Amtsblatt
der Europäischen Union

DE
Reihe L

2026/2083

21.9.2026

DURCHFÜHRUNGSVERORDNUNG (EU) 2026/2083 DER KOMMISSION

vom 18. September 2026

über MyHealth@EU

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847 ([1]), insbesondere auf Artikel 23 Absätze 4 und 8,

in Erwägung nachstehender Gründe:

(1) Ziel der Verordnung (EU) 2025/327 ist es, einerseits den Zugang natürlicher Personen zu ihren personenbezogenen elektronischen Gesundheitsdaten und ihre Kontrolle über diese Daten im Zusammenhang mit der Gesundheitsversorgung sowie andererseits den grenzüberschreitenden Austausch solcher Daten zu verbessern, damit die Kontinuität der Gesundheitsversorgung gewährleistet ist. Dazu wird der Kommission in Artikel 23 der genannten Verordnung der Auftrag erteilt, mit MyHealth@EU eine zentrale Interoperabilitätsplattform für den grenzüberschreitenden Austausch der in Artikel 14 der genannten Verordnung aufgeführten prioritären Datenkategorien sowie zusätzlicher Datenkategorien einzurichten. Der Austausch dieser Daten wird durch das europäische Austauschformat für elektronische Gesundheitsaufzeichnungen gemäß Artikel 15 der Verordnung (EU) 2025/327 unterstützt.

(2) MyHealth@EU nach der Verordnung (EU) 2025/327 baut auf der Architektur und den Prozessen auf, die für die eHealth-Service-Infrastruktur für grenzüberschreitende elektronische Gesundheitsinformationsdienste entwickelt wurden, welche mit dem Durchführungsbeschluss 2019/1765 der Kommission ([2]) eingerichtet wurde. Mit dieser Infrastruktur konnten die Mitgliedstaaten Patientenkurzakten, elektronische Verschreibungen und elektronische Abgaben von Arzneimitteln auf freiwilliger Basis austauschen. MyHealth@EU nach der Verordnung (EU) 2025/327 sollte auf dieser Erfahrung sowie der Architektur der im Rahmen des Durchführungsbeschlusses 2019/1765 entwickelten Dienste aufbauen, angepasst an technologische Entwicklungen und unter Berücksichtigung der Unterschiede zum europäischen Gesundheitsdatenraum.

(3) In Artikel 24 Absätze 2 und 3 der Verordnung (EU) 2025/327 ist die Möglichkeit der Anbindung befugter Teilnehmer an MyHealth@EU vorgesehen. In diesen Fällen sollten Artikel 7 mit Ausnahme von Absatz 1 Buchstabe a sowie die Artikel 8 bis 13 der vorliegenden Verordnung sinngemäß für befugte Teilnehmer gelten, damit die Kohärenz bei der Meldung erheblicher Sicherheitsvorfälle, den Konformitätsprüfungen und den technischen Anforderungen für die Aufrechterhaltung der Anbindung an MyHealth@EU gewährleistet ist.

(4) Um den Austausch personenbezogener elektronischer Gesundheitsdaten zwischen den nationalen Kontaktstellen für digitale Gesundheit zu erleichtern, sollte die Kommission eine Referenzimplementierungssoftware bereitstellen, die von den nationalen Kontaktstellen für digitale Gesundheit optional verwendet werden kann. Die Referenzimplementierung sollte auf dem Anforderungskatalog beruhen und regelmäßig aktualisiert werden, um Veränderungen Rechnung zu tragen.

(5) Um die semantische Interoperabilität der Dienste im Rahmen von MyHealth@EU zu gewährleisten, sollte die Kommission einen zentralen Terminologiedienst bereitstellen, der den Mitgliedstaaten die Möglichkeit bietet, Mappings und Übersetzungen zwischen Kodiersystemen und Werten des in Artikel 15 Absatz 1 der Verordnung (EU) 2025/327 genannten europäischen Austauschformats für elektronische Gesundheitsaufzeichnungen bereitzustellen.

(6) Die nationalen Kontaktstellen für digitale Gesundheit sollten personenbezogene elektronische Gesundheitsdaten grenzüberschreitend über ein sicheres Kommunikationsnetz austauschen, das von der Kommission bereitgestellt werden sollte.

([1]) ABl. L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj.

([2]) Durchführungsbeschluss 2019/1765 der Kommission vom 22. Oktober 2019 mit Vorschriften für die Errichtung, die Verwaltung und die Funktionsweise des Netzwerks der für elektronische Gesundheitsdienste zuständigen nationalen Behörden und zur Aufhebung des Durchführungsbeschlusses 2011/890/EU (ABl. L 270 vom 24.10.2019, S. 83, ELI: http://data.europa.eu/eli/dec_impl/2019/1765/oj).

(7) Damit nationale Kontaktstellen für digitale Gesundheit einander erkennen und eine vertrauenswürdige Kommunikation aufbauen können, sollten sie einen zentralen Konfigurationsdienst nutzen, den die Kommission bereitstellen sollte.

(8) Um die Interoperabilität zu gewährleisten, sollte die Kommission in Zusammenarbeit mit der gemäß Artikel 95 Absatz 1 der Verordnung (EU) 2025/327 eingerichteten europäischen Lenkungsgruppe MyHealth@EU einen Anforderungskatalog erstellen. Die Kommission sollte auf der Grundlage dieser Anforderungen technische Spezifikationen zur Bewilligung durch die Lenkungsgruppe vorschlagen. Die technischen Spezifikationen sollten mit dem europäischen Austauschformat für elektronische Gesundheitsaufzeichnungen in Einklang stehen, das in dem gemäß der Befugnisübertragung nach Artikel 15 Absatz 1 der Verordnung (EU) 2025/327 zu erlassenden Durchführungsrechtsakt festgelegt wird.

(9) Die Kommission sollte der Lenkungsgruppe einen jährlichen Arbeitsplan für den Betrieb und die Verwaltung der zentralen Interoperabilitätsplattform zur Bewilligung vorlegen. Dieser sollte auf den Zweijahres-Arbeitsplan des Ausschusses für den europäischen Gesundheitsdatenraum abgestimmt sein.

(10) Änderungen, die entweder nicht rückwirkend mit der vorherigen Version kompatibel sind oder deren Umsetzung für die nationalen Kontaktstellen für digitale Gesundheit und die befugten Teilnehmer verpflichtend ist, werden als Major Release behandelt und unterliegen dem vollständigen Änderungsmanagementverfahren. Im Gegensatz dazu sollte bei Korrekturen von Mängeln und Bugs, redaktionellen Klarstellungen und anderen Änderungen, mit denen keine neuen Funktionen eingeführt werden oder die Fähigkeit bestehender Implementierungen des Anforderungskatalogs zum Austausch nicht modifizierter Daten nicht beeinträchtigt wird, das vereinfachte Verfahren für das Minor Release befolgt werden. Vorschläge für größere Änderungen des Anforderungskatalogs sollten gründlich vorbereitet werden, bevor sie der Lenkungsgruppe zur Bewertung und Bewilligung vorgelegt werden. Daher sollte vorschriftsmäßig entweder eine Gruppe von Mitgliedern der Lenkungsgruppe oder die Kommission einen Änderungsvorschlag vorlegen, da diese für die Verwaltung von MyHealth@EU. zuständig ist.

(11) Um eine hohe Qualität bei der Entwicklung und beim Betrieb des Austauschs personenbezogener elektronischer Gesundheitsdaten über MyHealth@EU zu gewährleisten, sollte die Kommission im Namen der Lenkungsgruppe MyHealth@EU die Genehmigungsverfahren für den Austausch personenbezogener elektronischer Gesundheitsdaten verwalten.

(12) Die nationalen Kontaktstellen für digitale Gesundheit sollten durch technische Prüfungen und Konformitätsprüfungen nachweisen, dass sie den Anforderungskatalog einhalten. Die Kommission sollte technische Prüfungen erleichtern und Konformitätsprüfungen durchführen. Anschließend sollte die Kommission auf Abweichungen vom Anforderungskatalog hinweisen. Die Feststellungen der Konformitätsprüfungen und technischen Prüfungen sollten anhand von Faktoren wie Risiko und Folgen klassifiziert werden. Die nationalen Kontaktstellen für digitale Gesundheit sollten Aktionspläne zur Beseitigung festgestellter Risiken aufstellen. Die Kommission sollte der Lenkungsgruppe regelmäßig über alle weiterhin offenen Feststellungen und die diesbezüglichen Aktionspläne berichten.

(13) Eine nationale Kontaktstelle für digitale Gesundheit sollte sich stets an die neueste Version des Anforderungskatalogs halten. Um das Vertrauen in das Netz zu fördern und allen anderen nationalen Kontaktstellen zu zeigen, dass sie sich daran hält, sollte sie sich regelmäßig Konformitätsprüfungen unterziehen. Eine Konformitätsprüfung sollte ein gründliches Verfahren sein, und ihre Häufigkeit sollte in einem angemessenen Verhältnis zu dem Risiko stehen, das der Austausch personenbezogener elektronischer Gesundheitsdaten für deren Schutz, Sicherheit und Vertraulichkeit darstellt. Besteht der Verdacht, dass eine nationale Kontaktstelle für digitale Gesundheit gegen die Anforderungen verstößt, dann sollte die Kommission befugt sein, eine Ad-hoc-Konformitätsprüfung einzuleiten.

(14) Wenn eine nationale Kontaktstelle für digitale Gesundheit den Austausch personenbezogener elektronischer Gesundheitsdaten aufnimmt, sollte sie dies auf der Grundlage einer Genehmigung der Lenkungsgruppe tun. Damit wird sichergestellt, dass die Lenkungsgruppe den Austausch personenbezogener elektronischer Gesundheitsdaten kontrolliert. Damit die nationalen Kontaktstellen für digitale Gesundheit, die den Austausch aufnehmen, Planungssicherheit haben, sollte die Entscheidung der Lenkungsgruppe auf dem Ergebnis einer entsprechenden Konformitätsprüfung und technischen Prüfung beruhen.

(15) Um die Interoperabilität zwischen den nationalen Kontaktstellen für digitale Gesundheit beim Austausch personenbezogener elektronischer Gesundheitsdaten sicherzustellen, sollten sie dieselbe Version des Anforderungskatalogs verwenden. Technische Lösungen, die sich nach diesen Anforderungen richten, sollten ausgiebig geprüft werden, ehe sie beim Austausch personenbezogener elektronischer Gesundheitsdaten zum Einsatz kommen. Die Lenkungsgruppe sollte die Ergebnisse dieser Prüfungen bewerten und einer nationalen Kontaktstelle für digitale Gesundheit das Upgrade zu einem neuen Major Release genehmigen.

(16) Nach einer Konformitätsprüfung einer nationalen Kontaktstelle für digitale Gesundheit, die bereits personenbezogene elektronische Gesundheitsdaten austauscht, sollte die Lenkungsgruppe das Ergebnis bewerten und die Fortsetzung des Austauschs genehmigen.

(17) Es kann sein, dass eine nationale Kontaktstelle für digitale Gesundheit herausfindet, dass der Austausch personenbezogener elektronischer Gesundheitsdaten nicht richtig funktioniert. Die Kommission sollte in Zusammenarbeit mit der Lenkungsgruppe in einem Betriebsrahmen die Arten dieser Sicherheitsvorfälle erfassen und darin bestimmen, wie angemessen darauf reagiert werden kann.

(18) Es sollte klar definiert werden, welche personenbezogenen elektronischen Gesundheitsdaten durch MyHealth@EU verarbeitet werden können, und dies sollte den in der Verordnung (EU) 2025/327 festgelegten Verpflichtungen entsprechen.

(19) In Artikel 23 der Verordnung (EU) 2025/327 wird den nationalen Kontaktstellen für digitale Gesundheit die Aufgabe der gemeinsam Verantwortlichen und der Kommission die des Auftragsverarbeiters bei der Bereitstellung von MyHealth@EU zugewiesen. Damit einheitliche Bedingungen für die Durchführung der Verordnung (EU) 2025/327 gewährleistet sind, sollten die Aufgaben und Zuständigkeiten der nationalen Kontaktstellen für digitale Gesundheit und der Kommission in der vorliegenden Verordnung auf der Grundlage dieser Zuweisung festgelegt werden. Dazu sollten in der vorliegenden Verordnung der Gegenstand, die Dauer, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen sowie die Pflichten und Rechte des Verantwortlichen festgelegt werden, sofern sie nicht bereits in der Verordnung (EU) 2025/327 definiert wurden. Auch sollten darin die jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen festgelegt werden.

(20) Gemäß der Verordnung (EU) 2025/327 fungiert die Kommission als Auftragsverarbeiterin für die Verarbeitung personenbezogener Daten in MyHealth@EU im Namen der Mitgliedstaaten als gemeinsam Verantwortliche. Gemäß den Datenschutzvorschriften müssen die Verpflichtungen des Auftragsverarbeiters in einem Vertrag oder einem anderen Rechtsakt festgelegt werden, der den Auftragsverarbeiter gegenüber dem Verantwortlichen bindet. Mit dieser Verordnung werden die Verpflichtungen der Kommission als Auftragsverarbeiterin in einem verbindlichen Rechtsakt genau festgelegt. Vergleichbar müssen die gemeinsam Verantwortlichen ihre jeweiligen Zuständigkeiten für die Einhaltung ihrer Datenschutzpflichten durch eine Vereinbarung untereinander festlegen, sofern und soweit die jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen nicht durch Unionsrecht oder mitgliedstaatliches Recht festgelegt sind, dem die gemeinsam Verantwortlichen unterliegen. In dieser Verordnung werden die jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen gesetzlich festgelegt.

(21) Jede Verarbeitung personenbezogener Daten gemäß dieser Verordnung unterliegt den Verordnungen (EU) 2016/679 ([3]) und (EU) 2018/1725 ([4]) des Europäischen Parlaments und des Rates, soweit anwendbar. Die Kommission unterstützt mit der Verarbeitung personenbezogener Daten in ihrer Rolle als Auftragsverarbeiterin den Datenaustausch zwischen den nationalen Kontaktstellen für digitale Gesundheit, der eine Aufgabe im öffentlichen Interesse ist, die ihnen mit der Verordnung (EU) 2025/327 übertragen wurde.

(22) Für MyHealth@EU gelten die im Beschluss (EU, Euratom) 2017/46 der Kommission ([5]) festgelegten Vorschriften für die IT-Sicherheit.

(23) MyHealth@EU ist eine Weiterentwicklung der digitalen eHealth-Diensteinfrastruktur für grenzüberschreitende elektronische Gesundheitsinformationsdienste, die mit dem Durchführungsbeschluss 2019/1765 eingerichtet wurde, weshalb die daraus gewonnenen Erkenntnisse berücksichtigt werden sollten. Da die einzelnen technischen Anforderungen an den Datenaustausch im Wesentlichen gleichwertig sind, sollten insbesondere nationale Kontaktstellen für elektronische Gesundheitsdienste, deren Produktivsystem bereits mit der digitalen eHealth-Diensteinfrastruktur für grenzüberschreitende elektronische Gesundheitsinformationsdienste verbunden ist und die ebenfalls als nationale Kontaktstelle dieses Mitgliedstaats für digitale Gesundheit benannt werden, die erste Konformitätsprüfung für die Dienste, die sie im Produktivsystem nutzen, nicht wiederholen müssen, da sie bereits nachgewiesen haben, dass sie sich mit der zentralen Plattform verbinden können.

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

([4]) 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 (Text von Bedeutung für den EWR) (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) 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, ELI: http://data.europa.eu/eli/dec/2017/46/oj).

(24) Die Verordnung (EU) 2025/327 wird schrittweise Geltung erlangen. Die Verpflichtungen zum Datenaustausch über MyHealth@EU gelten ab dem 26. März 2029 für den Austausch von Patientenkurzakten, elektronischen Verschreibungen und Abgaben von Arzneimitteln und ab dem 26. März 2031 für den Austausch von medizinischer Bildgebung und damit zusammenhängenden, auf Bildgebung gestützten Befunden, von Ergebnissen medizinischer Untersuchungen, einschließlich Labor- und anderer diagnostischer Ergebnisse und damit zusammenhängender Berichte, sowie von Entlassungsberichten. In der vorliegenden Verordnung werden die detaillierten Vorschriften für die Funktionsweise von MyHealth@EU festgelegt; die Verpflichtung der nationalen Kontaktstellen der Mitgliedstaaten für digitale Gesundheit zum Austausch der prioritären Kategorien personenbezogener elektronischer Gesundheitsdaten über MyHealth@EU erlangt gemäß Artikel 105 der Verordnung (EU) 2025/327 Geltung.

(25) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und gab am 18. Mai 2026 seine Stellungnahme ab ([6]).

(26) Mit dieser Durchführungsverordnung werden verbindliche Anforderungen an grenzüberschreitende digitale öffentliche Dienste im Sinne der Verordnung (EU) 2024/903 des Parlaments und des Rates ([7]) eingeführt. Dementsprechend wurde eine Bewertung der Interoperabilität durchgeführt und der Bericht dieser Bewertung wird im Portal für ein interoperables Europa veröffentlicht, wenn der Rechtsakt erlassen ist.

(27) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 98 Absatz 1 der Verordnung (EU) 2025/327 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL 1

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Anwendungsbereich

(1) In dieser Verordnung werden die Vorschriften für die Anforderungen an die Cybersicherheit, die technische Interoperabilität, die semantische Interoperabilität, den Betrieb und das Dienstmanagement in Bezug auf die Verarbeitung durch die Kommission als Auftragsverarbeiter sowie ihre Verantwortlichkeiten gegenüber den gemeinsam Verantwortlichen festgelegt.

Sie bietet die für die technische Entwicklung von MyHealth@EU erforderlichen Maßnahmen sowie detaillierte Vorschriften über die Sicherheit, die Vertraulichkeit und den Schutz personenbezogener elektronischer Gesundheitsdaten und die Bedingungen für die Konformitätsprüfungen, die erforderlich sind, um an MyHealth@EU teilzunehmen und damit verbunden zu bleiben.

(2) Artikel 7 mit Ausnahme von Absatz 1 Buchstabe a sowie die Artikel 8 bis 13 gelten sinngemäß für befugte Teilnehmer gemäß Artikel 24 Absätze 2 und 3 der Verordnung (EU) 2025/327. Die Konformitätsprüfungen und technischen Prüfungen können sich bei diesen befugten Teilnehmern auch auf zusätzliche Anforderungen erstrecken, die für sie relevant sind.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Lenkungsgruppe“ die gemäß Artikel 95 Absatz 1 der Verordnung (EU) 2025/327 eingerichtete Lenkungsgruppe MyHealth@EU für die grenzüberschreitenden Infrastrukturen gemäß Artikel 23 der genannten Verordnung;

([6]) EDPS Formal comments on the draft Commission Implementing Regulation on MyHealth@EU.

([7]) Verordnung (EU) 2024/903 des Europäischen Parlaments und des Rates vom 13. März 2024 über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Verordnung für ein interoperables Europa) (ABl. L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

2. „Major Release“ eine Version des Anforderungskatalogs und der technischen Spezifikationen, die nicht rückwirkend mit der vorhergehenden Version kompatibel ist oder erhebliche Auswirkungen auf den Austausch personenbezogener elektronischer Gesundheitsdaten über MyHealth@EU hat;

3. „Minor Release“ eine Version des Anforderungskatalogs und der technischen Spezifikationen sowie ihrer Anwendung, die kein Major Release ist;

4. „Sicherheitsvorfall“ einen Vorfall gemäß der Begriffsbestimmung in Artikel 6 Nummer 6 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([8]);

5. „erheblicher Sicherheitsvorfall“ einen Sicherheitsvorfall im Sinne von Artikel 23 Absatz 3 der Richtlinie (EU) 2022/2555.

KAPITEL 2

GRENZÜBERSCHREITENDER DATENAUSTAUSCH UND ZENTRALE INTEROPERABILITÄTSPLATTFORM FÜR DIGITALE GESUNDHEIT

Artikel 3

Zentrale Interoperabilitätsplattform für digitale Gesundheit

(1) Die Kommission erbringt folgende Dienste für die in Artikel 23 Absatz 1 der Verordnung (EU) 2025/327 genannte zentrale Interoperabilitätsplattform für digitale Gesundheit:

a) eine Referenzimplementierungssoftware für nationale Kontaktstellen für digitale Gesundheit;

b) einen zentralen Terminologiedienst;

c) ein sicheres Kommunikationsnetz;

d) einen zentralen Konfigurationsdienst.

(2) Die Kommission erbringt die in Absatz 1 genannten Dienste im Einklang mit dem Anforderungskatalog gemäß Artikel 4 Absatz 2 und den technischen Spezifikationen gemäß Artikel 4 Absatz 3.

(3) Die nationalen Kontaktstellen für digitale Gesundheit können die Referenzimplementierung gemäß Absatz 1 Buchstabe a zur Unterstützung des Austauschs personenbezogener elektronischer Gesundheitsdaten über MyHealth@EU nutzen. Sollte sich eine nationale Kontaktstelle für den Einsatz alternativer Lösungen entscheiden, müssen diese dem Anforderungskatalog gemäß Artikel 4 Absatz 2 und den technischen Spezifikationen gemäß Artikel 4 Absatz 3 genügen.

(4) Die nationalen Kontaktstellen für digitale Gesundheit können den in Absatz 1 Buchstabe b genannten zentralen Terminologiedienst zur Unterstützung der Übersetzung und des Mappings der für Datensätze mit personenbezogenen elektronischen Gesundheitsdaten zu verwendenden Kodiersysteme und Werte gemäß Artikel 15 Absatz 1 Unterabsatz 1 Buchstabe b der Verordnung (EU) 2025/327 nutzen.

(5) Die Mitgliedstaaten sind für die Übersetzung und das Mapping von Kodiersystemen und Wertesätzen für den Austausch personenbezogener elektronischer Gesundheitsdaten im europäischen Austauschformat für elektronische Gesundheitsaufzeichnungen gemäß Artikel 15 Absatz 1 der Verordnung (EU) 2025/327 zuständig. Die Mitgliedstaaten halten die Übersetzungen und Mappings auf dem neuesten Stand.

(6) Die nationalen Kontaktstellen für digitale Gesundheit nutzen das sichere Kommunikationsnetz gemäß Absatz 1 Buchstabe c zur Unterstützung des Austauschs personenbezogener elektronischer Gesundheitsdaten zwischen nationalen Kontaktstellen für digitale Gesundheit. Für den Betrieb nationaler Infrastrukturen und nationaler Dienste zur Unterstützung des sicheren Kommunikationsnetzes sind weiterhin die nationalen Kontaktstellen für digitale Gesundheit zuständig.

(7) Die nationalen Kontaktstellen für digitale Gesundheit nutzen den zentralen Konfigurationsdienst gemäß Absatz 1 Buchstabe d, um der Kommission und allen anderen nationalen Kontaktstellen für digitale Gesundheit ihre Konfigurationsdaten zur Verfügung zu stellen.

([8]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

Artikel 4

Anforderungskatalog und technische Spezifikationen

(1) Tauschen nationale Kontaktstellen für digitale Gesundheit grenzüberschreitend personenbezogene elektronische Gesundheitsdaten gemäß Artikel 23 Absatz 3 der Verordnung (EU) 2025/327 aus, so führen sie diesen Austausch entsprechend dem in Absatz 2 genannten Anforderungskatalog und den in Absatz 3 genannten technischen Spezifikationen durch.

(2) Die Kommission erstellt und pflegt in Zusammenarbeit mit der Lenkungsgruppe den Anforderungskatalog für den grenzüberschreitenden Austausch personenbezogener elektronischer Gesundheitsdaten in MyHealth@EU. Dieser Anforderungskatalog enthält mindestens

a) eine Beschreibung der für den Austausch personenbezogener elektronischer Gesundheitsdaten implementierten Anwendungsfälle;

b) Anforderungen an die Durchführung des Austauschs personenbezogener elektronischer Gesundheitsdaten;

c) Rahmen und Verfahren für Prüfungen, Konformitätsprüfungen, Betrieb und Überwachung von Sicherheitsvorfällen in Bezug auf den Austausch personenbezogener elektronischer Gesundheitsdaten.

(3) In Zusammenarbeit mit der Lenkungsgruppe schlägt die Kommission auf der Grundlage des Anforderungskatalogs gemäß Absatz 2 die technischen Spezifikationen vor.

(4) Die Lenkungsgruppe bewilligt den Anforderungskatalog gemäß Absatz 2 und die technischen Spezifikationen gemäß Absatz 3.

Artikel 5

Betrieb und Verwaltung von MyHealth@EU

(1) Die Kommission führt in Zusammenarbeit mit der Lenkungsgruppe für den Betrieb und die Verwaltung von MyHealth@EU folgende Tätigkeiten durch:

a) Ermittlung, Analyse und Verwaltung von Anforderungen und technischen Spezifikationen;

b) Koordinierung der Entwicklung, Prüfung und Einführung;

c) Änderungen am Anforderungskatalog;

d) Umgang mit Sicherheitsvorfällen;

e) Sicherstellung der Aufrechterhaltung des Betriebs der Plattform.

(2) Die Kommission führt folgende Aufgaben aus:

a) Durchführung technischer Prüfungen in Bezug auf den grenzüberschreitenden Austausch personenbezogener elektronischer Gesundheitsdaten;

b) Unterstützung der Service Desks der nationalen Kontaktstellen für digitale Gesundheit oder befugter Teilnehmer.

(3) Die Kommission schlägt in Zusammenarbeit mit der Lenkungsgruppe einen jährlichen Arbeitsplan für die in den Absätzen 1 und 2 genannten Tätigkeiten zur Bewilligung durch die Lenkungsgruppe vor.

Artikel 6

Änderungen am Anforderungskatalog

(1) Die Kommission kann der Lenkungsgruppe auf Antrag von fünf oder mehr Mitgliedern der Lenkungsgruppe oder von sich aus eine wesentliche Änderung des Anforderungskatalogs vorschlagen. Der Änderungsvorschlag enthält mindestens Folgendes:

a) eine Beschreibung der Änderungen;

b) eine Begründung der Änderungen;

c) einen Zeitplan für die Umsetzung der Änderungen;

d) ein Major Release zur Umsetzung der vorgeschlagenen Änderungen.

(2) Die Lenkungsgruppe ist dafür zuständig, die Änderungen an dem in Artikel 4 Absatz 2 genannten Anforderungskatalog, den Zeitplan für die Umsetzung der Änderungen und das Major Release zu bewilligen.

(3) Sobald die in Absatz 2 genannten Änderungen bewilligt sind, setzen die Kommission, die nationalen Kontaktstellen für digitale Gesundheit und die befugten Teilnehmer sie entsprechend dem bewilligten Zeitplan für die Umsetzung und dem bewilligten Major Release um.

(4) Für ein Minor Release wird kein Änderungsvorschlag vorgelegt. Die Kommission kann der Lenkungsgruppe eine Änderung für ein Minor Release vorlegen. Bei Vorlage einer solchen Änderung ist die Lenkungsgruppe nach deren Empfang für die Bewilligung des Vorschlags für ein Minor Release einschließlich des Zeitplans für die Umsetzung zuständig. Sobald das Minor Release bewilligt ist, setzen die Kommission, die nationalen Kontaktstellen für digitale Gesundheit und die befugten Teilnehmer dieses entsprechend dem bewilligten Zeitplan für die Umsetzung um.

Artikel 7

Verwaltung der Genehmigung für den grenzüberschreitenden Austausch personenbezogener elektronischer Gesundheitsdaten

(1) Die Kommission ist im Namen der Lenkungsgruppe für die Verwaltung der Verfahren zur Genehmigung des Austauschs personenbezogener elektronischer Gesundheitsdaten zuständig. Diese sind:

a) Erteilung der Genehmigung an eine nationale Kontaktstelle für digitale Gesundheit, den Austausch personenbezogener elektronischer Gesundheitsdaten aufzunehmen;

b) Erteilung der Genehmigung an eine nationale Kontaktstelle für digitale Gesundheit oder einen befugten Teilnehmer, den Austausch personenbezogener elektronischer Gesundheitsdaten nach dem Upgrade zum neuesten Major Release fortzusetzen;

c) Erteilung der Genehmigung an eine nationale Kontaktstelle für digitale Gesundheit oder einen befugten Teilnehmer, den Austausch personenbezogener elektronischer Gesundheitsdaten nach einer operativen Konformitätsprüfung gemäß Artikel 9 Buchstabe b fortzusetzen;

d) Behebung erheblicher Sicherheitsvorfälle beim Austausch personenbezogener elektronischer Gesundheitsdaten.

(2) Die Kommission schlägt in Zusammenarbeit mit der Lenkungsgruppe eine Methodik für die Genehmigungsverfahren gemäß Absatz 1 zur Bewilligung durch die Lenkungsgruppe vor.

(3) Die Lenkungsgruppe beschließt auf der Grundlage der in den Artikeln 10 bis 12 festgelegten Anforderungen, ob sie eine Genehmigung gemäß Absatz 1 Buchstaben a, b oder c erteilt.

(4) Beschließt die Lenkungsgruppe, eine Genehmigung gemäß Absatz 1 nicht zu erteilen, kann die nationale Kontaktstelle für digitale Gesundheit die Lenkungsgruppe ersuchen, ihre Entscheidung zu revidieren.

Artikel 8

Bedingungen für die Teilnahme an und die Aufrechterhaltung der Verbindung mit MyHealth@EU, Konformitätsprüfungen und technische Prüfungen

(1) Die Kommission führt Konformitätsprüfungen durch und erleichtert technische Prüfungen, um die Einhaltung des Anforderungskatalogs gemäß Artikel 4 Absatz 2 und der technischen Spezifikationen gemäß Artikel 4 Absatz 3 beim Austausch personenbezogener elektronischer Gesundheitsdaten zwischen den nationalen Kontaktstellen für digitale Gesundheit zu bewerten.

(2) Bei einer Konformitätsprüfung sind Feststellungen zur Sicherheit und Vertraulichkeit sowie zum Schutz des Austauschs personenbezogener elektronischer Gesundheitsdaten über MyHealth@EU zu treffen. Die Feststellungen werden abhängig von den Konformitätsgraden, die in dem in Artikel 4 Absatz 2 Buchstabe c genannten Rahmen für Konformitätsprüfungen festgelegt werden, als „geringfügig“, „mittelschwer“ oder „kritisch“ eingestuft.

(3) Bei einer technischen Prüfung sind der grenzüberschreitende Austausch personenbezogener elektronischer Gesundheitsdaten zwischen den nationalen Kontaktstellen für digitale Gesundheit über MyHealth@EU und deren Konformität mit den technischen Spezifikationen gemäß Artikel 4 Absatz 3 zu bewerten. Die Feststellungen werden abhängig von den Konformitätsgraden, die in dem in Artikel 4 Absatz 2 Buchstabe c genannten Rahmen für Prüfungen festgelegt werden, als „geringfügig“, „mittelschwer“ oder „kritisch“ eingestuft.

(4) Die Kommission teilt den nationalen Kontaktstellen für digitale Gesundheit die Ergebnisse der Konformitätsprüfungen und technischen Prüfungen gemäß Absatz 1 mit. Diese Mitteilung enthält mindestens Feststellungen, Bemerkungen und Empfehlungen auf der Grundlage der Ergebnisse der Konformitätsprüfungen und technischen Prüfungen.

(5) Hat eine Konformitätsprüfung oder technische Prüfung Feststellungen ergeben, dann ergreift die betreffende nationale Kontaktstelle für digitale Gesundheit unabhängig von deren Konformitätsgrad Maßnahmen, um die Feststellungen abzuschließen, nachdem sie von der Kommission über das Ergebnis der Konformitätsprüfung oder der technischen Prüfung informiert wurde. Nach Erhalt der Informationen über die Feststellungen ist der Kommission binnen 15 Werktagen ein Aktionsplan mit den Maßnahmen zur Behebung der festgestellten Mängel vorzulegen.

(6) Nach der Umsetzung eines Aktionsplans unterrichtet die nationale Kontaktstelle für digitale Gesundheit die Kommission. Anschließend bewertet die Kommission die entsprechenden Nachweise und beschließt, die jeweiligen Feststellungen gegebenenfalls abzuschließen.

(7) Die Kommission teilt der Lenkungsgruppe aus Konformitätsprüfungen und technischen Prüfungen stammende Feststellungen, die noch ungeklärt sind, regelmäßig mit.

Artikel 9

Häufigkeit der Konformitätsprüfungen

Die Kommission bewertet die Konformität des Austauschs personenbezogener elektronischer Gesundheitsdaten mit dem Anforderungskatalog gemäß Artikel 4 Absatz 2 und den technischen Spezifikationen gemäß Artikel 4 Absatz 3

a) vor Aufnahme des Austauschs personenbezogener elektronischer Gesundheitsdaten;

b) alle fünf Jahre nach der letzten Konformitätsprüfung;

c) wenn die Kommission der Ansicht ist, dass ein kritisches Risiko für die Sicherheit, die Vertraulichkeit und den Schutz personenbezogener elektronischer Gesundheitsdaten besteht.

Artikel 10

Genehmigung der Aufnahme des Austauschs personenbezogener elektronischer Gesundheitsdaten

Eine nationale Kontaktstelle für digitale Gesundheit lässt sich eine Genehmigung gemäß Artikel 7 Absatz 1 Buchstabe a erteilen, ehe sie den Austausch personenbezogener elektronischer Gesundheitsdaten aufnimmt. Die Genehmigung beruht auf:

a) einem Prüfungsergebnis ohne kritische Feststellungen gemäß Artikel 8 Absatz 4;

b) einem Konformitätsprüfungsergebnis ohne kritische Feststellungen gemäß Artikel 8 Absatz 4;

c) Aktionsplänen gemäß Artikel 8 Absatz 5.

Artikel 11

Genehmigung der Aktualisierung und Fortführung des Austauschs personenbezogener elektronischer Gesundheitsdaten nach einem Upgrade

(1) Jede nationale Kontaktstelle für digitale Gesundheit lässt sich spätestens einen Monat vor Ablauf des Zeitplans gemäß Artikel 6 Absatz 3 eine Genehmigung gemäß Artikel 7 Absatz 1 Buchstabe b erteilen. Die Genehmigung beruht auf einem Ergebnis einer technischen Prüfung gemäß Artikel 8 Absatz 4 ohne kritische Feststellungen.

(2) Erhält eine nationale Kontaktstelle für digitale Gesundheit keine Genehmigung gemäß Absatz 1, so ergreift die Lenkungsgruppe Abhilfemaßnahmen, die auch die befristete Aussetzung des Austauschs personenbezogener elektronischer Gesundheitsdaten umfassen können.

(3) Wird der Austausch personenbezogener elektronischer Gesundheitsdaten gemäß Absatz 2 ausgesetzt, ergreift die nationale Kontaktstelle für digitale Gesundheit folgende Maßnahmen:

a) sie schafft Abhilfe in Bezug auf die Feststellungen, die zu der Aussetzung geführt haben;

b) sie lässt sich eine Genehmigung gemäß Artikel 7 Absatz 1 Buchstabe b erteilen;

c) sie führt ein Upgrade auf das neueste Major Release durch und stellt den Austausch personenbezogener elektronischer Gesundheitsdaten wieder her.

Artikel 12

Fortsetzung des Austauschs personenbezogener elektronischer Gesundheitsdaten nach einer operativen Konformitätsprüfung

(1) Jede nationale Kontaktstelle für digitale Gesundheit lässt sich spätestens zwei Monate nach Erhalt des Ergebnisses einer Konformitätsprüfung gemäß Artikel 8 Absatz 4 eine Genehmigung gemäß Artikel 7 Absatz 1 Buchstabe c erteilen. Die Genehmigung beruht auf einem Ergebnis einer Konformitätsprüfung ohne kritische Feststellungen.

(2) Erhält eine nationale Kontaktstelle für digitale Gesundheit keine Genehmigung gemäß Absatz 1, so ergreift die Lenkungsgruppe Abhilfemaßnahmen, die auch die befristete Aussetzung des Austauschs personenbezogener elektronischer Gesundheitsdaten umfassen können.

(3) Wenn der Austausch personenbezogener elektronischer Gesundheitsdaten gemäß Absatz 2 ausgesetzt wird, ergreift die nationale Kontaktstelle für digitale Gesundheit folgende Maßnahmen:

a) sie schließt die Feststellungen, die zu der Aussetzung geführt haben, ab;

b) sie lässt sich eine Genehmigung gemäß Artikel 7 Absatz 1 Buchstabe c erteilen;

c) sie stellt den Austausch personenbezogener elektronischer Gesundheitsdaten wieder her.

Artikel 13

Erhebliche Sicherheitsvorfälle

(1) Eine nationale Kontaktstelle für digitale Gesundheit oder gegebenenfalls die Kommission meldet dem Vorsitz der Lenkungsgruppe, der Kommission und allen diesbezüglich betroffenen nationalen Kontaktstellen für digitale Gesundheit einen erheblichen Sicherheitsvorfall so bald wie möglich, in jedem Fall aber binnen 24 Stunden, nachdem sie davon Kenntnis erlangt hat.

(2) Die Kommission befasst sich im Anschluss an die in Absatz 1 genannte Meldung oder von sich aus im Einvernehmen mit dem Vorsitz der Lenkungsgruppe mit dem erheblichen Sicherheitsvorfall.

(3) Die nationale Kontaktstelle für digitale Gesundheit, deren grenzüberschreitender Austausch personenbezogener elektronischer Gesundheitsdaten von dem erheblichen Sicherheitsvorfall betroffen ist, und erforderlichenfalls die Lenkungsgruppe ergreifen die zur Eindämmung dieses Sicherheitsvorfalls notwendigen Maßnahmen. Diese Maßnahmen können die befristete Aussetzung des Austauschs personenbezogener elektronischer Gesundheitsdaten umfassen.

(4) Die betroffene nationale Kontaktstelle für digitale Gesundheit stellt den ausgesetzten grenzüberschreitenden Austausch personenbezogener elektronischer Gesundheitsdaten nach der Behebung des erheblichen Sicherheitsvorfalls mit Zustimmung der Lenkungsgruppe so bald wie möglich wieder her.

(5) Die nationale Kontaktstelle für digitale Gesundheit, deren grenzüberschreitender Austausch personenbezogener elektronischer Gesundheitsdaten von dem erheblichen Sicherheitsvorfall betroffen war, oder — wenn ein in Artikel 3 Absatz 1 genannter Dienst von dem erheblichen Sicherheitsvorfall betroffen war — die Kommission erstattet der Lenkungsgruppe spätestens einen Monat nach Übermittlung der in Absatz 1 genannten Meldung Bericht. Dieser Bericht muss mindestens Folgendes umfassen:

a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

b) Angaben zur Art der Bedrohung bzw. der zugrunde liegenden Ursache, die wahrscheinlich den erheblichen Sicherheitsvorfall ausgelöst hat;

c) die bereits ergriffenen oder noch laufenden Abhilfemaßnahmen.

KAPITEL 3

VERARBEITUNG, SICHERHEIT, VERTRAULICHKEIT UND SCHUTZ PERSONENBEZOGENER DATEN

Artikel 14

Verarbeitung personenbezogener Daten in MyHealth@EU

Die Verarbeitung personenbezogener Daten in MyHealth@EU ist beschränkt auf

a) die prioritären Kategorien personenbezogener elektronischer Gesundheitsdaten gemäß Artikel 14 Absatz 1 Unterabsatz 1 der Verordnung (EU) 2025/327;

b) die zusätzlichen Kategorien personenbezogener elektronischer Gesundheitsdaten gemäß Artikel 14 Absatz 1 Unterabsatz 3 der Verordnung (EU) 2025/327;

c) für die Verwaltung von MyHealth@EU, einschließlich des Helpdesk, erforderliche personenbezogene Daten.

Artikel 15

Aufgaben der nationalen Kontaktstellen für digitale Gesundheit als gemeinsam Verantwortliche

(1) Die nationalen Kontaktstellen für digitale Gesundheit haben in ihrer Eigenschaft als gemeinsam Verantwortliche die nachstehend aufgeführten Aufgaben.

a) Sie richten eine Anlaufstelle mit einem Funktionspostfach für die Kommunikation zwischen den gemeinsam Verantwortlichen und zwischen den gemeinsam Verantwortlichen und dem Auftragsverarbeiter ein.

b) Sie stimmen sich in der Lenkungsgruppe untereinander ab, um der Kommission als Auftragsverarbeiterin koordinierte Anweisungen zu erteilen.

c) Sie übermitteln der Kommission als Auftragsverarbeiterin über die Lenkungsgruppe alle erforderlichen, mit den anderen gemeinsam Verantwortlichen in der Gruppe vereinbarten Anweisungen.

d) Sie sind dafür verantwortlich, die betroffenen Personen gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679 über die Verarbeitung personenbezogener Daten in MyHealth@EU zu informieren.

e) Sie befassen sich mit Anträgen betroffener Personen auf Ausübung ihrer Rechte als betroffene Personen gemäß der Verordnung (EU) 2016/679. Geht bei einem gemeinsam Verantwortlichen ein Antrag ein, der nicht in seine Zuständigkeit für MyHealth@EU fällt, so leitet er den Antrag an den entsprechenden gemeinsam Verantwortlichen weiter und informiert die betroffene Person.

f) Sie ergreifen alle geeigneten organisatorischen, physischen und logischen Sicherheitsmaßnahmen, um den sicheren Betrieb jeder nationalen Kontaktstelle für digitale Gesundheit zu gewährleisten, und dokumentieren diese Maßnahmen. Mit diesen Maßnahmen wird sichergestellt, dass

   i) zur Verarbeitung der personenbezogenen Daten befugte Personen einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen oder sich zur Vertraulichkeit verpflichtet haben;

   ii) der Austausch personenbezogener Daten über MyHealth@EU systematisch protokolliert wird, um Aufzeichnungen über den Austausch personenbezogener Daten zu führen, einschließlich der Identität der beteiligten Akteure, der Kategorien personenbezogener Daten und der Zwecke, für die sie ausgetauscht wurden.

g) Sie unterstützen einander bei der Ermittlung von und beim Umgang mit Sicherheitsvorfällen im Zusammenhang mit der Verarbeitung in MyHealth@EU, einschließlich Verletzungen des Schutzes personenbezogener Daten. Insbesondere melden die gemeinsam Verantwortlichen einander und der Kommission

   i) alle Risiken für die Sicherheit der in MyHealth@EU verarbeiteten Daten;

   ii) jeden Sicherheitsvorfall im Zusammenhang mit Vorgängen zur Verarbeitung personenbezogener Daten in MyHealth@EU;

iii) jede Verletzung des Schutzes personenbezogener Daten, die wahrscheinlichen Folgen der Verletzung und die Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen sowie alle Maßnahmen, die ergriffen wurden, um gegen die Verletzung vorzugehen und das Risiko für jene Rechte und Freiheiten zu mindern;

iv) jeden Verstoß gegen technische oder organisatorische Schutzvorkehrungen für die Verarbeitungsvorgänge in MyHealth@EU.

h) Sie unterrichten die zuständigen Aufsichtsbehörden und, falls erforderlich, die betroffenen Personen im Einklang mit den Artikeln 33 und 34 der Verordnung (EU) 2016/679 über alle Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit Verarbeitungsvorgängen in MyHealth@EU.

i) Erforderlichenfalls arbeiten sie bei der Durchführung von Folgenabschätzungen zu den vorgesehenen Verarbeitungsvorgängen für den Schutz personenbezogener Daten gemäß Artikel 35 der Verordnung (EU) 2016/679 zusammen.

(2) Benötigt ein gemeinsam Verantwortlicher zur Erfüllung seiner Pflichten gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 Informationen von einem anderen gemeinsam Verantwortlichen, so übermittelt er eine besondere Anfrage an das in Absatz 1 Buchstabe a genannte einschlägige Funktionspostfach. Der andere gemeinsam Verantwortliche bemüht sich nach besten Kräften, diese Informationen zur Verfügung zu stellen.

Artikel 16

Aufgaben der Kommission als Auftragsverarbeiterin

Die Kommission hat in ihrer Eigenschaft als Auftragsverarbeiterin die nachstehend aufgeführten Aufgaben. Die Kommission kann Dritte als Unterauftragsverarbeiter mit der Wahrnehmung dieser Aufgaben beauftragen.

a) Sie richtet einen sicheren und zuverlässigen Kommunikationsdienst für die an MyHealth@EU teilnehmenden nationalen Kontaktstellen für digitale Gesundheit (im Folgenden „zentraler sicherer Kommunikationsdienst“) ein und pflegt diesen.

b) Sie konfiguriert den zentralen sicheren Kommunikationsdienst so, dass die nationalen Kontaktstellen für digitale Gesundheit sicher, zuverlässig und effizient Informationen austauschen können.

c) Sie ergreift Maßnahmen zur Erleichterung der Interoperabilität und der Kommunikation zwischen dem zentralen sicheren Kommunikationsdienst und den gemeinsam Verantwortlichen von MyHealth@EU.

d) Sie verarbeitet personenbezogene Daten nur auf Weisung der gemeinsam Verantwortlichen von MyHealth@EU, es sei denn, sie ist rechtlich dazu verpflichtet. In diesem Fall teilt die Kommission dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das besagte Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Kommission unterrichtet unverzüglich die gemeinsam Verantwortlichen, wenn erteilte Weisungen ihrer Ansicht nach gegen geltende Datenschutzbestimmungen verstoßen.

e) Sie ergreift die erforderlichen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau für die im sicheren Kommunikationsdienst verarbeiteten personenbezogenen Daten zu gewährleisten. Diese Maßnahmen werden in einem Sicherheitsplan festgehalten, der stets auf dem neuesten Stand zu halten ist. Die Maßnahmen umfassen Folgendes:

i) Einführung eines Verfahrens zur Risikobewertung, um potenzielle Bedrohungen des Systems zu ermitteln und abzuschätzen;

ii) Gewährleistung, dass die zur Verarbeitung personenbezogener Daten befugten Personen einer angemessenen gesetzlichen Geheimhaltungspflicht, wie sie in Artikel 17 des Statuts der Beamten der Europäischen Gemeinschaften gemäß der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates [9] festgelegt ist, unterliegen oder sich zur Vertraulichkeit verpflichtet haben;

iii) Ergreifung geeigneter Maßnahmen, mit denen sichergestellt wird, dass ihr Personal und ihre Auftragnehmer ihre Verantwortlichkeiten im Hinblick auf die Informationssicherheit und den Schutz nicht als Verschlusssache eingestufter vertraulicher Informationen verstehen;

iv) Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen, um unbefugten Zugriff auf personenbezogene Daten zu verhindern;

[9] Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates vom 29. Februar 1968 zur Festlegung des Statuts der Beamten der Europäischen Gemeinschaften und der Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften sowie zur Einführung von Sondermaßnahmen, die vorübergehend auf die Beamten der Kommission anwendbar sind (ABl. L 56 vom 4.3.1968, S. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj).

v) Gewährleistung der Integrität der über den sicheren Kommunikationsdienst übermittelten Informationen;

vi) erforderlichenfalls Ergreifung von Maßnahmen, mit denen der unbefugte Zugang zum sicheren Kommunikationsdienst von der Domain der nationalen Kontaktstellen für digitale Gesundheit aus verhindert wird;

vii) Gewährleistung, dass die innerhalb des zentralen sicheren Kommunikationsdienstes übermittelten Daten verschlüsselt sind;

viii) Ergreifung geeigneter physischer Sicherheitsmaßnahmen, darunter

1. Kontrolle des Zugangs zu den Einrichtungen und Führen eines Besucherregisters für Rückverfolgungszwecke;

2. Gewährleistung, dass externe Personen, denen Zugang zu Räumlichkeiten gewährt wird, von entsprechend befugten Mitarbeitern begleitet werden.

f) Sie führt ein Verfahren für das Änderungsmanagement ein und hält die gemeinsam Verantwortlichen über alle Änderungen auf dem Laufenden, die sich auf die Kommunikation mit anderen nationalen Infrastrukturen oder die Sicherheit dieser Infrastrukturen auswirken können.

g) Sie überwacht in Echtzeit die Leistung aller Komponenten ihres Zentralen Sicheren Kommunikationsdienstes, erstellt regelmäßige Statistiken und führt Aufzeichnungen.

h) Sie führt Audit- und Überprüfungsverfahren ein, um

i) die Übereinstimmung der umgesetzten Sicherheitsmaßnahmen mit dem Sicherheitsplan gemäß Buchstabe e zu überprüfen;

ii) die Integrität der Systemdateien, der Sicherheitsparameter und der erteilten Genehmigungen regelmäßig zu kontrollieren;

iii) durch Überwachung Sicherheitsverstöße aufzudecken;

iv) Änderungen zur Behebung bestehender Schwachstellen bei der Sicherheit umzusetzen;

v) ein Verfahren für den Umgang mit Sicherheitsvorfällen aufzustellen, in dem das Melde- und Eskalationsprogramm festgelegt ist;

vi) die betroffenen gemeinsam Verantwortlichen zu benachrichtigen.

i) Sie veröffentlicht auf ihrer Website Informationen für die Patienten über die Verarbeitung personenbezogener Daten auf MyHealth@EU, nachdem die gemeinsam Verantwortlichen dem Inhalt zugestimmt haben.

j) Sie unterstützt die gemeinsam Verantwortlichen, indem sie ihnen Informationen über den sicheren Kommunikationsdienst von MyHealth@EU liefert, um den Verpflichtungen gemäß den Artikeln 32 bis 36 der Verordnung (EU) 2016/679 nachzukommen.

k) Sie löscht nach Beendigung des Datenaustauschs alle im Namen eines Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass sie dies getan hat, es sei denn, die Speicherung der personenbezogenen Daten ist rechtlich vorgeschrieben.

l) Sie liefert den gemeinsam Verantwortlichen alle erforderlichen Informationen für den Nachweis der Einhaltung ihrer Verpflichtungen als Auftragsverarbeiterin, lässt — auch auf Anfrage von Verantwortlichen — die Durchführung unabhängiger Prüfungen einschließlich Inspektionen sowie Überprüfungen von Sicherheitsmaßnahmen unter Bedingungen zu, die dem Protokoll (Nr. 7) zum Vertrag über die Arbeitsweise der Europäischen Union betreffend die Vorrechte und Befreiungen der Europäischen Union genügen, und trägt zu diesen Prüfungen bei.

Artikel 17

Sicherheit von MyHealth@EU

Die Kommission gewährleistet die Sicherheit von MyHealth@EU gemäß dem Beschluss (EU, Euratom) 2017/46 der Kommission.

KAPITEL 4

ÜBERGANGSMAßNAHMEN

Artikel 18

Übergangsmaßnahmen

Nationale Kontaktstellen für elektronische Gesundheitsdienste, die vor dem 26. März 2029 personenbezogene elektronische Gesundheitsdaten über die digitale eHealth-Diensteinfrastruktur für grenzüberschreitende elektronische Gesundheitsinformationsdienste gemäß dem Durchführungsbeschluss 2019/1765 ausgetauscht haben und die gemäß Artikel 23 Absatz 2 der Verordnung (EU) 2025/327 als nationale Kontaktstellen für digitale Gesundheit benannt wurden, können diese Daten weiterhin im Rahmen von MyHealth@EU austauschen, und es wird davon ausgegangen, dass sie die in der vorliegenden Verordnung festgelegten Genehmigungsanforderungen für die Aufnahme des Austauschs personenbezogener elektronischer Gesundheitsdaten erfüllen.

KAPITEL 5

SCHLUSSBESTIMMUNGEN

Artikel 19

Inkrafttreten und Geltungsbeginn

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

Sie gilt ab dem 26. März 2027.

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

Brüssel, den 18. September 2026

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN