutzen das Dashboard, um die in Artikel 27 und Artikel 28 Absatz 2 genannten Informationen bereitzustellen.

ABSCHNITT 8

ZUSAMMENARBEIT MIT ANDEREN GOVERNANCE-STRUKTUREN

Artikel 23

Umfang der Zusammenarbeit

Die Kommission, die Koordinierungsgruppe für das Zugangstor und ihre Untergruppen arbeiten mit den einschlägigen, durch das Unionsrecht oder internationale Übereinkünfte geschaffenen Governance-Strukturen in den für das OOTS relevanten Bereichen zusammen, um Synergien zu erzielen und die in diesen anderen Gremien entwickelten Lösungen so weit wie möglich wiederzuverwenden.

ABSCHNITT 9

VERANTWORTLICHKEITEN FÜR WARTUNG UND BETRIEB DER KOMPONENTEN DES OOTS

Artikel 24

Verantwortlichkeiten der Kommission

Die Kommission ist Eignerin der gemeinsamen Dienste und des Dashboards für technische Unterstützung und zuständig für deren Entwicklung, Verfügbarkeit, Überwachung, Aktualisierung, Wartung und Hosting.

Artikel 25

Verantwortlichkeiten der Mitgliedstaaten

Jeder Mitgliedstaat gilt hinsichtlich der in Artikel 2 Buchstaben a bis f und h genannten nationalen Komponenten des OOTS als deren Eigner und ist gegebenenfalls für die Einrichtung sowie für die Entwicklung, Verfügbarkeit, Überwachung, Aktualisierung, Wartung und das Hosting verantwortlich.

Artikel 26

Änderungen und Aktualisierungen

(1) Die Kommission unterrichtet die Mitgliedstaaten über Änderungen und Aktualisierungen der gemeinsamen Dienste.

(2) Die Mitgliedstaaten unterrichten die Kommission über Änderungen und Aktualisierungen der in ihre Zuständigkeit fallenden Komponenten, die Auswirkungen auf die Funktion des OOTS haben könnten.

(3) Informationen über kritische Aktualisierungen werden unverzüglich zur Verfügung gestellt. Bei anderen, nicht kritischen Aktualisierungen, die Auswirkungen auf Komponenten des OOTS, die Eigentum anderer Mitgliedstaaten sind, oder die gemeinsamen Dienste haben können, wird die Vorlaufzeit von der Koordinierungsgruppe für das Zugangstor auf der Grundlage eines Vorschlags der zuständigen Untergruppe festgelegt.

Artikel 27

Verfügbarkeit des OOTS

(1) Das OOTS ist rund um die Uhr und sieben Tage pro Woche mit einer Verfügbarkeitsrate der eDelivery-Zugangspunkte, der Vorschaubereiche und der gemeinsamen Dienste von mindestens 98 % in Betrieb, mit Ausnahme der gemäß Absatz 2 dieses Artikels geplanten Wartungsarbeiten. Die Verfügbarkeitsziele für die übrigen Komponenten des OOTS werden in den in Artikel 19 Absatz 1 Buchstabe d genannten Dienstleistungsvereinbarungen festgelegt.

(2) Die Mitgliedstaaten und die Kommission kündigen die geplanten Wartungsarbeiten in Bezug auf die betreffenden Komponenten des OOTS wie folgt an:

a) fünf Arbeitstage vor Wartungsarbeiten, die eine Nichtverfügbarkeit von bis zu vier Stunden zur Folge haben können;

b) zehn Arbeitstage vor Wartungsarbeiten, die eine Nichtverfügbarkeit von bis zu zwölf Stunden zur Folge haben können;

c) 30 Arbeitstage vor Wartungsarbeiten an der Infrastruktur des Datenzentrums, die eine Nichtverfügbarkeit von bis zu sechs Tagen pro Jahr zur Folge haben können.

Soweit möglich, werden Wartungsarbeiten außerhalb der Arbeitszeiten geplant.

(3) Sofern Mitgliedstaaten feste wöchentliche Wartungszeiten festgelegt haben, unterrichten sie die Kommission darüber, an welchem Tag und zu welchen Uhrzeiten solche festen wöchentlichen Wartungszeiten geplant sind. Unbeschadet der in Absatz 2 Buchstaben a, b und c genannten Verpflichtungen sind die Mitgliedstaaten von der Verpflichtung befreit, die Kommission jedes Mal davon in Kenntnis zu setzen, wenn die Systeme während solcher fester Wartungszeiten nicht verfügbar sind.

(4) Im Falle eines unerwarteten technischen Ausfalls der Komponenten des OOTS der Mitgliedstaaten unterrichtet der betreffende Mitgliedstaat die anderen Mitgliedstaaten und die Kommission unverzüglich über deren Nichtverfügbarkeit und, sofern dies bekannt ist, über den Zeitpunkt der voraussichtlichen Wiederaufnahme des Betriebs der Komponenten.

(5) Im Falles eines unerwarteten Ausfalls der gemeinsamen Dienste unterrichtet die Kommission die Mitgliedstaaten unverzüglich über die Nichtverfügbarkeit eines oder mehrerer gemeinsamer Dienste und, sofern dies bekannt ist, über den Zeitpunkt der voraussichtlichen Wiederaufnahme des Betriebs des Dienstes.

(6) Die in diesem Artikel genannten Benachrichtigungen sind über das in Artikel 22 genannte Dashboard für technische Unterstützung vorzunehmen.

ABSCHNITT 10

SICHERHEIT

Artikel 28

Sicherheit der gemeinsamen Dienste und der nationalen Komponenten

(1) Die Kommission gewährleistet die Sicherheit der in Artikel 4 Absatz 1 genannten gemeinsamen Dienste sowie der in Artikel 2 Buchstabe h genannten Integrationselemente und Schnittstellen, für die sie zuständig ist.

(2) Die Mitgliedstaaten gewährleisten die Sicherheit der nationalen Komponenten des OOTS und der in Artikel 2 Buchstabe h genannten Integrationselemente und Schnittstellen, für die sie zuständig sind.

(3) Die Mitgliedstaaten und die Kommission treffen zu den in den Absätzen 1 und 2 genannten Zwecken zumindest für die Komponente, für die sie zuständig sind, die erforderlichen Maßnahmen, um

a) zu verhindern, dass Unbefugte Zugang zu Komponenten erhalten, für die die Mitgliedstaaten zuständig sind,

b) zu verhindern, dass Unbefugte Daten eingeben, abfragen, ändern oder löschen,

c) etwaige Aktivitäten gemäß den Buchstaben a und b aufzudecken und

d) dafür zu sorgen, dass Sicherheitsvorfälle gemäß den anerkannten internationalen Sicherheitsnormen für die Informationstechnologie protokolliert werden.

(4) Die Mitgliedstaaten stellen insbesondere sicher, dass

a) die von ihnen betriebenen Verbindungen zu und von den eDelivery-Zugangspunkten sowie die gesamte interne Kommunikation zwischen verschiedenen nationalen Behörden mindestens dasselbe Sicherheitsniveau wie der elektrische Zustelldienst eDelivery erfüllen, um die Sicherheit und Vertraulichkeit des Austauschs und die Integrität der über das OOTS ausgetauschten Nachweise zu schützen;

b) die Herkunft der von dem Zugangspunkt der Nachweise anfordernden Behörde übermittelten Nachweisanfrage und die von dem Zugangspunkt des Nachweislieferanten übermittelte Antwort auf eine Nachweisanfrage oder Fehlermeldung nicht widerlegt werden können.

(5) Nach Absatz 4 ist der Mitgliedstaat des Nachweislieferanten bei einem bestimmten Austausch von Nachweisen für die Qualität, Vertraulichkeit, Integrität und Verfügbarkeit der angeforderten Nachweise verantwortlich, bis diese den eDelivery-Zugangspunkt der Nachweise anfordernden Behörde oder gegebenenfalls eine intermediäre Plattform erreichen. Der Mitgliedstaat der Nachweise anfordernden Behörde ist in einem bestimmten Austausch von Nachweisen für die Vertraulichkeit und Integrität der angeforderten Nachweise ab dem Zeitpunkt zuständig, zu dem sie seinen eDelivery-Zugangspunkt erreichen.

(6) Die Mitgliedstaaten und die Kommission gewährleisten die Vertraulichkeit, Integrität und Verfügbarkeit der in Artikel 17 Absätze 1, 2 und 3 genannten Protokolle durch geeignete und verhältnismäßige Sicherheitsmaßnahmen für die von ihnen aufgezeichneten Protokolle.

Artikel 29

Überwachung der elektronischen Systeme

(1) Die Mitgliedstaaten und die Kommission führen regelmäßige Kontrollen der Komponenten des OOTS, für die sie zuständig sind, durch.

(2) Die in den Artikeln 20 und 21 genannten zentralen Kontaktstellen für technische Unterstützung nutzen das in Artikel 22 genannte Dashboard für die technische Unterstützung, um einander über die bei den Kontrollen festgestellten Mängel, die zu einer Verletzung oder einer mutmaßlichen Verletzung der Sicherheit des OOTS führen könnten, zu unterrichten.

Artikel 30

Verwaltungsmanagementsystem

Die Kommission richtet ein Verwaltungsmanagementsystem ein, um die Authentifizierungs- und Autorisierungsregeln für die Validierung der Identifizierungsdaten, die den Zugang zu den gemeinsamen Diensten und dem Dashboard für technische Unterstützung ermöglichen, zu verwalten.

ABSCHNITT 11

SCHLUSSBESTIMMUNGEN

Artikel 31

Erprobung des OOTS

(1) Die Mitgliedstaaten und die Kommission legen im Rahmen der Koordinierungsgruppe für das Zugangstor einen Zeitplan für die Erprobung und eine Reihe von Indikatoren fest, anhand deren die Ergebnisse der Erprobung gemessen und als positiv gewertet werden können.

(2) Die Kommission stellt Erprobungsdienste zur Verfügung, die die Mitgliedstaaten nutzen können, um die Konformität der technischen Lösungen mit den in Absatz 1 genannten Indikatoren zu untersuchen.

(3) Die Mitgliedstaaten und die Kommission erproben die Funktion der einzelnen Komponenten des OOTS und überprüfen, ob sie gemäß den in Absatz 1 genannten Indikatoren ordnungsgemäß funktionieren können. Es werden nur diejenigen Komponenten des OOTS, bei denen die Erprobung zu positiven Ergebnissen führt, den Nutzern zur Verfügung gestellt.

Artikel 32

Unterstützung durch die Kommission

Die Kommission stellt ein Team von Sachverständigen als Teil der Kontaktstelle der Kommission für technische Unterstützung zur Verfügung, das die nationalen Kontaktstellen für technische Unterstützung und die nationalen Koordinatoren in allen Aspekten im Zusammenhang mit der Funktionsweise des OOTS in technischer Hinsicht unterstützt, insbesondere bei

a) der Bereitstellung von Leitlinien,

b) der Organisation von Workshops und Vorführungen,

c) der Beantwortung einzelner Fragen.

Artikel 33

Verarbeitung personenbezogener Daten

Die zuständigen Behörden der Mitgliedstaaten handeln in Bezug auf die Verarbeitung personenbezogener Daten, die in den über das OOTS ausgetauschten Nachweisen enthalten und in den Komponenten des OOTS gespeichert sind, deren Eigentümer sie gemäß Artikel 25 der vorliegenden Verordnung sind, in ihrer Eigenschaft als Nachweise anfordernde Behörde oder Nachweislieferant als Verantwortliche im Sinne von Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 und wie in den Artikeln 34 und 35 der vorliegenden Verordnung näher ausgeführt.

Artikel 34

Aufgaben der Nachweise anfordernden Behörde als Verantwortliche

(1) Bei jedem Austausch von Nachweisen über das OOTS ist allein die jeweilige Nachweise anfordernde Behörde oder gegebenenfalls die intermediäre Plattform für die Vollständigkeit und Rechtmäßigkeit der Nachweisanfrage zuständig. Die Nachweise anfordernde Behörde vergewissert sich insbesondere, dass die Nachweise für das jeweilige Verfahren, für das sie von einem Nutzer angefordert werden, erforderlich sind.

(2) Sobald die über das OOTS ausgetauschten Nachweise der Nachweise anfordernden Behörde oder gegebenenfalls der intermediären Plattform zur Verfügung stehen, entweder nachdem der Nutzer entschieden hat, mit dem Austausch von Nachweisen gemäß Artikel 14 Absatz 3 Buchstabe f der Verordnung (EU) 2018/1724 fortzufahren, oder im Falle der in Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 genannten Verfahren, stellt die Nachweise anfordernde Behörde oder gegebenenfalls die intermediäre Plattform dasselbe Schutzniveau für personenbezogene Daten gemäß der Verordnung (EU) 2016/679 wie in einer Situation sicher, in der der Nutzer die Nachweise übermittelt oder hochlädt, ohne auf das OOTS zurückzugreifen.

Artikel 35

Aufgaben des Nachweislieferanten als Verantwortlicher

(1) Der jeweilige Nachweislieferant bzw. die intermediäre Plattform ist unbeschadet seiner bzw. ihrer Verpflichtungen gemäß der Verordnung (EU) 2016/679 bei jedem Austausch von Nachweisen über das OOTS allein dafür zuständig, zu überprüfen,

a) ob die angeforderten Nachweise, die sich in seinem bzw. ihrem Besitz befinden, dem Nutzer gemäß Artikel 16 zugeordnet werden können,

b) ob der Nutzer berechtigt ist, den angeforderten Nachweis zu verwenden.

(2) Stellt eine intermediäre Plattform den Vorschaubereich gemäß Artikel 15 Absatz 1 Buchstabe b Ziffer ii der vorliegenden Verordnung zur Verfügung, so gilt sie als Auftragsverarbeiter, der im Namen des Nachweislieferanten gemäß Artikel 4 Nummer 8 der Verordnung (EU) 2016/679 handelt.

Artikel 36

Inkrafttreten

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

Sie gilt ab dem 12. Dezember 2023.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 5. August 2022

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN