1 von 53

BG. 111

Gesamtändernder Abänderungsantrag

der Abgeordneten Rudolf Silvan, Mag. Dr. Juliane Bogner-Strauß, Fiona Fiedler, BEd,

Kolleginnen und Kollegen

zum Antrag der Abgeordneten Rudolf Silvan, Mag. Dr. Juliane Bogner-Strauß, Fiona Fiedler, BEd, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem das Gesundheitstelematikgesetz 2012 und das Allgemeine Sozialversicherungsgesetz geändert werden (413/A):

Der Gesundheitsausschuss wolle beschließen:

„Bundesgesetz, mit dem das Gesundheitstelematikgesetz 2012 und das Allgemeine Sozialversicherungsgesetz geändert werden

Der Nationalrat hat beschlossen:

Artikel 1
Änderung des Gesundheitstelematikgesetzes 2012

Das Gesundheitstelematikgesetz 2012, BGBl. I Nr. 111/2012, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 105/2024, mit dem das Gesundheitstelematikgesetz 2012, das Allgemeine Sozialversicherungsgesetz, das Epidemiegesetz 1950, das Patientenverfügungs-Gesetz und das Suchtmittelgesetz geändert werden, wird wie folgt geändert:

1. Im Inhaltsverzeichnis entfällt der Eintrag zu § 12.

2. Im Inhaltsverzeichnis wird im Eintrag zum 6. Abschnitt die Bezeichnung „6. Abschnitt" durch die Bezeichnung „7. Abschnitt" ersetzt, *nach § 24h werden folgende Einträge eingefügt:*

„6. Abschnitt: Grenzüberschreitende Gesundheitsversorgung

1. Unterabschnitt
Allgemeine Bestimmungen zu MyHealth@EU

24i	Allgemeine Bestimmungen zur grenzüberschreitenden Gesundheitsversorgung
24j	Nationale Kontaktstelle für digitale Gesundheit
24k	Grundsätze der Datenverarbeitung
24l	Überprüfung der Identität von natürlichen Personen im grenzüberschreitenden Kontext
24m	Überprüfung der Identität von Gesundheitsdiensteanbietern im grenzüberschreitenden Kontext
24n	Rechte natürlicher Personen

2. Unterabschnitt
Elektronische Verschreibungen und elektronische Abgaben (EU-Rezept)

24o	Allgemeine Bestimmungen zum EU-Rezept
24p	Österreich als Herkunftsmitgliedstaat
24q	Österreich als Behandlungsmitgliedstaat
24r	Grundsätze der Datenverarbeitung

3. Unterabschnitt

EU-Patientenkurzakte

24s	Allgemeine Bestimmungen zur EU-Patientenkurzakte
24t	Österreich als Behandlungsmitgliedstaat
24u	Grundsätze der Datenverarbeitung"

3. Im Inhaltsverzeichnis lautet der Eintrag zu § 28c:

„28c Verordnungsermächtigungen für den 6. Abschnitt"

4. Im Inhaltsverzeichnis wird nach dem Eintrag zu § 28c folgender Eintrag eingefügt:

„28d Anhörung und Weisungsrechte"

5. In § 1 Abs. 2 wird im Schlussteil der Z 3 das Wort „sowie“ *durch einen Beistrich ersetzt, am Ende der Z 4 das Wort* „sowie“ *angefügt und die folgende Z 5 angefügt:*

„5. einheitliche Regelungen für die ungerichtete Kommunikation elektronischer Gesundheitsdaten und genetischer Daten im Rahmen von spezifischen Anwendungen der grenzüberschreitenden Gesundheitsversorgung zu schaffen (6. Abschnitt).“

6. In § 2 Z 2 wird im Einleitungsteil nach dem Wort „Verordnung“ *die Wort- und Zeichenfolge* „ , oder in einem anderen Behandlungsmitgliedstaat gemäß Z 22a,“ *und am Ende der lit. e das Wort* „oder“ *eingefügt und die folgende lit. f angefügt:*

„f) Unterstützung der grenzüberschreitenden Gesundheitsversorgung.“

7. In § 2 Z 9 wird am Ende der lit. e der Beistrich durch das Wort „sowie“ *ersetzt und lit. f entfällt.*

7a. § 2 Z 10 lit. e lautet:

„e) Einrichtungen der Pflege, deren Betrieb einer Melde-, Anzeige- oder Bewilligungspflicht nach bundes- oder landesgesetzlichen Vorschriften unterliegt oder von einem Bundesland finanziert wird sowie der behördlichen Aufsicht, Kontrolle oder einem faktisch gleichzusetzenden Einfluss unterliegt, wobei Einrichtungen für Menschen mit Behinderungen nicht umfasst sind,“

8. Dem § 2 werden folgende Z 20 bis 28 angefügt:

„20. „MyHealth@EU-Mitgliedstaat“: ein Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums, der an MyHealth@EU teilnimmt.

21. „Herkunftsmitgliedstaat“: ein MyHealth@EU-Mitgliedstaat, in dem natürliche Personen ihren Wohnsitz haben oder sozialversichert sind.

22. „Gesundheitsversorgung“: Gesundheitsversorgung gemäß Art. 3 lit. a der Patientenmobilitätsrichtlinie.

22a. „Behandlungsmitgliedstaat“: Behandlungsmitgliedstaat gemäß Art. 3 lit. d Patientenmobilitätsrichtlinie.

22b. „grenzüberschreitende Gesundheitsversorgung“: grenzüberschreitende Gesundheitsversorgung gemäß Art. 3 lit. e der Patientenmobilitätsrichtlinie.

23. „MyHealth@EU“: die grenzüberschreitende Infrastruktur zur Verarbeitung von in den Anwendungen der grenzüberschreitenden Gesundheitsversorgung gemäß dem 6. Abschnitt definierten Daten im Falle Österreichs als Herkunftsmitgliedstaat gemäß Z 21 sowie Daten aus anderen Mitgliedstaaten im Falle Österreichs als Behandlungsmitgliedstaat gemäß Z 22a für Zwecke der grenzüberschreitenden Gesundheitsversorgung.

24. „Nationale Kontaktstelle für digitale Gesundheit“: ein organisatorisches und technisches Zugangstor zur Verarbeitung von in den Anwendungen der grenzüberschreitenden Gesundheitsversorgung gemäß dem 6. Abschnitt definierten Daten im Falle Österreichs als Herkunftsmitgliedstaat gemäß Z 21 sowie Daten aus anderen Mitgliedstaaten im Falle Österreichs als Behandlungsmitgliedstaat gemäß Z 22a für Zwecke der grenzüberschreitenden Gesundheitsversorgung.

25. „Elektronische Verschreibung“: Verschreibung für ein Arzneimittel im Sinne von Art. 3 lit. k der Patientenmobilitätsrichtlinie.

26. „Elektronische Abgabe“: Informationen über die Abgabe eines Arzneimittels an eine natürliche Person durch eine Apotheke auf der Grundlage einer elektronischen Verschreibung.

27. „EU-Rezept“: grenzüberschreitende Gesundheitsanwendung, die sowohl in Österreich ausgestellte, elektronische Verschreibungen, die in Apotheken anderer MyHealth@EU-Mitgliedstaaten eingelöst werden (Österreich als Herkunftsmitgliedstaat), als auch in anderen MyHealth@EU-Mitgliedstaaten ausgestellte, elektronische Verschreibungen für natürliche Personen des jeweiligen MyHealth@EU-Mitgliedstaats, die in österreichischen Apotheken gemäß § 1 des Apothekengesetzes (im Folgenden Apotheken) eingelöst werden (Österreich als Behandlungsmitgliedstaat) umfasst.

28. „EU-Patientenkurzakte“: grenzüberschreitende Gesundheitsanwendung, die wichtige klinische Fakten in Bezug auf eine bestimmte natürliche Person enthält und für eine sichere und effiziente Gesundheitsversorgung dieser Person unerlässlich ist, ausschließlich im Falle Österreichs als Behandlungsmitgliedstaat.“

9. § 12 entfällt samt Überschrift.

10. In § 12a Abs. 2 wird am Ende der Z 3 das Wort „sowie“ *durch einen Beistrich ersetzt und wird die Z 4a angefügt:*

„4a. Anwendungen der grenzüberschreitenden Gesundheitsversorgung (6. Abschnitt) sowie“

11. In § 12b Abs. 1 wird am Ende der Z 3 das Wort „sowie“ *durch einen Beistrich ersetzt und am Ende der Z 4 das Wort* „sowie“ *angefügt und folgende Z 5 angefügt:*

„5. im Rahmen der grenzüberschreitenden Gesundheitsversorgung (6. Abschnitt)“

11a. In § 12b Abs. 1 wird im Schlussteil das Wort „erfassen“ *durch das Wort* „verarbeiten“ *ersetzt.*

11b. In § 13 Abs. 3 wird im Einleitungsteil nach der Wortfolge „genannten Ziele sind“ *die Wort- und Zeichenfolge* „ – mit Ausnahme von Pflegesituationsberichten (Z 6) –“ *eingefügt.*

11c. In § 13 Abs. 3 Z 4 wird nach der Wort- und Zeichenfolge „Angehörige des ärztlichen Berufes (§ 2 Z 10 lit. a)“ *die Wort-und Zeichenfolge* „sowie durch Krankenanstalten gemäß § 2 Z 10 lit. d und Einrichtungen der Pflege gemäß § 2 Z 10 lit. e“ *eingefügt.*

11d. § 13 Abs. 3 Z 6 lautet:

„6. Pflegesituationsberichte (§ 2 Z 9 lit. a sublit. dd) durch Einrichtungen der Pflege (§ 2 Z 10 lit. e), wobei diese ab 1. Jänner 2027 verpflichtend in ELGA zu speichern sind,“

12. In § 18 Abs. 1 Z 1 wird nach der Wortfolge „eHealth-Anwendungen“ *die Wortfolge* „und Anwendungen der grenzüberschreitenden Gesundheitsversorgung gemäß dem 6. Abschnitt“ *eingefügt.*

13. In § 18 Abs. 4a wird die Wort- und Zeichenfolge „gemäß dem 5. Abschnitt“ *durch die Wort- und Zeichenfolge* „und Anwendungen der grenzüberschreitenden Gesundheitsversorgung gemäß dem 6. Abschnitt“ *ersetzt.*

14. In § 18 Abs. 4a Z 2 wird die Wortfolge „einem gültigen österreichischen Reisedokument gemäß § 2 des Passgesetzes 1992, BGBl. Nr. 839/1992,“, *durch die Wortfolge* „einem gültigen Reisepass im Sinne des Passgesetzes 1992, BGBl. Nr. 839/1992, ausgenommen eines Reisepasses gemäß § 4a des Passgesetzes 1992“ *ersetzt.*

14a In § 18 Abs. 4a Z 2 wird die Wortfolge „eines gültigen Personalausweises“ *durch die Wortfolge* „einem gültigen Personalausweis“ *ersetzt.*

15. In § 18 Abs. 4b Z 1 wird das Wort „Passersätze“ *durch die Wortfolge* „Übernahmserklärungen für Staatsbürger“ *ersetzt.*

16. In § 18 Abs. 4b Z 4 wird die Wortfolge „Reisedokuments gemäß § 2 Passgesetz“ *durch die Wortfolge* „Reisepasses im Sinne des Passgesetzes 1992, ausgenommen eines Reisepasses gemäß § 4a des Passgesetzes 1992“ *ersetzt.*

17. In § 21 Abs. 1 wird nach der Wortfolge „eHealth-Anwendungen“ *die Wortfolge* „und Anwendungen der grenzüberschreitenden Gesundheitsversorgung gemäß dem 6. Abschnitt“ *eingefügt.*

18. In § 21 Abs. 4 wird die Wortfolge „gemäß dem 5. Abschnitt“ *durch die Wortfolge* „und Anwendungen der grenzüberschreitenden Gesundheitsversorgung gemäß dem 6. Abschnitt“ *ersetzt.*

19. In § 22 Abs. 1 wird die Wortfolge „gemäß den Bestimmungen des 5. Abschnitts“ *durch die Wortfolge* „und in Anwendungen der grenzüberschreitenden Gesundheitsversorgung gemäß dem 6. Abschnitt“ *ersetzt.*

20. § 23 Abs. 1 wird am Ende der Z 1 das Wort „und“ *durch einen Beistrich ersetzt, in Z 2 wird die Wortfolge* „nach Maßgabe des 5. Abschnitts“ *durch ein* „und“ *ersetzt und folgende Z 3 angefügt:*

„3. Anwendungen der grenzüberschreitenden Gesundheitsversorgung gemäß dem 6. Abschnitt“

21. Der bisherige 6. Abschnitt erhält die Abschnittsbezeichnung „7" und es wird nach § 24h folgender neuer 6. Abschnitt eingefügt:

„6. Abschnitt:
Grenzüberschreitende Gesundheitsversorgung

1. Unterabschnitt
Allgemeine Bestimmungen zu MyHealth@EU

Allgemeine Bestimmungen zur grenzüberschreitenden Gesundheitsversorgung

§ 24i. (1) Die grenzüberschreitende Gesundheitsversorgung über MyHealth@EU ist für Zwecke der Gesundheitsvorsorge sowie aus Gründen des öffentlichen Interesses im Bereich öffentliche Gesundheit erforderlich gemäß Art. 9 Abs. 2 lit. h und i DSGVO.

(2) Die Teilnahme an MyHealth@EU ist für in Österreich wohnhafte oder sozialversicherte natürliche Personen freiwillig und unentgeltlich. Sie setzt das erklärte Einverständnis der Teilnehmenden (Opt-In) voraus, welches jederzeit zurückgezogen werden kann. Das Einverständnis (Opt-in) stellt keine Einwilligung iSd Art. 9 Abs. 2 lit. a DSGVO dar und erfüllt daher keine dementsprechende Rechtswirkung.

(3) Sozialversicherungsrechtliche Vorschriften bleiben von diesem Abschnitt unberührt.

Nationale Kontaktstelle für digitale Gesundheit

§ 24j. (1) Zur Sicherstellung der in § 24i genannten Ziele ist von dem für das Gesundheitswesen zuständigen Bundesminister oder der zuständigen Bundesministerin als datenschutzrechtlich Verantwortlichem oder Verantwortlicher (Art. 4 Z 7 DSGVO) die Nationale Kontaktstelle für digitale Gesundheit einzurichten und zu betreiben. Sie ist Teil der öffentlichen Gesundheitstelematik-Infrastruktur gemäß § 3 Z 15 Gesundheits-Zielsteuerungsgesetz (G-ZG), BGBl. I Nr. 26/2017.

(2) Aufgaben der Nationalen Kontaktstelle sind die Kommunikation mit den ELGA-Komponenten gemäß § 24k Abs. 3 sowie anwendungsbezogenen Komponenten gemäß den folgenden Unterabschnitten und die Kommunikation mit den Kontaktstellen anderer MyHealth@EU-Mitgliedstaaten.

(3) Die von der Nationalen Kontaktstelle gespeicherten Protokolldaten haben neben nicht-personenbezogenen Meta-Daten auch Angaben zum Patienten oder zur Patientin (MyHealth@EU-ID gemäß § 24l Abs. 2) sowie zur Identität des Gesundheitsdiensteanbieters (§ 24m) zu enthalten und sind zur Nachvollziehbarkeit der Rechtmäßigkeit von Zugriffen spätestens 10 Jahre nach Abschluss der jeweiligen, ursprünglichen Verarbeitung für die Zwecke der Anwendungen der folgenden Unterabschnitte zu löschen.

Grundsätze der Datenverarbeitung

§ 24k. (1) Die Verarbeitung (Art. 4 Z 2 DSGVO) von personenbezogenen Daten gemäß folgenden Unterabschnitten ist nur zulässig, wenn

1. im Falle Österreichs als Herkunftsmitgliedstaat die in Österreich wohnhafte oder sozialversicherte natürliche Person ihr Einverständnis (Opt-In) zur Datenverarbeitung gemäß § 24i Abs. 2 erklärt hat,
2. die natürliche Person gemäß § 24l eindeutig identifiziert wurde,
3. dem für das Gesundheitswesen zuständigen Bundesminister oder der zuständigen Bundesministerin als Nationale Kontaktstelle oder als ELGA- und eHealth-Supporteinrichtung gemäß § 24m eindeutig identifiziert wurde und gemäß Abs. 2 zur Verarbeitung der Daten berechtigt ist sowie
4. die gemäß den folgenden Unterabschnitten beteiligten Gesundheitsdiensteanbieter gemäß § 24m eindeutig identifiziert wurden und gemäß dem jeweiligen Unterabschnitt zur Verarbeitung der Daten berechtigt sind.

(2) Die durch MyHealth@EU verfügbar gemachten Daten dürfen ausschließlich

1. für Zwecke der grenzüberschreitenden Gesundheitsversorgung von
   a) dem für das Gesundheitswesen zuständigen Bundesminister oder der zuständigen Bundesministerin als Nationalen Kontaktstelle,
   b) Gesundheitsdiensteanbietern, die eine natürliche Person anderer MyHealth@EU-Mitgliedstaaten in Österreich gemäß den folgenden Unterabschnitten behandeln oder betreuen sowie

2. zum Zwecke der Wahrnehmung der Rechte der natürlichen Person gemäß § 24n Abs. 1 von
   a) der natürlichen Person selbst,
   b) gesetzlichen oder bevollmächtigten Vertreter/inne/n der natürlichen Person,
   c) der ELGA- und eHealth-Supporteinrichtung sowie
   d) der Nationalen Kontaktstelle

verarbeitet werden.

(3) Für die Zwecke des Abs. 2 dürfen die folgenden ELGA-Komponenten verwendet werden:

1. der Patient/inn/enindex gemäß § 18,
2. der Gesundheitsdiensteanbieterindex gemäß § 19,
3. das Berechtigungssystem gemäß § 21,
4. das Protokollierungssystem gemäß § 22 sowie
5. das Zugangsportal gemäß § 23.

Überprüfung der Identität von natürlichen Personen im grenzüberschreitenden Kontext

§ 24l. (1) Im Falle Österreichs als Herkunftsmitgliedstaat hat der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin eine E-ID taugliche Anwendung gemäß den §§ 4 ff E-GovG bereitzustellen, die es natürlichen Personen ermöglicht, sich auf Basis der Verwendung der Funktion E-ID im jeweiligen Behandlungsmitgliedstaat zu identifizieren. Nach erfolgter eindeutiger Identifikation der natürlichen Person unter Verwendung der Funktion E-ID hat der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin ein eindeutiges Identifizierungsmerkmal zu erstellen und so anzuzeigen, dass der behandelnde Gesundheitsdiensteanbieter eine Überprüfung dieser Daten vornehmen kann. § 18 Abs. 4a Z 2 bleibt hiervon unberührt.

(2) Zum Zwecke der Überprüfung der Identität von natürlichen Personen sowie der eindeutigen Zuordnung von Dokumenten ist der für das Gesundheitswesen zuständige Bundesminister oder die für das Gesundheitswesen zuständige Bundesministerin ermächtigt, das bereichsspezifische Personenkennzeichen Gesundheit (bPK-GH) für die Zwecke dieses Abschnitts zu verwenden, und auf den Patient/inn/enindex gemäß § 18 zuzugreifen. Zur Übermittlung personenbezogener Daten an die Nationale Kontaktstelle eines MyHealth@EU-Mitgliedstaats hat der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin das bPK-GH durch eine als „MyHealth@EU-ID" zu bezeichnende, kryptographische Ableitung zu ersetzen. Eine Zuordnung der MyHealth@EU-ID zu einem bPK-GH darf ausschließlich für die Zwecke dieses Abschnitts erfolgen. Die bPK-GH darf nicht an die Nationale Kontaktstelle eines anderen MyHealth@EU-Mitgliedstaats übermittelt werden, sondern lediglich die MyHealth@EU-ID.

(3) Natürliche Personen anderer MyHealth@EU-Mitgliedstaaten sind von österreichischen Gesundheitsdiensteanbietern mittels der vom jeweiligen Herkunftsmitgliedstaat vorgegebenen Identifikationsmittel eindeutig zu identifizieren. Zu diesem Zweck dürfen Gesundheitsdiensteanbieter insbesondere die folgenden Daten der natürlichen Personen verarbeiten:

1. Angaben zur Person (akademische Titel, Vor- und Nachname(n), Geburtsdatum, Geschlecht)
2. Angaben zum Wohnort (Wohnsitzstaat, Adresse)
3. Angaben zum Identitätsnachweis (Reisepass- und Personalausweis-Nummern, Sozialversicherungsnummer, sonstige numerische oder alphanumerische Identifikatoren)

Überprüfung der Identität von Gesundheitsdiensteanbietern im grenzüberschreitenden Kontext

§ 24m. Nachweis und Prüfung der eindeutigen Identität von Gesundheitsdiensteanbietern in Österreich haben

1. gemäß § 4 Abs. 4 und
2. für die Zwecke des § 2 Z 2 lit. a bis d mittels Zwei-Faktor-Authentifizierung der jeweils zugreifenden, natürlichen Person

zu erfolgen.

Rechte der natürlichen Personen

§ 24n. (1) In Österreich wohnhafte oder sozialversicherte natürliche Personen sowie deren gesetzliche oder bevollmächtigte Vertreter/innen haben das Recht, elektronisch durch einen Zugang über das Zugangsportal (§ 23) oder direkt gegenüber dem für das Gesundheitswesen zuständigen Bundesminister oder der zuständigen Bundesministerin als ELGA- und eHealth-Supporteinrichtung (§ 17) die folgenden Rechte geltend zu machen:

1. Wahrnehmung der Betroffenenrechte gemäß dem Kapitel III der DSGVO,
2. Abgabe oder Zurückziehung des Einverständnisses zur Teilnahme (Opt-in) gemäß § 24i Abs. 2.

(2) Die für die Wahrnehmung der Rechte erforderliche Entscheidungsfähigkeit (§ 24 Abs. 2 ABGB) wird im Zweifel ab Vollendung des 14. Lebensjahres (mündige Minderjährige) vermutet.

(3) Natürliche Personen anderer MyHealth@EU-Mitgliedstaaten haben das Recht, ihre Betroffenenrechte gemäß Abs. 1 Z 1 auch gegenüber den in Abs. 1 angeführten Stellen auszuüben. Falls kein Verantwortlicher iSd Art. 4 Z 7 DSGVO seinen Sitz in Österreich hat, ist die Anfrage an die zuständige Nationale Kontaktstelle für digitale Gesundheit weiterzuleiten.

2. Unterabschnitt
Elektronische Verschreibungen und elektronische Abgaben (EU-Rezept)

Allgemeine Bestimmungen zum EU-Rezept

§ 24o. (1) Der Dachverband der Sozialversicherungsträger hat im übertragenen Wirkungsbereich (Artikel 120b Abs. 2 Bundes-Verfassungsgesetz, BGBl. I Nr. 1/1930 in der jeweils geltenden Fassung) des für das Gesundheitswesen zuständigen Bundesministers oder der zuständigen Bundesministerin das EU-Rezept gemäß § 2 Abs. 2 Z 27 einzurichten und zu betreiben. Der Dachverband der Sozialversicherungsträger ist dabei an die Weisungen des für das Gesundheitswesen zuständigen Bundesministers oder der zuständigen Bundesministerin gebunden. Das EU-Rezept ist Teil der öffentlichen Gesundheitstelematik-Infrastruktur gemäß § 3 Z 15 G-ZG.

(2) Zum Zwecke der Erstellung des EU-Rezepts darf der Dachverband der Sozialversicherungsträger neben den ELGA-Komponenten gemäß § 24k Abs. 3 die Anwendung „e-Rezept" des elektronischen Verwaltungssystems des Dachverbands der Sozialversicherungsträger gemäß § 31a ASVG und die Verordnungsdaten des jeweiligen e-Rezeptes heranziehen. Sozialversicherungsrechtliche Vorschriften bleiben von diesem Abschnitt unberührt.

(3) Die Nationale Kontaktstelle hat ihre Aufgaben gemäß § 24j Abs. 3 für das EU-Rezept zu erfüllen.

Österreich als Herkunftsmitgliedstaat

§ 24p. Zum Zwecke der Abgabe von in Österreich elektronisch verschriebenen Arzneimitteln durch Gesundheitsdiensteanbieter in einem anderen MyHealth@EU-Mitgliedstaat hat der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin die Daten des EU-Rezepts gemäß § 24o Abs. 2 als Nationale Kontaktstelle gemäß § 24j auf Anfrage an die Nationale Kontaktstelle im jeweiligen Behandlungsmitgliedstaat zu übermitteln. Zu diesem Zwecke ist den Gesundheitsdiensteanbietern der anderen MyHealth@EU-Mitgliedstaaten die Überprüfung der Identität der natürlichen Person gemäß § 24l zu ermöglichen.

Österreich als Behandlungsmitgliedstaat

§ 24q. (1) Apotheken dürfen auf elektronische Verschreibungen, die ihnen aus anderen MyHealth@EU-Mitgliedstaaten über MyHealth@EU von der Nationalen Kontaktstelle gemäß § 24j übermittelt werden, zugreifen und derart verschriebene Arzneimittel, unter Wahrung der berufsrechtlichen Bestimmungen des Apothekengesetzes, abgeben. Geben Apotheken Arzneimittel auf der Grundlage einer solchen Verschreibung ab, so haben sie die Abgabe dem MyHealth@EU-Mitgliedstaat, der die Verschreibung ausgestellt hat, über MyHealth@EU an die Nationale Kontaktstelle zu melden (elektronische Abgabe).

(2) Die Erfüllung der in § 24m genannten Voraussetzungen in Apotheken hat mittels geeigneter elektronischer Identifikation (z. B. mittels Identifikationskarten) der dort beschäftigten natürlichen Personen zu erfolgen.

Grundsätze der Datenverarbeitung

§ 24r. (1) Die Verarbeitung (Art. 4 Z 2 DSGVO) von über das EU-Rezept verfügbar gemachten Daten gemäß § 24p sowie über MyHealth@EU verfügbar gemachten Daten gemäß § 24q ist nur zulässig, wenn die Grundsätze gemäß § 24k eingehalten werden.

(2) Gemeinsame Verantwortliche des EU-Rezepts im Sinne des Art. 4 Z 7 in Verbindung mit Art. 26 DSGVO sind:

1. im Falle Österreichs als Herkunftsmitgliedstaat:
   a) der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin als Nationale Kontaktstelle und

b) der jeweils behandelnde Arzt oder die jeweils behandelnde Ärztin,

2. im Falle Österreichs als Behandlungsmitgliedstaat
   a) der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin als Nationale Kontaktstelle sowie
   b) die jeweils abgebende Apotheke,

wobei die Festlegung der datenschutzrechtlichen Pflichten im Sinne des Art. 26 DSGVO durch Verordnung des für das Gesundheitswesen zuständigen Bundesministers oder der zuständigen Bundesministerin zu erfolgen hat.

3. Unterabschnitt
EU-Patientenkurzakte

Allgemeine Bestimmungen zur EU-Patientenkurzakte

§ 24s. (1) Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin hat eine grenzüberschreitende Anwendung zum Abruf der EU-Patientenkurzakte gemäß § 2 Abs. 2 Z 28 einzurichten und zu betreiben. Die grenzüberschreitende Anwendung zum Abruf der EU-Patientenkurzakte ist Teil der öffentlichen Gesundheitstelematik-Infrastruktur gemäß § 3 Z 15 G-ZG.

(2) Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin als Nationale Kontaktstelle hat seine/ihre Aufgaben gemäß § 24j Abs. 3 für den Abruf der EU-Patientenkurzakte zu erfüllen.

(3) Im Rahmen der EU-Patientenkurzakte dürfen (sofern vorhanden und zutreffend) die folgenden Datenarten verarbeitet werden:

1. Angaben zur natürlichen Person (inklusive Identitätsdaten, Kontaktdaten, Angaben zur Versicherung),
2. Allergien,
3. Medizinische Warnungen,
4. Informationen über Impfungen/Prophylaxen, gegebenenfalls in Form eines Impfausweises,
5. Medizinische Probleme (aktuelle, gelöste, abgeschlossene oder inaktive Probleme, auch in einer internationalen Kodierung zur Klassifizierung),
6. Informationen in Textform zur medizinischen Vorgeschichte,
7. Medizinprodukte und Implantate,
8. Medizinische Verfahren oder Pflegeverfahren,
9. Funktionszustand,
10. Derzeitige und frühere Medikation,
11. Gesundheitsrelevante Beobachtungen zum sozialen Hintergrund (Konsum von Alkohol, Tabak, etc.),
12. Schwangerschaftshistorie,
13. von der natürlichen Person selbst zur Verfügung gestellte Daten,
14. Beobachteter Gesundheitszustand,
15. der aktuelle Versorgungsplan,
16. Angaben zu seltenen Krankheiten (zum Beispiel Einzelheiten über die Auswirkungen oder Merkmale der Krankheit, etc.) und
17. Ergebnisse von Untersuchungen.

Österreich als Behandlungsmitgliedstaat

§ 24t. (1) Gesundheitsdiensteanbieter im Sinne des 3. Unterabschnitts (im Folgenden „Gesundheitsdiensteanbieter") sind ELGA-Gesundheitsdiensteanbieter im Sinne des § 2 Z 10 lit. a.

(2) Gesundheitsdiensteanbieter dürfen auf die EU-Patientenkurzakte, die ihnen aus anderen MyHealth@EU-Mitgliedstaaten mittels der grenzüberschreitenden Anwendung gemäß § 24s Abs. 1 über MyHealth@EU von dem für das Gesundheitswesen zuständigen Bundesminister oder der zuständigen Bundesministerin als Nationalen Kontaktstelle gemäß § 24j übermittelt wird, zugreifen.

(3) Die Identifikation des Gesundheitsdiensteanbieters als natürliche Person oder der von ihm beschäftigten natürlichen Personen hat gemäß § 24m zu erfolgen.

Grundsätze der Datenverarbeitung

§ 24u. (1) Die Verarbeitung (Art. 4 Z 2 DSGVO) von über MyHealth@EU verfügbar gemachten Daten gemäß § 24t ist nur zulässig, wenn die Grundsätze gemäß § 24k eingehalten werden.

(2) Gemeinsame Verantwortliche der EU-Patientenkurzakte im Sinne des Art. 4 Z 7 in Verbindung mit Art. 26 DSGVO sind:

1. im Falle Österreichs als Behandlungsmitgliedstaat
   a) der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin als Nationale Kontaktstelle sowie
   b) der Gesundheitsdiensteanbieter,

wobei die Festlegung der datenschutzrechtlichen Pflichten im Sinne des Art. 26 DSGVO durch Verordnung des für das Gesundheitswesen zuständigen Bundesministers oder der zuständigen Bundesministerin zu erfolgen hat."

22. Dem § 26 werden folgende Abs. 19 und 20 angefügt:

„(19) Die Einträge im Inhaltsverzeichnis zum 6. und 7. Abschnitt sowie zu § 28c und § 28d, § 1 Abs. 2 Z 3 bis 5, § 2 Z 2 Einleitungsteil sowie lit. e und f, § 2 Z 9 lit. e, § 2 Z 20 bis 28, § 12a Abs. 2 Z 3 und 4a, § 12b Abs. 1 Z 3 bis 5 sowie der Schlussteil, § 18 Abs. 1 Z 1, § 18 Abs. 4a Einleitungsteil sowie Z 2, Abs. 4b Z 1 und 4, § 21 Abs. 1 und 4, § 22 Abs. 1, § 23 Abs. 1 Z 1 bis 3, der 6. Abschnitt, die Abschnittsbezeichnung des 7. Abschnitts, § 28c und § 28d in der Fassung des Bundesgesetzes BGBl. Nr. I xxx/2025 treten mit 15. Februar 2026 in Kraft. § 2 Z 9 lit. f, § 12 samt Eintrag im Inhaltsverzeichnis und Überschrift treten mit 15. Februar 2026 außer Kraft.

(20) § 2 Z 10 lit. e, § 13 Abs. 3 (Einleitungsteil), § 13 Abs. 3 Z 6 und § 28a Abs. 1 Z 3 in der Fassung des Bundesgesetzes BGBl. Nr. I xxx/2025 treten mit dem der Kundmachung folgenden Tag in Kraft, § 13 Abs. 3 Z 4 in der Fassung des Bundesgesetzes BGBl. Nr. I xxx/2025 tritt mit 1. Jänner 2027 in Kraft."

22a. In § 28a Abs. 1 Z 3 entfällt nach der Wortfolge „speichern und zu erheben sind" *der Beistrich und es wird die Wort- und Zeichenfolge* „sowie den jeweiligen Zeitpunkt, ab dem die Nutzung der ELGA-Komponenten (§ 24) zur Verarbeitung von ELGA-Gesundheitsdaten technisch sichergestellt sein muss," *angefügt.*

23. § 28c erhält die Bezeichnung „**§ 28d.**".

24. Nach § 28b wird folgender § 28c (neu) samt Überschrift eingefügt:

„Verordnungsermächtigungen für den 6. Abschnitt

§ 28c. (1) Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin hat auf Grundlage des 6. Abschnittes mit Verordnung die datenschutzrechtlichen Pflichten im Sinne des Art. 26 DSGVO für die gemeinsamen Verantwortlichen des EU-Rezepts (§ 24r Abs. 2) festzulegen.

(2) Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin hat auf Grundlage des 6. Abschnittes mit Verordnung die datenschutzrechtlichen Pflichten im Sinne des Art. 26 DSGVO für die gemeinsamen Verantwortlichen der EU-Patientenkurzakte (§ 24u Abs. 2) festzulegen."

Artikel 2
Änderung des Allgemeinen Sozialversicherungsgesetzes

Das Allgemeine Sozialversicherungsgesetz, BGBl. I Nr. 189/1955, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 50/2025, wird wie folgt geändert:

1. In § 31a Abs. 4 wird der Punkt am Ende der Z 9 durch einen Strichpunkt ersetzt und folgende Z 10 angefügt:

„10. Erstellung von EU-Rezepten nach § 24o GTelG 2012."

2. In § 31d Abs. 3 Z 3 wird die Wortfolge „zum 31. Dezember 2025" *durch die Wortfolge* „längstens zum 31. Dezember 2026" *ersetzt.*

3. Nach § 812 wird folgender § 813 samt Überschrift eingefügt.

„Schlussbestimmungen zu Art. 2 des Bundesgesetzes BGBl. I Nr. xxx/202x

§ 813. (1) § 31a Abs. 4 Z 9 und Z 10 in der Fassung BGBl. I Nr. xxx/202x tritt am 31. Dezember 2025 in Kraft.

(2) § 31d Abs. 3 Z 3 in der Fassung BGBl. I Nr. xxx/202x tritt am auf die Kundmachung folgendem Tag in Kraft.““

Begründung:

Der gegenständliche Antrag gründet auf dem Ministerialentwurf 38/ME, der vom 29. Juli bis 9. September 2025 dem allgemeinen Begutachtungsverfahren unterzogen wurden.

Durch den gegenständlichen Antrag sollen im Gesundheitstelematikgesetz 2012 sozialversicherungsrechtlich relevante Bestimmungen zum „EU-Rezept" und zur EU-Patientenkurzakte verankert werden. Hintergrund dieser Bestimmungen ist – neben den Aspekten der Behandlungskontinuität und der Patient/innen-Sicherheit – die Fälschungssicherheit von in Österreich ausgestellten EU-Rezepten sowie der Abbau bürokratischer Hürden, womit auch der Prozess der Kostenerstattung von im Ausland eingelösten Verschreibungen erleichtert wird (Übersetzungen von Handelsnamen, Bestätigung der Abgabe, etc.). Ebenso betreffen die gegenständlichen Bestimmungen zu einem hohen Grad Pensionist/innen, die vielfach regelmäßig urlaubs- oder wohnortbedingt Verschreibungen im EU-Ausland einlösen müssen und insbesondere vom Übersetzungsservice innerhalb des Systems „MyHealth@EU" profitieren können. Hintergrund der EU-Patientenkurzakte ist die Erleichterung der Anamnese durch Gesundheitsdiensteanbieter bei der Behandlung von Patient:innen anderer Herkunftsstaaten, insbesondere hinsichtlich etwaigen Sprachbarrieren.

Am 5. März 2025 wurde die Verordnung über den europäischen Gesundheitsdatenraum (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; ABl. L, 2025/327) veröffentlicht (aufrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32025R0327).

Der Europäische Raum für Gesundheitsdaten ist einer der Eckpfeiler der europäischen Gesundheitsunion (siehe die Mitteilung der Kommission vom 11.11.2020 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Schaffung einer europäischen Gesundheitsunion: Die Resilienz der EU gegenüber grenzüberschreitenden Gesundheitsgefahren stärken, COM[2020] 724 final) und stellt den ersten gemeinsamen EU-Datenraum in einem spezifischen Bereich dar, der aus der EU-Datenstrategie hervorgeht (siehe dazu die Mitteilung der Kommission vom 19.2.2020 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, COM[2020] 66 final).

Der Europäische Raum für Gesundheitsdaten soll unter anderem Einzelpersonen dabei unterstützen, die Kontrolle über ihre eigenen Gesundheitsdaten zu bewahren, indem deren Handlungskompetenz durch einen besseren digitalen Zugang zu ihren personenbezogenen elektronischen Gesundheitsdaten sowie ihrer Kontrolle darüber sowohl im eigenen Land als auch auf EU-Ebene, und damit letztlich der freie Verkehr von Personen innerhalb der Union, unterstützt werden soll.

Dazu sieht die Verordnung ein Kapitel II zur Primärnutzung elektronischer Gesundheitsdaten vor, worunter die Verarbeitung personenbezogener elektronischer Gesundheitsdaten für die Erbringung von Gesundheitsdiensten zur Beurteilung, Erhaltung oder Wiederherstellung des Gesundheitszustands der natürlichen Person, auf die sich die Daten beziehen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten zu verstehen ist.

Zur Erreichung dieser grenzüberschreitenden Gesundheitsversorgung werden die Mitgliedstaaten insbesondere dazu verpflichtet, Nationale Kontaktstellen für digitale Gesundheit einzurichten und zu benennen, und diese an die bestehende unionsweite Infrastruktur zum grenzüberschreitenden Austausch elektronischer Gesundheitsdaten „MyHealth@EU" anzubinden.

Im Rahmen dessen sind einige Arten elektronischer Gesundheitsdaten als Priorität für die Integration in den Europäischen Raum für Gesundheitsdaten festgelegt worden, deren Implementierung für die Mitgliedstaaten in einem stufenweisen Prozess mit einer Übergangszeit ebenso verpflichtend ist.

Unter diese prioritären Datenkategorien grenzüberschreitender Services fallen mitunter elektronische Verschreibungen für Arzneimittel und deren elektronische Abgaben durch Apotheken ebenso wie die elektronische Patientenkurzakte. Mit dem „EU-Rezept" sollen sowohl in Österreich ausgestellte, elektronische Verschreibungen für in Österreich wohnhafte oder sozialversicherte Personen (siehe zur Definition im besonderen Teil zu Z 8) in Apotheken anderer Mitgliedstaaten eingelöst werden können (Österreich als Herkunftsmitgliedstaat), als auch in anderen Mitgliedstaaten ausgestellte, elektronische Verschreibungen für Personen des jeweiligen Mitgliedstaats in österreichischen öffentlichen Apotheken eingelöst werden können (Österreich als Behandlungsmitgliedstaat). Sozialversicherungsrechtliche Vorschriften bleiben davon gänzlich unberührt. Mit der EU-Patientenkurzakte sollen in einem ersten Schritt Patientenkurzakten von in anderen Mitgliedstaaten wohnhaften oder sozialversicherten Personen

im Rahmen einer Behandlung durch einen österreichischen Gesundheitsdiensteanbieter abgerufen werden können.

Diese Vorgaben des Europäischen Raums für Gesundheitsdaten für die Mitgliedstaaten werden erst mit Anwendbarkeit der Verordnung im März 2029 verpflichtend, dennoch sollen die Nationale Kontaktstelle für digitale Gesundheit als Infrastruktur sowie die Anwendungen EU-Rezept und EU-Patientenkurzakte in Österreich schon vorzeitig implementiert werden. Grund dafür ist eine nur noch jetzt mögliche Kofinanzierung mit Mitteln der EU-Kommission aus dem Förderprogramm „EU4Health". Der vorliegende Entwurf ist daher kein Vorschlag für einen Umsetzungsrechtsakt (da aufgrund der für den EHDS gewählten Rechtsform Verordnung sonst gegen das Transformationsverbot verstoßen würde), sondern ein rein inhaltlicher Vorgriff betreffend den mit dem EHDS ohnehin verpflichtend umzusetzenden Punkten der Nationalen Kontaktstelle für digitale Gesundheit, des EU-Rezepts und der EU-Patientenkurzakte. Diese (sowie andere) Punkte wurden von anderen Mitgliedstaaten der Union bereits auf Grundlage nationaler Rechtsakte umgesetzt, weshalb die Anbindung an MyHealth@EU bereits zum jetzigen Zeitpunkt Sinn ergibt.

Die vorgeschlagene Implementierung des EU-Rezepts und der EU-Patientenkurzakte in Österreich entspricht nicht zuletzt auch den nationalen Bestrebungen zur Digitalisierung des Gesundheitswesens:

Bereits nach dem Regierungsprogramm 2020–2024 „Aus Verantwortung für Österreich" sollen die Fortschritte der Digitalisierung auch im Gesundheitsbereich einen einfacheren und verbesserten Zugang zu medizinischen Leistungen ermöglichen und die Digitalisierung in Diagnose und Behandlung vorangetrieben werden. Ebenso ist im Regierungsprogramm 2025-2029 „Jetzt das Richtige Tun. Für Österreich" die *„verantwortungsvolle Umsetzung des Europäischen Raums für Gesundheitsdaten (EHDS) unter höchsten Sicherheitsstandards unter der Schirmherrschaft von Statistik Austria, Austrian Micro Data Center (AMDC) und Gesundheit Österreich (GÖG) und Einrichtung entsprechender Kontrollmechanismen (Berichte an das Parlament)*" vorgesehen, welche ebenso die Primärdatennutzung inkludiert.

Darüber hinaus beschloss der Ministerrat am 1. Juni 2023 die digitalen Ziele der Bundesregierung in Form des „Digital Austria Act – Für mehr Wohlstand, Sicherheit und neue Chancen durch Innovation", in dessen Punkt 7.2. die Erweiterung des nationalen e-Rezepts um die grenzüberschreitende elektronische Verschreibung (ePrescription) und elektronische Abgabe (eDispensation) vorgesehen ist.

Im Juni 2024 wurde die „eHealth-Strategie Österreich" (abrufbar unter: https://www.sozialministerium.at/dam/jcr:6f5c5706-b2c4-48a2-8b6a-c7f72f9580e3/240806-eHealth-bf.pdf) beschlossen, wonach es mitunter möglich werden soll, grenzüberschreitende Leistungen für Bürger/innen anzubieten, wie z. B. die Möglichkeit, ein Rezept in jeder Apotheke innerhalb der EU einlösen zu können (siehe unter anderem die Maßnahme M3.11 zur Mitwirkung bei für die öffentlichen GTI relevanten EU-Initiativen).

Vor diesem Hintergrund soll mit dem vorliegenden Entwurf die Rechtsgrundlage für die grenzüberschreitenden Gesundheitsanwendungen EU-Rezept und EU-Patientenkurzakte geschaffen werden. Die Verwendung des EU-Rezepts und der EU-Patientenkurzakte liegt im (erheblichen) öffentlichen Interesse, welches sich insbesondere ergibt aus:

- der Sicherstellung der Kontinuität der Gesundheitsversorgung durch eine verbesserte, schnellere Verfügbarkeit medizinischer Informationen, die zu einer Qualitätssteigerung diagnostischer und therapeutischer Entscheidungen sowie der Behandlung und Betreuung führen,
- der Erhöhung der Patient/inn/en/sicherheit,
- der Steigerung der Prozess- und Ergebnisqualität von Gesundheitsdienstleistungen,
- der Aufrechterhaltung einer qualitativ hochwertigen, ausgewogenen und allgemein zugänglichen Gesundheitsversorgung sowie
- der Stärkung der Patient/inn/en/rechte, insbesondere in Bezug auf die Verfügbarkeit ihrer elektronischen Gesundheitsdaten und ihre Kontrolle über diese Daten,

jeweils auf grenzüberschreitender Ebene.

Die Zuständigkeit zur Erlassung dieses Bundesgesetzes stützt sich auf den Kompetenztatbestand „Gesundheitswesen" (Art. 10 Abs. 1 Z 12 B-VG).

Zu Art. 1 (Änderung des Gesundheitstelematikgesetzes 2012)

Zu Z 1 (Inhaltsverzeichnis – Entfall des § 12, Abschnittsbezeichnung 7) und Z 2 (Inhaltsverzeichnis – 6. Abschnitt):

Durch die Einfügung eines neuen 6. Abschnitts ist es notwendig, diese Änderungen auch ins Inhaltsverzeichnis zu übernehmen. § 12 soll entfallen, daher wird auch der entsprechende Eintrag im Inhaltsverzeichnis gelöscht.

Zu Z 3 (§ 1 Abs. 2 Z 3), Z 4 (§ 1 Abs. 2 Z 4 und Z 5)

Die Ziele des Gesundheitstelematikgesetzes 2012 (im Folgenden „GTelG 2012") sind entsprechend dem gegenständlichen Vorhaben um einheitliche Regelungen für die ungerichtete Kommunikation elektronischer Gesundheitsdaten und genetischer Daten im Rahmen von spezifischen Anwendungen der grenzüberschreitenden Gesundheitsversorgung zu ergänzen. Von der vorliegenden Novelle nicht umfasst ist jedoch die unmittelbare Verarbeitung genetischer Daten (etwa ganze Genome oder auch nur Ausschnitte dessen). Siehe dazu auch die Erläuterungen zum 1. Unterabschnitt des 6. Abschnitts.

Zu Z 5 (§ 2 Z 2), Z 6 (§ 2 Z 2 lit. f):

Die Erweiterung der Definition der Gesundheitsdiensteanbieter ist notwendig für die neuen Zwecke des 6. Abschnitts und erfolgt sowohl in formeller Sicht auf Gesundheitsdiensteanbieter in MyHealth@EU-Mitgliedstaaten anstelle der Erfassung nur österreichischer Gesundheitsdiensteanbieter, als auch in inhaltlicher Sicht durch die Aufnahme des Zwecks der Unterstützung der grenzüberschreitenden Gesundheitsversorgung. Im aktuellen Gesetzesvorhaben dient die Erweiterung der Aufnahme von Apothekerinnen und Apothekern in MyHealth@EU-Mitgliedstaaten dem Anwendungsfall der elektronischen Abgabe gemäß § 24p. Der neue Zweck in § 2 Z 2 lit. f dient der Erfassung der notwendigen Infrastruktur in Form der Nationalen Kontaktstelle für digitale Gesundheit gemäß § 24j in Entsprechung der ELGA-Infrastruktur sowie den übrigen Bestimmungen des GTelG 2012. Ebenso umfasst ist der Zugriff auf die EU-Patientenkurzakte durch bestimmte ELGA-Gesundheitsdiensteanbieter in § 24t GTelG 2012.

Die Ausgestaltung der tatsächlichen Zugriffsrechte obliegt aufgrund des Behandlungslandprinzips bei grenzüberschreitenden Gesundheitsanwendungen in Verbindung mit Art. 168 Abs. 7 AEUV dem jeweiligen Behandlungsmitgliedstaat. Analog zur nationalen Rechtsgrundlage, welche Apotheken den Zugriff auf in anderen MyHealth@EU-Mitgliedstaaten ausgestellte EU-Rezepte erlaubt, müssen die anderen MyHealth@EU-Mitgliedstaaten spiegelbildliche Bestimmungen anhand der nationalen Berufsrechte in ihrem jeweiligen Rechtssystem vorsehen. Dabei ist anzumerken, dass die Datenschutzgrundverordnung, insbesondere dessen Art. 5 jede Datenverarbeitung auf die für die Zweckerfüllung absolut notwendigen Zugriffsrechte („need-to-know-Prinzip") beschränkt. Die Einhaltung dessen ist durch die jeweilige nationale Aufsichtsbehörde für Datenschutz zu kontrollieren.

Zu Z 7 (§ 2 Z 9 lit f):

Die aus der Patientenmobilitätsrichtlinie stammenden Definition der patient summary entfällt aufgrund der nun detaillierten Regelung im Rahmen von MyHealth@EU. Dies entspricht auch der Rechtslage ab Anwendbarkeit der Bestimmungen des EHDS zur Patientenkurzakte.

Zu Z 7a (§ 2 Z 10 lit. e):

In der Praxis werden in mehreren Bundesländern die mobilen Einrichtungen der Pflege im Wege der Privatwirtschaftsverwaltung auf Basis von Vereinbarungen zwischen den Trägern und den Bundesländern betrieben, wobei eine Aufsicht bzw. Kontrolle dieser Einrichtungen lediglich auf vertraglicher Basis vereinbart werden kann. Durch die Änderung soll klargestellt werden, dass auch diese Einrichtungen von der gesetzlichen Regelung erfasst sind.
Klarstellend ist festzuhalten, dass unter der Formulierung „oder von einem Bundesland finanziert" auch eine solche Förderung aus Mitteln des Sozialfonds, welcher durch Land und Gemeinden finanziert wird, verstanden werden kann.

Weiters soll klargestellt werden, dass Einrichtungen für Menschen mit Behinderungen („Einrichtungen der Behindertenhilfe", „Einrichtungen der Teilhabe") nicht unter die Definition einer Einrichtung der Pflege im Sinne des GTelG 2012 fallen. Sie sind somit keine ELGA-Gesundheitsdiensteanbieter und dadurch weder zur Speicherung des Pflegesituationsberichts gemäß § 13 Abs. 3 Z 6 verpflichtet, noch berechtigt, überhaupt auf ELGA zuzugreifen.

Hintergrund dieser Änderung ist, dass Einrichtungen für Menschen mit Behinderungen keine Pflegeeinrichtungen im klassischen Sinn sind und der Fokus viel mehr auf soziale Teilhabe, statt auf medizinischer Pflege liegt. Es besteht die Gefahr, dass durch eine pauschale Zuordnung zur Pflege der

Eindruck entsteht, dass es sich bei Menschen mit Behinderungen um medizinisch betreute Personen mit Pflegebedarf handelt. Diese medizinische Sicht von Behinderung widerspricht dem sozialen und menschenrechtlichen Modell von Behinderung, das die Grundlage der UN-Behindertenrechtskonvention (UNBRK) bildet.

Zu Z 8 (§ 2 Z 20-28):

Die Einschränkung der Definition des „MyHealth@EU-Mitgliedstaats" auf solche „mit aufrechter Verbindung zur österreichischen Nationalen Kontaktstelle für digitale Gesundheit" resultiert aus der Notwendigkeit, noch vor Produktivnahme des Datenaustauschs zwischen den jeweiligen Länderpaaren bilateral die Interoperabilität für das jeweilige Service (im gegenständlichen Fall für elektronische Verschreibungen und elektronische Abgaben) sowohl als Herkunfts-, als auch Behandlungsmitgliedstaat zu testen und damit sicherzustellen (**Z 20**).

Aus der vorgeschlagenen Definition des Herkunftsmitgliedstaats (**Z 21**) erschließt sich, dass dem 6. Abschnitt ein anderes Begriffsverständnis von „Bürger/innen" zugrunde liegt als dem 5. Abschnitt: Gemeinsam ist beiden – neben der technischen Nutzung der ELGA-Infrastruktur nach dem 4. Abschnitt – aus rechtlicher Sicht, dass sie unabhängig von der jeweiligen Staatsbürgerschaft Anwendung finden, während Bürgerinnen nach dem 6. Abschnitt entgegen jenen nach dem 5. Abschnitt – entsprechend deren jeweils unterschiedlichen Regelungsbereichen, Zwecken und damit verbundenen Prozessabläufen – nicht notwendigerweise im Patientenindex gemäß § 18 eingetragen sein müssen [vgl. ErlRV 232 BlgNR XXVII. GP, 5], sondern einen bestehenden (Haupt- oder Neben-)Wohnsitz oder ein aufrechtes Sozialversicherungsverhältnis in entweder Österreich als Herkunftsmitgliedstaat, oder einem anderen Herkunftsmitgliedstaat haben müssen, um die grenzüberschreitenden Gesundheitsservices nach dem 6. Abschnitt in Österreich als Behandlungsmitgliedstaat oder einem anderen Behandlungsmitgliedstaat in Anspruch nehmen zu können. Insoweit knüpft der gegenständliche Entwurf insbesondere auch an geltenden sozialversicherungsrechtliche Vorschriften an, ändert diese aber in keinster Weise, was daher im vorgeschlagenen § 24i Abs. 3 explizit zum Ausdruck gebracht werden soll.

Für Näheres zu „MyHealth@EU" (**Z 23**) siehe die Erläuterungen zu § 24i, für Details zur „Nationalen Kontaktstelle für digitale Gesundheit" (**Z 24**) die Erläuterungen zu § 24j.

Zu Z 9 (Entfall des § 12):

Es wird der Entfall der Bestimmung mit der Begründung der Einfügung eines 6. Abschnitts vorgeschlagen.

Zu Z 10 (§ 12a Abs. 2 Z 3, 5 und 6), Z 11 und Z 11a (§ 12b Abs. 1 Z 3, Z 4, Z 5):

Diese Bestimmungen sollen der Erweiterung der bereits existierenden Plattformen (Öffentliches Gesundheitsportal, Plattform für Gesundheitsdiensteanbieter) auf grenzüberschreitende Anwendungen dienen.

Zu Z 11b und Z 11d (§ 13 Abs. 3 Z 6):

Bisher fiel ein Großteil der mobilen Pflegedienste in den Ländern nicht unter die Definition der „Einrichtung der Pflege" gemäß § 2 Z 10 lit. e, weshalb sie nicht als ELGA-Gesundheitsdiensteanbieter zu qualifizieren waren und demgemäß nicht zur Speicherung des Pflegesituationsberichts verpflichtet waren, ja nicht einmal berechtigt waren, auf ELGA zuzugreifen.

Durch die vorgeschlagene Änderung in § 2 Z 10 lit. e (siehe die Erläuterungen zu Z 7a) fallen diese mobilen Pflegedienste künftig jedoch schon unter die neue Definition.

Um diesen Pflegeeinrichtungen eine ausreichende Vorbereitungszeit für die Anbindung an ELGA zu ermöglichen, soll der Beginn der Speicherverpflichtung um ein Jahr verschoben zu werden.

Da mit der vorgeschlagenen Änderung in Z 4 (siehe die Erläuterungen zu Z 11c) eine gänzlich neue Speicherverpflichtung für Pflegeeinrichtungen eingeführt wird, scheint es angebracht, die Speicherverpflichtungen gänzlich und nicht nur in Bezug auf mobile Pflegedienste zu harmonisieren.

Zu Z 11c (§ 13 Abs. 3 Z 4)

Es handelt sich bei der vorgeschlagenen Änderung um eine Klarstellung der bereits geltenden Rechtsgrundlage. Unter den Begriff „Krankenanstalten" sind auch selbstständige Ambulatorien gemäß § 2 Abs. 1 Z 5 KAKuG, deren Leistungsspektrum Aufgaben der ärztlichen Berufe im Sinne des § 2 Z 10 GTelG 2012 umfasst, zu verstehen. Sofern eine Krankenanstalt die Verordnung eines Arzneimittels nicht selbst vornimmt (sondern dies beispielsweise nur empfiehlt oder bisherige Verordnungen im Entlassungsbericht festhält) trifft die Pflicht zur Speicherung der Medikationsdaten jene:n Angehörige:n des ärztlichen Berufs, der:die die Verordnung tatsächlich vornimmt.

Weiters sollen auch Einrichtungen der Pflege Medikationsdaten speichern. Dies soll Angehörigen der Gesundheitsberufe, die in Pflegeeinrichtungen tätig sind und im Rahmen dieser Tätigkeit Verordnungen ausstellen ermöglichen, diese in der eMedikation zu speichern.

Zu Z 12 (§ 18 Abs. 1 Z 1), Z 13 (§ 18 Abs. 4a), Z 17 (§ 21 Abs. 1), Z 18 (§ 21 Abs. 4), Z 20 (§ 23 Abs. 1 Z 2)

Mit dem gegenständlichen Vorhaben wird es notwendig, die ELGA-Infrastruktur nicht nur den eHealth-Anwendungen gemäß dem 5. Abschnitt, sondern nun auch den Anwendungen der grenzüberschreitenden Gesundheitsversorgung zu öffnen.

Zu Z 14 (§ 18 Abs. 4a Z 2), Z 15 (§ 18 Abs. 4b Z 1), Z 16 (§ 18 Abs. 4b Z 4):

Es erfolgt eine legistische Klarstellung, dass Personalausweise als Passersätze im Sinne des § 18 Passgesetz 1992 für die Überprüfung der Identität im Rahmen des § 18 herangezogen werden können, nicht jedoch Übernahmserklärungen für Staatsbürger im Sinne des § 18 Passgesetz 1992 sowie gewöhnliche Reisepässe für bestimmte Anlassfälle, die über keine Datenträger verfügen, gemäß § 4a Passgesetz 1992 (umgangssprachlich „Notpass" genannt).

Zu Z 19 (§ 22 Abs. 1):

Die Erweiterung des Anwendungsbereichs des Protokollierungssystems auch auf Anwendungen des 6. Abschnitts gewährleistet die Übernahme der ELGA-Systematik auch auf Anwendungen im grenzüberschreitenden Kontext. Es ist allerdings darauf hinzuweisen, dass diese Protokollierungspflicht nur für österreichische Gesundheitsdiensteanbieter gelten kann. Mangels Anwendbarkeit österreichischen Rechts kann Gesundheitsdiensteanbietern in anderen MyHealth@EU-Mitgliedstaaten beispielsweise nicht vorgeschrieben werden, dass auch die Namen der natürlichen Personen erfasst werden, die für sie tätig werden.

Zu Z 21 (6. Abschnitt, § 24i bis § 24r):

Die Menschen können ihre Gesundheitsdaten nicht immer einfach elektronisch abrufen, und wenn sie Ärzte in mehr als einem Krankenhaus oder medizinischen Zentrum konsultieren möchten, können sie die Daten oft nicht an andere Angehörige der Gesundheitsberufe weitergeben. Auf nationaler Ebene wurde dem bereits im Jahr 2012 mit der Einführung der Elektronischen Gesundheitsakte ELGA begegnet.

Über die nationalen Grenzen hinweg wird die Situation noch schwieriger. Wenn eine Patientin oder ein Patient einen Arzt oder eine Ärztin in einem anderen Land aufsucht, sind die medizinischen Daten oft nicht zugänglich, was zu Verzögerungen, Fehldiagnosen oder falschen Behandlungen führen kann. In den meisten Fällen können Ärztinnen und Ärzte die Gesundheitsdaten der Patienten und Patientinnen nicht einsehen, wenn diese sich in einem anderen Land haben behandeln lassen. Die Kontinuität der Versorgung und der rasche Zugang zu personenbezogenen elektronischen Gesundheitsdaten sind für die Menschen in Grenzregionen noch wichtiger, da sie häufig die Grenze überqueren, um Gesundheitsdienstleistungen in Anspruch nehmen zu können.

Die Richtlinie 2011/24/EU über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung wurde im Jahr 2011 angenommen und bis 2015 in allen Mitgliedstaaten umgesetzt. In Art. 14 dieser Richtlinie wurde erstmals in einer EU-Rechtsvorschrift auf elektronische Gesundheitsdienste (eHealth) Bezug genommen und das Netzwerk für elektronische Gesundheitsdienste (eHealth Network) geregelt, dessen Maßnahmen freiwilligen Charakter haben und die Mitgliedstaaten zwar politisch, nicht aber rechtlich, verpflichten. So wurde den Mitgliedstaaten beispielsweise empfohlen, bei nationalen Ausschreibungen für Standards und Spezifikationen das europäische Austauschformat für elektronische Patientenakten (European Electronic Health Record Exchange Format, EEHRxF) zu verwenden, um Interoperabilität herzustellen.

Bezüglich der Verwendung personenbezogener elektronischer Gesundheitsdaten für Primärzwecke im Zusammenhang mit der grenzüberschreitenden Gesundheitsversorgung wurde die Plattform „MyHealth@EU" als unionsweite digitale Infrastruktur eingerichtet, an die bereits viele Mitgliedstaaten angebunden sind und die bisher zwei grenzüberschreitende Gesundheitsdienste unterstützt: Zum einen die Patientenkurzakte (Patient Summary) und zum anderen die elektronische Verschreibung und elektronische Abgabe (ePrescription, eDispensation), wozu das eHealth-Netzwerk jeweils eine Leitlinie angenommen und diese den Mitgliedstaaten zur Implementierung empfohlen hat. Weiterführende Informationen zur Plattform MyHealth@EU einschließlich zu der vom eHealth-Netzwerk verabschiedeten Leitlinie für die hier zur Regelung vorgeschlagene elektronische Verschreibung und elektronische Abgabe sind online abrufbar unter https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_de. An weiteren grenzüberschreitenden Services wie medizinischen Bilddaten, Laborergebnissen und Entlassungsberichten von Krankenanstalten wird auf Unionsebene bereits gearbeitet, um langfristig auch diese in der gesamten EU verfügbar zu machen.

Nach Ansicht der EU-Kommission machen jedoch zum einen die schleppende Anbindung von Mitgliedstaaten und die bisherige Verfügbarkeit von nur zwei grenzüberschreitenden Services, und zum anderen die rasanten Fortschritte im Bereich der elektronischen Gesundheitsdienste in den letzten Jahren, insbesondere aufgrund der COVID-19-Pandemie, erforderlich, das Vorgehen auf EU-Ebene besser zu koordinieren, was schließlich in der Verordnung über den europäischen Gesundheitsdatenraum mündete.

Gemäß Kapitel II der nun kundgemachten Verordnung zur Schaffung eines europäischen Gesundheitsdatenraums werden die Mitgliedstaaten zur Errichtung einer Nationalen Kontaktstelle für digitale Gesundheit als Infrastruktur sowie zur Implementierung der genannten grenzüberschreitenden Services verpflichtet.

Diese Vorgaben des Europäischen Raums für Gesundheitsdaten für die Mitgliedstaaten werden erst mit Inkrafttreten und Anwendbarkeit der Verordnung verpflichtend, dennoch sollen die Nationale Kontaktstelle für digitale Gesundheit als Infrastruktur sowie die Anwendung EU-Rezept in Österreich schon vorzeitig implementiert werden. Grund dafür ist eine nur noch jetzt mögliche Kofinanzierung mit Mitteln der EU-Kommission aus dem Förderprogramm „EU4Health".

Zum 1. Unterabschnitt (§§ 24i bis § 24n), Allgemeine Bestimmungen zu MyHealth@EU):

„MyHealth@EU" ist die unionsweite, grenzüberschreitende Infrastruktur zur Verarbeitung von ELGA-Gesundheitsdaten sowie Daten aus anderen Mitgliedstaaten für Zwecke der grenzüberschreitenden Gesundheitsversorgung, bestehend aus den Nationalen Kontaktstellen für digitale Gesundheit unter der Verantwortung der Mitgliedstaaten einerseits, und der von der Kommission betriebenen, zentralen Plattform für digitale Gesundheit andererseits (auf die hier mangels Regelungsbedarf nicht weiter einzugehen ist; siehe dazu die Erläuterungen zu § 24j Abs. 1).

Mit der vorgeschlagenen Novelle sollen das EU-Rezept sowie die EU-Patientenkurzakte als erste grenzüberschreitende Gesundheitsanwendungen über MyHealth@EU implementiert werden, der weitere Anwendungen bestimmter (laut Verordnung über den europäischen Gesundheitsdatenraum „prioritärer") Datenkategorien wie etwa Entlassungsbriefe von Krankenanstalten und Laborbefunde folgen werden. Nicht explizit umfasst sind genetische Daten, die ebenfalls Gegenstand der Regelungen des GTelG 2012 sind. Aufgrund der Vielzahl folgender Datenkategorien sowie deren jeweiligem Umfang (insb. Entlassungsbriefe gemäß § 2 Z 9 lit. a sub-lit. aa) kann jedoch nicht vollständig ausgeschlossen werden, dass sich aus den Inhalten dieser medizinischen Dokumente direkt Angaben zu genetischen Daten oder indirekt Hinweise zu diesen ergeben (etwa im Falle bestimmter Erkrankungen). Es kann jedoch ausgeschlossen werden, dass im Rahmen dieser MyHealth@EU-Daten direkt genetische Daten (etwa ein vollständiges Genom oder Ausschnitte dessen) übermittelt werden, da diese weder im EU-weiten „requirements-Katalog", noch in den Implementierungsleitfäden zu den ELGA-Gesundheitsdaten vorgesehen sind, weshalb diese nicht als ELGA-Dokument erfasst werden können und damit auch den Anwendungen des 6. Abschnitts nicht zur Verfügung stehen.

Die im 1. Unterabschnitt des 6. Abschnitts vorgeschlagenen Regelungen sollen nicht nur für das EU-Rezept gemäß dem 2. Unterabschnitt und die EU-Patientenkurzakte gemäß dem 3. Unterabschnitt gelten, sondern für sämtliche, künftig über MyHealth@EU zur Verfügung gestellten Services, die in weiteren Unterabschnitten zu regeln sein werden. Denn all den genannten Gesundheitsanwendungen ist vor allem dreierlei gemein:

Erstens handelt es sich dabei durchwegs um Formen der ungerichteten Kommunikation, da alle über MyHealth@EU angebotenen Services den teilnehmenden Bürger/innen und zugriffsberechtigten Gesundheitsdiensteanbietern in elektronischer Form zeit- und ortsunabhängig („ungerichtet") zur Verfügung stehen, wobei die Empfänger der Gesundheitsdaten nicht (wie bei der gerichteten Kommunikation von A nach B) abschließend im Vorhinein namentlich bekannt, sondern (wie bei der ELGA gemäß dem 4. Abschnitt) lediglich generisch, etwa durch generelle Definitionen, festgelegt sein müssen.

Zweitens werden alle über MyHealth@EU angebotenen Services mittels der gleichen Prozessschritte abgewickelt, was folgend kurz skizziert werden soll, wobei Österreich entweder Herkunftsmitgliedstaat (für österreichische natürliche Personen) oder Behandlungsmitgliedstaat (für natürliche Personen des EWR) sein kann:

Eine natürliche Person (zur Definition siehe die Erläuterungen zu § 2 Z 21) wird von einem Gesundheitsdiensteanbieter in seinem/ihrem Herkunftsstaat behandelt und dabei entweder eine elektronische Verschreibung ausgestellt und/oder die erfolgte Behandlung in der elektronischen Gesundheitsakte der natürlichen Person dokumentiert.

Diese natürliche Person begibt sich in weiterer Folge von Österreich in einen anderen (Behandlungs-)Mitgliedstaat, und muss dort von einem Gesundheitsdiensteanbieter betreut – d.h. entweder medizinisch behandelt oder in einer Apotheke mit Arzneimitteln versorgt – werden.

Nachdem der Gesundheitsdiensteanbieter im Behandlungsmitgliedstaat die Identität der natürliche Person geprüft und diesen oder diese erfolgreich authentifiziert hat, übermittelt er von seiner lokalen Software aus eine Datenanfrage über die nationale Infrastruktur an die Nationale Kontaktstelle des Behandlungsmitgliedstaats, welche diese über die zentrale Plattform der Kommission (siehe dazu die Erläuterungen zu § 24j Abs. 1 und den Anhang des Durchführungsbeschlusses 2019/1765) an die Nationale Kontaktstelle des Herkunftsmitgliedstaats der natürlichen Person, welche die Anfrage wiederum über die nationale Infrastruktur an jenen Gesundheitsdiensteanbieter weiterleitet, der die natürliche Person in seinem oder ihrem Herkunftsmitgliedstaat zuvor betreut hat. Von diesem werden sodann die angefragten Daten der natürlichen Person(elektronische Verschreibung oder in der elektronischen Gesundheitsakte bereitgestellte Befunde) mittels des oben beschriebenen Prozesses – über die nationale Infrastruktur und Nationale Kontaktstelle des Herkunftsmitgliedstaats zu jener des Behandlungsmitgliedstaats übermittelt, welche die Daten sodann über die nationale Infrastruktur an den anfragenden Gesundheitsdiensteanbieter übermittelt, der die natürliche Person sodann entsprechend (mittels elektronischer Abgabe der elektronischen Verschreibung oder Einsicht in die elektronische Gesundheitsakte) betreuen kann. Im Falle einer elektronischen Abgabe erfolgt als zusätzlicher Prozessschritt deren Übermittlung – wiederum mittels des oben beschriebenen Prozesses – an die jeweilige Anwendung des Herkunftsmitgliedstaats (in Österreich an das EU-Rezept-Service des Dachverbands), wo schließlich die erfolgte Abgabe – d.h. die elektronische Verschreibung als abgegeben – vermerkt wird.

Weitere Informationen hierzu können über die Website der Europäischen Kommission zu elektronischen grenzüberschreitenden Gesundheitsdiensten (abrufbar unter: https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_de) abgerufen werden, auf welcher auch die Leitlinien des eHealth-Netzes zu elektronischen Verschreibungen und zu Patientenkurzakten abrufbar sind.

Drittens soll schließlich die datenschutzrechtliche Information gemäß Art. 13 f. DSGVO für sowohl österreichische als auch ausländische natürliche Personen sowie für österreichische Gesundheitsdiensteanbieter (unabhängig vom jeweiligen Service) über die MyHealth@EU-Website der EU-Kommission (siehe https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_de) abrufbar sein, und deren Inhalte in eine neue, von der Gesundheit Österreich GmbH eigens für MyHealth@EU erstellte und betriebene Website integriert werden, wo im Rahmen der Öffentlichkeitsarbeit auch weitere relevante Informationen über MyHealth@EU zur Verfügung gestellt werden sollen.

Trotz der dargestellten Gemeinsamkeiten aller über MyHealth@EU angebotenen, grenzüberschreitenden Gesundheitsanwendungen, unterscheidet sich doch die Nutzung der technischen Komponenten je nach (dem jeweiligen Zweck der) Anwendung, weshalb im 2. und 3. Unterabschnitt (und künftig auch in den folgenden Unterabschnitten) jeweils anwendungsspezifische Regelungen vorgeschlagen werden, welche die (allgemeinen) Regelungen des 1. Unterabschnitts entsprechend ergänzen sollen.

Zu § 24i (Ziele der grenzüberschreitenden Gesundheitsversorgung):

Die Zwecke des 6. Abschnitts entsprechen im Grunde jenen der Elektronischen Gesundheitsakte in § 13, konkretisiert um das grenzüberschreitende Element. Es sind dies daher jeweils auf grenzüberschreitender Ebene 1.) die Sicherstellung der Kontinuität der Gesundheitsversorgung durch eine verbesserte, schnellere Verfügbarkeit medizinischer Informationen, die zu einer Qualitätssteigerung diagnostischer und therapeutischer Entscheidungen sowie der Behandlung und Betreuung führt,2.) die Erhöhung der Patient/inn/ensicherheit, 3.) die Steigerung der Prozess- und Ergebnisqualität von Gesundheitsdienstleistungen, 4.) die Aufrechterhaltung einer qualitativ hochwertigen, ausgewogenen und allgemein zugänglichen Gesundheitsversorgung sowie 5.) die Stärkung der Patient/inn/enrechte, insbesondere in Bezug auf die Verfügbarkeit ihrer elektronischen Gesundheitsdaten und ihre Kontrolle über diese Daten.Wie bereits in der Einleitung der Erläuterungen zum 6. Abschnitt ausgeführt dient dieser nicht zuletzt der Vorbereitung auf den Europäischen Gesundheits-Datenraum, welcher unter anderem die Interoperabilität der in den Mitgliedstaaten bestehenden nationalen Systemen vorsieht. Die Zwecke des Abs. 1 sind weit gefasst und müssen immer zusammen mit den konkreten Zwecken der weiteren Unterabschnitte gelesen werden. Im gegenständlichen Gesetzesvorhaben sind die Zwecke in § 24o Abs. 2 konkretisiert, welche im Einklang mit den übergeordneten Zielen des § 24i Abs. 1 stehen. Mit anderen Worten sind die übergeordneten Zwecke Zielvorgaben, welche gegenständlich zumindest in Bezug auf die Verschreibung und Abgabe von Arzneimitteln durch den Anwendungsfall EU-Rezept und durch den

Abruf der EU-Patientenkurzakte erreicht werden sollen. Da es sich um Gesundheitsdaten handelt ist Art. 9 (iVm Art. 6 Verordnung [EU] 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Datenschutz-Grundverordnung], ABl. Nr. L 119 vom 04.05.2016 S. 1 [im Folgenden: DSGVO]) betreffend die Rechtmäßigkeit der Verarbeitung einschlägig. Die in Abs. 1 festgeschriebenen Zwecke entsprechen jeweils den Fällen des Art. 9 Abs. 2 lit h bis i iVm Art. 6 Abs. 1 lit. c, e DSGVO, wobei jeweils jeder Zweck der Z 1-5 sowohl im Interesse der Patient/inn/en, der Gesundheitsdiensteanbieter und der öffentlichen Gesundheit liegt. Kurz zusammengefasst wird es Patient/inn/en ermöglicht, potenziell lebenswichtige Arzneimitteln ohne Sprachbarrieren zu beziehen, Gesundheitsdiensteanbieter wird die im Interesse der Patient/inn/en stehende, reibungslose Erbringung ihrer Gesundheitsleistungen ermöglicht, und wird dem Ziel der öffentlichen Gesundheit durch eine lückenlose grenzüberschreitende Gesundheitsversorgung entsprochen. Zu den insbesondere im Zusammenhang mit den Art. 9 Abs. 2 lit. h, i DSGVO ergriffenen, angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen siehe die Erläuterungen zu Abs. 2 (Opt-in), § 24k (Grundsätze der Datenverarbeitung), §§ 24l, 24m (verpflichtende Überprüfung der Identität von Bürgerinnen und Bürgern sowie von Gesundheitsdiensteanbietern).

Das in **Abs. 2** vorgesehene Opt-in stellt eine zusätzliche Maßnahme dar, mit welcher sichergestellt werden soll, dass sich die Patient/innen der Konsequenzen ihrer Handlungen bewusst sind. Den natürlichen Personen bleibt es damit freigestellt, an MyHealth@EU zu partizipieren, um von den Anwendungsfällen des 2. Unterabschnitts Gebrauch zu machen. Es handelt sich daher nicht um eine Einwilligung iSd Art. 6 Abs. 1 lit. a iVm Art. 9 Abs. 2 lit. a DSGVO, sondern ist der 6. Abschnitt als Recht eines Mitgliedstaats iSd Art. 9 Abs. 2 lit. h-i DSGVO anzusehen. Siehe hierzu bereits Seite 15 des Arbeitspapiers „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“ der Artikel 29-Datenschutzgruppe.

Dies ist notwendig, da das Opt-in sinnvoll nur gemäß dem Prozess des § 24n Abs. 1 verwaltet werden kann, um dieses direkt, zentral und verlässlich allen gemeinsam Verantwortlichen iSd Art. 4 Z 7 iVm Art. 26 DSGVO, sowie allen Auftragsverarbeitern gegenüber zu administrieren. Im Falle der Einwilligung könnte diese zwar vor jedem/jeder Verantwortlichen iSd Art. 4 Z 7 DSGVO (im Folgenden: Verantwortlicher) abgegeben oder zurückgezogen werden, doch hat dies keinen Mehrwert für die Betroffenen, da die in § 24n vorgesehenen Zugangsmöglichkeiten weit niederschwelliger sind als in der DSGVO vorgesehen. Das Opt-in kann daher nur mit Wirkung pro futuro zurückgezogen werden, wodurch zwar die Löschfristen für bereits erfolgte Datenverarbeitungen unberührt bleiben, jedoch keine weiteren Datenverarbeitungen im Rahmen von MyHealth@EU mehr erfolgen können. Der für das Gesundheitswesen zuständige Bundesminister/die für das Gesundheitswesen zuständige Bundesministerin hat dafür Sorge zu tragen, dass nicht nur ein allgemeines Opt-in abgegeben werden kann, sondern dies auch nach Anwendungsfällen des 2. Unterabschnitts spezifiziert werden kann. Die Information der Betroffenen zu diesem Opt-in erfolgt (wie generell für die Datenverarbeitung) im Rahmen der verpflichtenden Datenschutz-Information gemäß Art 13, 14 DSGVO und firmiert EU-weit als „Patient Information Notice“. Die Abgabe eines Opt-in hat keine Auswirkung auf einen erklärten Widerspruch (Opt-out) gemäß § 15 GTelG 2012. Auch im Falle eines aufrechten Widerspruchs kann ein Opt-in für das EU-Rezept erklärt werden, da das für dessen Erstellung notwendige e-Rezept keine Möglichkeit eines Widerspruchs vorsieht und vom Widerspruch gemäß § 15 GTelG 2012 unabhängig ist.

Mit dem vorgeschlagenen **Abs. 3** soll explizit klargestellt werden, dass sozialversicherungsrechtliche Vorschriften vom gegenständlichen Entwurf nicht berührt werden, d.h. weder werden diese dadurch eingeschränkt, noch können daraus wie immer geartete sozialversicherungsrechtliche Ansprüche von Bürger/innen abgeleitet werden, sondern knüpft der vorgeschlagene Entwurf vielmehr an geltenden sozialversicherungsrechtlichen Vorschriften an (vgl. die Erläuterungen zu § 2 Z 21).

Zu § 24j (Nationale Kontaktstelle für digitale Gesundheit):

Die vorgeschlagene Festlegung der datenschutzrechtlichen Verantwortlichkeit beschränkt sich (ebenso wie jene der gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO im vorgeschlagenen § 24r Abs. 2) ausschließlich auf die nationale Ebene bzw. Infrastruktur und ist klar von jener auf Unionsebene zu unterscheiden, weil letztere bereits im tertiären Unionsrecht festgelegt wurde, nämlich im 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. Nr. L 270 vom 24.10.2019 S. 83: Gemäß dessen Art. 7 Abs. 1 gelten die Mitgliedstaaten als Verantwortliche für die von ihnen über die digitale eHealth-Service-Infrastruktur (MyHealth@EU) für grenzüberschreitende elektronische Gesundheitsinformationsdienste (im gegenständlichen Fall elektronische Verschreibungen und elektronische Abgaben) verarbeiteten

personenbezogenen Daten. Gemäß Art. 7 Abs. 2 des Durchführungsbeschlusses gilt die Kommission, die über ihre „zentrale Plattform für digitale Gesundheit" technische und organisatorische Lösungen für MyHealth@EU bereitstellt und verschlüsselte personenbezogenen Patientendaten im Namen der Mitgliedstaaten zwischen den Nationalen Kontaktstellen verarbeitet, als deren Auftragsverarbeiterin. Nachdem die Vorschriften für die Verarbeitung durch die Kommission als Auftragsverarbeiterin gemäß Art. 28 DSGVO und Art. 29 der Verordnung (EU) 2018/1725 (EU-DSGVO) bereits im Anhang des Durchführungsbeschlusses geregelt werden, wird in der vorgeschlagenen Novelle nicht weiter darauf eingegangen. Des Weiteren soll klargestellt werden, dass die Nationale Kontaktstelle (ebenso wie die Anwendung EU-Rezept, siehe dazu zu § 24o Abs. 1) Teil der öffentlichen Gesundheitstelematik-Infrastruktur ist gemäß § 3 Z 15 des Bundesgesetzes zur partnerschaftlichen Zielsteuerung-Gesundheit, BGBl. I Nr. 26/2017. Sie dient unter anderem der Weiterentwicklung von ELGA sowie des eHealth-Angebots in der Regelversorgung in Richtung der grenzüberschreitenden Vernetzung im Rahmen von MyHealth@EU sowie der Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten (**Abs. 1**).

Die Nationale Kontaktstelle für digitale Gesundheit des § 24j dient als zentrale Datendrehscheibe im Bereich der grenzüberschreitenden Gesundheitsversorgung. Diese knüpft an die etablierte ELGA-Infrastruktur an, um die ausschließlich anlassbezogene Kommunikation mit den Nationalen Kontaktstellen anderer MyHealth@EU-Mitgliedstaaten zu ermöglichen **(Abs. 2)**. Zu unterscheiden ist hierbei zwischen der allgemeinen „Zentralen Plattform für digitale Gesundheit", welche in Verantwortlichkeit der Mitgliedstaaten durch die Europäische Kommission als Auftragsverarbeiter betrieben wird, und den konkreten Datenverarbeitungen bei der Übermittlung zwischen Nationalen Kontaktstellen. Der Austausch von Daten zwischen den Nationalen Kontaktstellen basiert auf dem Kreis des Vertrauens iSd Art. 1 Abs. 3 DSGVO, der zwischen den MyHealth@EU-Mitgliedstaaten geschaffen wird. Er basiert auf den von der Europäischen Union vorgegebenen Standards für die Teilnahme an MyHealth@EU, welche jeweils im nationalen Recht umzusetzen sind. Unterschiedliche MyHealth@EU-Mitgliedstaaten werden daher entsprechend ihren nationalen Systemen unterschiedliche Ansätze verfolgen (siehe hierzu etwa die Erläuterungen zu § 24l Abs. 3 oder § 24m), doch ist darauf zu vertrauen, dass diese die vorgegebenen Standards erfüllen. Die Kommunikation zwischen den Nationalen Kontaktstellen erfolgt mittels dem „TESTA-Netzwerk" (Trans European Services for Telematics between Administrations). Dieses ist für den europaweiten Austausch von sensiblen Informationen zwischen Behörden gedacht und garantiert Service Levels für Netzwerkverfügbarkeit, Leistung und Sicherheit (Vertraulichkeit, Integrität, Authentifizierung und Verfügbarkeit). Es bietet u.a. eine dezidierte private Netzwerkinfrastruktur getrennt vom Internet; volle Verschlüsselung jeglicher Datenübertragung; Firewalls, Intrusion Detection und Prevention an allen Eingangsknoten; eine eigene nicht öffentliche Domain (testa.eu); Zugangsbeschränkung für exakt definierte Teilnehmer sowie die Verwendung von kryptografischen Algorithmen nach dem Stand der Technik. Insofern können die Vorgaben des GTelG 2012 hinsichtlich Vertraulichkeit (§ 6) und Integrität (§ 5) als erfüllt betrachtet werden. Zur Nutzung der ELGA-Komponenten gemäß § 24 Abs. 3 siehe die Erläuterungen zu § 24k Abs. 3.

Die in **Abs. 3** vorgesehene Löschfrist von 10 Jahren orientiert sich an den übrigen Löschfristen des GTelG 2012, beispielsweise in §§ 18, 20, sowie den nicht gesetzlich festgelegten Aufbewahrungsfristen die auch für die ELGA- und eHealth-Supporteinrichtung bestehen. Die 10-jährige Frist stellt dabei jedoch nur die maximale Aufbewahrungsfrist dar. Dem für das Gesundheitswesen zuständigen Bundesminister oder der zuständigen Bundesministerin als Nationale Kontaktstelle für digitale Gesundheit (und damit als Verantwortliche/r) obliegt es, gemäß Art. 5 DSGVO neben der laufenden Evaluation der eigenen Datenverarbeitungen auch die Aufbewahrungsdauer festzulegen. Je nach den jeweils geltenden (gesetzlichen) Anforderungen könnte daher auch eine kürzere Aufbewahrungsfrist geboten sein, wenn sich herausstellt, dass bereits vor Ablauf der 10-jährigen Frist eine Aufbewahrung für die Zweckerreichung nicht mehr notwendig ist. Die Frist beginnt nach Abschluss der ursprünglichen Verarbeitung zu laufen, also sobald das EU-Rezept im Ausland erfolgreich eingelöst und die elektronische Abgabe erfolgreich rückübermittelt wurde, oder sobald die Abgabe durch eine österreichische Apotheke erfolgreich in den Herkunftsmitgliedstaat übermittelt wurde oder sobald die EU-Patientenkurzakte erfolgreich durch einen österreichischen Gesundheitsdiensteanbieter abgerufen wurde.

Zu §24k (Grundsätze der Datenverarbeitung):

Die in § 24k angeführten Grundsätze gelten grundsätzlich für sämtliche Anwendungen des 2. Unterabschnitts, welche jeweils noch ergänzende Grundsätze für einen konkreten Anwendungsfall vorschreiben können (siehe § 24r). Es handelt sich im Wesentlichen um technische und organisatorische Maßnahmen iSd Art. 5 DSGVO, jedoch werden diese erweitert sowie die Ergreifung alternativer Maßnahmen ausgeschlossen, die womöglich ein geringeres Schutzniveau für die Betroffenen zur Folge

hätten. Hiefür wird von der Öffnungsklausel des Art. 9 Abs. 4 DSGVO iVm Art. 168 (7) AEUV, BGBl. III Nr. 86/1999, in der geltenden Fassung, Gebrauch gemacht, um das Schutzniveau der DSGVO zu übertreffen. Die Pflicht zur eindeutigen Identifizierung des **Abs. 1** entspricht bereits den Grundsätzen der DSGVO, zu deren spezifischen Anforderungen siehe bereits die Erläuterungen zu §§ 24l, 24m.

Die in **Abs. 2** angeführten Zwecke entsprechen im Wesentlichen jenen Zwecken der Definition des Gesundheitsdiensteanbieters in § 2 Z 2 lit. a, e und f, unterteilt nach der jeweiligen spezifischen Rolle. Ergänzend hinzu kommt lediglich die Klarstellung, dass auch Bürger/innen und deren Vertreter/innen für die Zwecke der Z 2 Daten verarbeiten dürfen.

Die taxative Aufzählung der zu verwendenden ELGA-Komponenten in **Abs. 3** ist an die grundsätzlichen Zwecke des Abs. 2 geknüpft. Daraus alleine ergibt sich jedoch noch keine Verarbeitungsgrundlage, da die Erfüllung dieser Zwecke nur in konkreten Anwendungsfällen des 2. und 3. Unterabschnitts erfolgen kann. Der jeweilige Verantwortliche hat daher gemäß der allgemeinen Systematik der DSGVO in jedem Anwendungsfall des 2. oder 3. Unterabschnitts ohnehin zu prüfen, welche Komponenten und in welchem Umfang diese für die Bereitstellung der einzelnen Anwendung erforderlich sind. Architekturbedingt und im Sinne der Verwaltungsökonomie ist zu erwarten, dass die Anwendungsfälle des 2. Unterabschnitts die aufgezählten ELGA-Komponenten regelmäßig brauchen werden. Der zentrale Patientenindex dient bereits für nationale Zwecke der Identifikation der Patient/inn/en, diese muss auch im grenzüberschreitenden Kontext bis zur grenzüberschreitenden Übermittlung der personenbezogenen Daten gegeben sein. Gleiches gilt im Falle der nationalen Gesundheitsdiensteanbieter für die Identifizierungsmöglichkeiten des § 4 Abs. 2 (eHealth-Verzeichnisdienst, Gesundheitsdiensteanbieterindex, eID). Das Protokollierungssystem dient auch im grenzüberschreitenden Kontext der Dokumentation und Nachvollziehbarkeit der Verarbeitungen, und die Ausübung der Teilnahmerechte wird gewöhnlich jedenfalls über das Zugangsportal zu ermöglichen sein. Eine Abkehr von dieser Systematik, oder eine Erweiterung der Datenverarbeitung (Empfänger, Datenkategorien, Zwecke, etc.) wäre als lex specials zu Abs. 3 im 2. oder 3. Unterabschnitt zu regeln.

Zu § 24l (Überprüfung der Identität von Bürger/inne/n):

Die Überprüfung der Identität der Bürger/innen wird mittels zwei unterschiedlicher Methoden (Abs. 1 und Abs. 2) ermöglicht. Beiden Möglichkeiten gemein ist, dass sie zum Schutz vor etwaigem Missbrauch der Daten oder unbefugtem Datenzugriff geeignet sind. Vor jedem Abruf hat eine Überprüfung der Identität der Bürger/innen zu erfolgen. Ein Abruf der Daten ist daher technisch ausgeschlossen, wenn der Gesundheitsdiensteanbieter nicht über eine Identifizierungsmarke (Abs. 1) oder über eine Ausweisnummer (Abs. 2) des Bürgers oder der Bürgerin verfügt. Beide Merkmale sind weder öffentlich bekannt noch ist eine Einsichtnahme in diese für jedermann rechtlich zulässig, weshalb dies eine hinreichende Garantie zum Schutze der Rechte und Freiheiten der natürlichen Personen bietet.

Die Identifizierung nach **Abs. 1** erfolgt unter Verwendung der Funktion E-ID gemäß den §§ 4 ff E-GovG, BGBl. I Nr. 10/2004 in der jeweils geltenden Fassung. Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin hat hiefür eine entsprechende E-ID taugliche Anwendung gemäß den §§ 4 ff E-GovG für die Bürger/innen zur Verfügung zu stellen. Nach erfolgtem Log-In wird eine Identifikations-Marke zur einmaligen, zeitlich beschränkten Verwendung (kurz: One Time Token, OTT) erzeugt. Im Falle der Identifizierung nach Abs. 1 kann der Gesundheitsdiensteanbieter im MyHealth@EU-Mitgliedstaat ausschließlich mit Hilfe dieses OTT eine eindeutige Zuordnung zum Patienten oder zur Patientin vornehmen und nur auf Grundlage dieser bereits durch die E-ID erreichte 2-Faktor-Authentfizierung die Verordnungsdaten zum/zur Bürger/in einsehen. Da sowohl im Falle des Abs. 1 als auch des Abs. 2 der die Identität prüfende Gesundheitsdiensteanbieter seinen Sitz in einem MyHealth@EU-Mitgliedstaat hat, können aufgrund des Territorialitätsprinzips keine für diesen verbindliche Rechtsvorschriften betreffend die Datenverarbeitung erlassen werden. Es obliegt daher dem jeweiligen Gesundheitsdiensteanbieter als Verantwortlichem, oder dem jeweiligen MyHealth@EU-Mitgliedstaat, eine entsprechende Rechtsgrundlage für die Datenverarbeitung zu finden bzw. zu erlassen. Für Österreich siehe die Erläuterungen zu Abs. 4. Abschließend soll klargestellt werden, dass die bereits in § 18 Abs. 4a Z 2 vorgesehene Identifizierung mittels Abgleich der zentralen Evidenz mit der Pass- oder Personalausweisnummer auch für die Zwecke des 6. Abschnitts herangezogen werden können, wie sich dies bereits direkt durch § 18 Abs. 4a ergibt.

Sowohl der Identifizierung nach Abs. 1 als auch nach § 18 Abs. 4a Z 2 gemein ist die Identifizierung im weiteren Prozess gemäß **Abs. 2**. Der für das Gesundheitswesen zuständige Bundesminister/die für das Gesundheitswesen zuständige Bundesministerin hat hiefür im Einklang mit dem E-GovG sowie der E-Government-Bereichsabgrenzungsverordnung das bPK-GH zu verwenden. Für jene Fälle, in denen im aus einem ELGA-Datenspeicher abgerufenen Dokument keine bPK-GH vorhanden ist, darf der für das Gesundheitswesen zuständige Bundesminister/die für das Gesundheitswesen zuständige Bundesministerin

den zentralen Patientenindex gemäß § 18 heranziehen um das bPK-GH zu ermitteln um eine Zuordnung der Dokumente zu ermöglichen. Da die bPK-GH nicht in einen anderen Mitgliedstaat übermittelt werden darf, erfolgt vor der Übermittlung eine Umwandlung der bPK-GH in die sogenannte „MyHealth@EU-ID". Dabei handelt es sich um eine pseudonyme Identifikationsnummer, die aus dem bPK-GH kryptographisch abgeleitet wird. Dabei wird das Base64 kodierte bPK-GH mittels des Hash-Verfahrens SHA-3 (Keccak) transformiert, sodass keine direkte Rückführung auf das Originalkennzeichen möglich ist. Das Ergebnis wird anschließend "URL-safe-Base64" zur „MyHealth@EU-ID" kodiert. Verwendet wird diese ID zur eindeutigen Identifizierung einer Person innerhalb von MyHealth@EU, ohne das tatsächliche bPK-GH preiszugeben (datenschutzfreundlich & pseudonymisiert).

Die in **Abs. 3** aufgezählten Datenkategorien stellen den maximalen Umfang der von den heimischen Gesundheitsdiensteanbietern zu verarbeitenden personenbezogenen Daten dar. Eine exakte Auflistung dieser Kategorien ist jedoch nicht möglich, da im System MyHealth@EU von jedem partizipierenden EU-Mitgliedstaat auf die Identifizierung durch die anderen MyHealth@EU-Mitgliedstaaten vertraut werden muss (siehe dazu die Erläuterungen zu § 24m). In anderen MyHealth@EU-Mitgliedstaaten wird diese Identifizierung voraussichtlich anders geregelt sein als in Österreich (siehe Erläuterungen zu Abs. 1 und 2), etwa durch einheitliche Bürgerkarten, Sozialversicherungs- oder Steuernummern. Österreichische Gesundheitsdiensteanbieter unterliegen dabei etwaigen beruflichen Verschwiegenheitspflichten ebenso wie der DSGVO, welche einer Weiterverarbeitung dieser Daten regelmäßig (und gegebenenfalls strafbewährt) entgegenstehen.

Zu § 24m (Überprüfung der Identität von Gesundheitsdiensteanbietern):

Die Überprüfung der Identität von Gesundheitsdiensteanbietern hat auch im grenzüberschreitenden Kontext des 6. Abschnitts grundsätzlich anhand der etablierten ELGA-Infrastruktur zu erfolgen. Sowohl die Nationale Kontaktstelle als auch die Gesundheitsdiensteanbieter sind grundsätzlich in den in § 4 aufgezählten Registern geführt.

Die unterschiedliche Behandlung von Gesundheitsdiensteanbietern nach Zwecken widerspiegelt die tatsächlichen Verhältnisse der Datenverarbeitungen. Während jene Gesundheitsdiensteanbieter in einem direkten Behandlungszusammenhang tatsächlichen Zugriff auf die Inhaltsdaten als Gesundheitsdaten haben, und daher ein höherer Maßstab an deren Transparenz und Kontrolle zu legen ist, erfüllen die übrigen Gesundheitsdiensteanbieter im Falle der Nationalen Kontaktstelle lediglich administrative Rollen, bzw. hat die ELGA- und eHealth-Supporteinrichtung ohnehin die eindeutige Identität und Authentizität der Betroffenen zu überprüfen (elektronisch via eID oder schriftlich/persönlich mittels Ausweis/Unterschriftenprobe) und unterliegt jeweils eigenen Protokollierungspflichten.

Für den ersten konkreten Anwendungsfall des EU-Rezepts gemäß dem 2. Unterabschnitt ist Grundvoraussetzung für den Nachweis und die Prüfung der eindeutigen Identität von Gesundheitsdiensteanbietern in Österreich deren Teilnahme am e-Card-System als Vertragspartner mit der Ausprägung „öffentliche Apotheke". Zusätzlich zum allgemeinen System ist es für Zwecke des 2. Unterabschnitts auch notwendig, die jeweilig gesteckte Admin-Karte einem/einer Mitarbeitenden als natürliche Person zuzuweisen. Erfasst werden daher sowohl die abgebende Apotheke an sich, als auch der/die jeweilige Mitarbeitende der/die die konkrete Abgabe durchgeführt hat. Die Zuweisung kann vom Apotheker oder von der Apothekerin geändert oder gelöscht werden, allerdings nur mit Wirkung pro futuro. Erfolgte Abgaben werden lückenlos protokolliert mit dem Namen des/der Mitarbeitenden, der Laufnummer der Admin-Karte und der Apotheke. Die 2-Faktor-Authentifizierung wird durch das physische Innehaben der Admin-Karte sowie das Wissen eines festzulegenden PIN-Codes erreicht.

In diesem Zusammenhang ist darauf hinzuweisen, dass im Fall Österreichs als Herkunftsland die Identifizierung und Authentifizierung von Gesundheitsdiensteanbietern im Mitgliedstaat ausschließlich dessen nationalem Recht zu folgen haben. Da in diesem Fall der Sachverhalt der elektronischen Abgabe ausschließlich im Mitgliedstaat verwirklicht wird kann gemäß dem Territorialitätsprinzip kein österreichisches Recht anwendbar sein. Vielmehr kommt hier der Kreis des Vertrauens zwischen den Mitgliedstaaten zum Tragen, da auch diese den Vorgaben seitens der EU unterliegen (2-Faktor-Authentifizierung, Protokollierung auf Ebene der natürlichen Person, Informationen zur zuständigen Stelle für Identifizierung und Authentifizierung, rechtliche Zulässigkeit der Datenverarbeitung für Gesundheitsdiensteanbieter).

Zu § 24n (Rechte der Bürger/innen):

Analog zur Systematik der ELGA (§ 16) und der eHealth-Anwendung „eImpfpass" (§ 24e) sollen mit § 24n Betroffene die Möglichkeit haben, elektronisch durch einen Zugang über das Zugangsportal (§ 23) sowie bei der die Anfragen schriftlich und physisch entgegennehmenden ELGA- und eHealth-Supporteinrichtung (§ 19) als erste Anlaufstellen für Betroffene, ihre Rechte gemäß Abs. 1 Z 1 und Z 2

geltend zu machen. Insbesondere die rund um die Uhr erreichbare ELGA- und eHealth-Supporteinrichtung dient (wie schon bisher) der Erleichterung der Ausübung der Rechte der Bürger/innen. Diese Stellen sollen daher auch die Wahrnehmung der Betroffenenrechte gemäß dem Kapitel III der DSGVO erledigen, wobei deren Wahrnehmung direkt gegenüber einem oder mehreren Verantwortlichen weiterhin möglich ist. Ebenso soll das Opt-in gemäß § 24i Abs. 2 (siehe die Erläuterungen hierzu) gegenüber diesen Stellen abgegeben oder zurückgezogen werden können. Im Gegensatz zu den übrigen Betroffenenrechten der DSGVO kann das Opt-in jedoch nicht bei jedem Verantwortlichen eingebracht werden **(Abs. 1)**.

Gemäß Art 26 DSGVO hat die Aufteilung der Pflichten mittels Vereinbarung oder Rechtsvorschrift zu erfolgen. Bei der vorgeschlagenen Z 1 handelt es sich um einen Vorgriff der Pflichtenaufteilung der Verordnung. Nämlich insofern, als die Betroffenenrechte gegenüber dem für das Gesundheitswesen zuständigen Bundesminister oder der zuständigen Bundesministerin wahrzunehmen sind, denn diese betreibt die ELGA- und eHealth-Supporteinrichtung. Die Wahrnehmung der Rechte elektronisch durch einen Zugang über das Zugangsportal (§ 23) stellt eine Erleichterung für die betroffenen Personen zur Wahrnehmung ihrer Rechte dar. Es handelt sich daher um keine Einschränkung der Betroffenenrechte.

Die Regelung in **Abs. 2** knüpft an § 173 des Allgemeinen Bürgerlichen Gesetzbuchs (ABGB), JGS Nr. 946/1811, an und stellt eine Regelung zur Rechtssicherheit der Gesundheitsdiensteanbieter auf, wonach im Zweifelsfall die Rechtsausübung mündigen Minderjährigen ab Vollendung des 14. Lebensjahres (und nicht ihren Vertreter/inne/n) zusteht.

Für den Fall, dass sich eine Anfrage gemäß Abs. 1 Z 1 nicht (nur) an Verantwortliche mit Sitz in Österreich richtet, sieht **Abs. 3** vor, dass diese dennoch jedenfalls bei den Stellen des Abs. 1 eingebracht werden kann. In diesem Fall bleibt es den Betroffenen erspart, selbst den jeweiligen Verantwortlichen in einem Mitgliedstaat ausfindig machen zu müssen, insbesondere in Fällen etwaiger Sprachbarrieren.

Zu § 24o (Allgemeine Bestimmungen zum EU-Rezept):

Der Dachverband ist im übertragenen Wirkungsbereich „Gesundheit“ (GH) zur Verwendung des entsprechenden bereichsspezifischen Personenkennzeichens (bPK-GH) nicht nur berechtigt, sondern verpflichtet. Das vom Dachverband zu errichtende und zu betreibende EU-Rezept ist eine Angelegenheit der Privatwirtschaftsverwaltung, dies gilt ebenso für ELGA und MyHealth@EU sowie generell bei der Gesundheitsversorgung (siehe [ErlRV 1936 XXIV. GP, 5]) – **(Abs. 1)**.

Der Dachverband ist nach **Abs. 2** berechtigt, sowohl die in § 24k Abs. 3 aufgezählten ELGA-Komponenten, als auch das elektronische Verwaltungssystem des Dachverbands (im Folgenden: „ELSY“) gemäß § 31a Allgemeines Sozialversicherungsgesetz, BGBl. Nr. 189/1955 idF BGBl. Nr. 18/1956 in der jeweils geltenden Fassung, im übertragenen Wirkungsbereich zu verwenden. Die Verwendung der ELGA-Komponenten durch den Dachverband als Systempartner gemäß § 2 Z 11 entspricht der übrigen Systematik des GTelG 2012. Auch die Verwendung des ELSY entspricht der bereits geltenden Systematik des GTelG 2012 (z. B. § 18 Abs. 4 Z 1, Abs. 5, § 19 Abs. 2 Z 1), jedoch wird bisher nur auf Identitätsdaten sowie Daten der e-Card referenziert. Für die Erstellung des EU-Rezepts ist es jedoch unerlässlich, auf die vom Dachverband betriebene Anwendung „e-Rezept“ zuzugreifen. Der Betrieb dieser Anwendung liegt im eigenen Wirkungsbereich der Sozialversicherung und soll vom gegenständlichen Gesetzesvorhaben nicht berührt werden, weshalb sich dadurch auch keine Änderungen betreffend die Verantwortlichkeit, den Aufbau, den Betrieb oder die Haftung für die Anwendung „e-Rezept“ ergeben. Die weitere Verwendung im übertragenen Wirkungsbereich erfolgt daher nicht für Zwecke der Sozialversicherung, jedoch wird der Zweck der Erstellung des EU-Rezepts explizit in der neuen Z 10 des § 31a Abs. 4 ASVG vorgesehen. Ziel des EU-Rezepts ist die Bereitstellung von österreichischen Verschreibungen in anderen Mitgliedstaaten, unabhängig davon auf wessen Rechnung die Abgabe dieser erfolgt. Zu diesem Zwecke wird ein in Österreich nach nationalem Recht erstelltes e-Rezept und im Zeitpunkt der Ausstellung unabhängig von einer potenziellen Einlösung in einem anderen Mitgliedstaat herangezogen. Praktisch hat dies zur Folge, dass e-Rezepte für Kassen-Rezepte jedenfalls dem bestehenden, nationalen Verschreibungsprozess entsprechen, da diese bereits jetzt verpflichtend als e-Rezept auszustellen sind. Lediglich für nicht (nicht verpflichtend als e-Rezept auszustellende) Privatrezepte kann es notwendig sein, vom verschreibenden Arzt oder der verschreibenden Ärztin die Ausstellung des Privatrezept als e-Rezepts zu erbitten, sollte dies nicht bereits durch den Arzt oder die Ärztin direkt erfolgen. Das e-Rezept (sowohl als Kassenrezept als auch als Privatrezept) wird im Falle einer Einlösung in einem Mitgliedstaat ad hoc (technisch „on-the-fly“) in ein EU-Rezept umgewandelt. Für die Zwecke des zentral von der Europäischen Kommission betriebenen Semantik-Services zur Übersetzung des Arzneimittels wird neben dem Markennamen auch der bereits jetzt im e-Rezept gespeicherte Wirkstoff-Name herangezogen. National hat dies keine Auswirkung, lediglich im Falle der Einlösung als EU-Rezept wird hiefür die Wirkstoffbezeichnung herangezogen. Dies

entspricht den europäischen Vorgaben. Zur Klarstellung der Zugehörigkeit zur öffentlichen Gesundheitstelematik-Infrastruktur siehe bereits zu § 24j Abs. 1.

Zu § 24p (Österreich als Herkunftsmitgliedstaat):

Die Anfrage der Nationalen Kontaktstelle im Behandlungsmitgliedstaat wird automatisiert erstellt. Das auslösende Ereignis, welches zu einer Anfrage führt, ist immer die Einlösung einer Verordnung bei einem Gesundheitsdiensteanbieter im Behandlungsmitgliedstaat. Zum Schutz vor Missbrauch sind die in § 24l aufgezählten Möglichkeiten der Identifizierung des Bürgers oder der Bürgerin aufgezählt. Diese Identifizierung ist zwingend durchzuführen, bevor Daten zu einem EU-Rezept vom Gesundheitsdiensteanbieter eingesehen werden können. Die Ausgestaltung der rechtlichen und technischen Rahmenbedingungen für Gesundheitsdiensteanbieter obliegt jedoch dem Recht des Behandlungsmitgliedstaats. Zum Prozess der Erstellung des EU-Rezepts siehe bereits die Erläuterungen zu § 24o, zum System von MyHealth@EU zu § 24j.

Zu § 24q (Österreich als Behandlungsmitgliedstaat):

Durch **Abs. 1** wird für Apotheken gemäß § 1 Apothekengesetz, RGBl. Nr. 5/1907 in der jeweils geltenden Fassung, eine Möglichkeit geschaffen, zum Zwecke der elektronischen Abgabe von Arzneimitteln an MyHealth@EU zu partizipieren. Hierdurch erfolgt keine Einschränkung oder Erweiterung des den Apotheken gemäß § 5 Apothekengesetz vorbehaltenen Tätigkeitsbereichs oder sonstiger berufsrechtlicher Bestimmungen:

Ob ein Arzneimittel der Verschreibungspflicht in Österreich unterliegt, ergibt sich aus der auf § 1 Abs. 1 des Rezeptpflichtgesetzes, BGBl. Nr. 413/1972 in der jeweils geltenden Fassung, beruhenden Rezeptpflichtverordnung. Darüber hinaus enthält das Rezeptpflichtgesetz in § 2a ein Verbot, Arzneimittel mit verbotenen Wirkstoffen gemäß § 1 Abs. 2 Z 1 Anti-Doping-Bundesgesetz 2007 zu Zwecken des Dopings im Sport zu verschreiben und findet das Rezeptpflichtgesetz nach dessen § 7 auf Arzneimittel, die ein Suchtgift im Sinne des Suchtmittelgesetzes in der jeweils geltenden Fassung enthalten, keine Anwendung. Erhält also eine österreichische Apotheke über MyHealth@EU eine in einem anderen Mitgliedstaat ausgestellte elektronische Verschreibung eines Arzneimittels, das in Österreich nicht verschrieben werden darf, so hat die Apotheke die Einlösung dieser Verschreibung zu verweigern.

Somit ist die Erfüllung der für Apotheken geltenden, berufsrechtlichen Anforderungen gemäß dem Apothekengesetz notwendige Bedingung für deren freiwillige Teilnahme an MyHealth@EU. Sofern aber eine Teilnahme erfolgt, haben die Apotheken neben ihren berufsrechtlichen Pflichten auch die speziellen Pflichten des 2. Unterabschnitts und – soweit anwendbar – auch die Pflichten des 1. Unterabschnitts des 6. Abschnitts zu erfüllen. Im Besonderen trifft die Apotheke die Pflicht zur Meldung der elektronischen Abgabe über MyHealth@EU, wobei diese nicht verantwortlich ist für die erfolgreiche Übermittlung dieser elektronischen Abgabe in den Herkunftsmitgliedstaat.

Zum Prozesslauf der elektronischen Abgabe siehe bereits die Erläuterungen zu § 24l bezüglich der Identifizierung von Bürger/inne/n anderer Mitgliedstaaten sowie zu § 24m bezüglich der gesteigerten Identifizierungspflicht für Apotheken im Anwendungsfall des 2. Unterabschnitts. Zur Übermittlung der Daten zum EU-Rezept siehe bereits die Erläuterungen zu § 24j.

Zu § 24r (Grundsätze der Datenverarbeitung):

Die Wiederholung der Anforderungen des § 24k in **Abs. 1** dient der klaren Festschreibung der Grundsätze auch für den Anwendungsfall des EU-Rezepts. Aufgrund der gleichzeitigen Erarbeitung sowohl der allgemeinen Bestimmungen als auch des Anwendungsfalls EU-Rezept und der EU-Patientenkurzakte sind diese deckungsgleich. Bei künftigen Anwendungsfällen können weiter Vorgaben notwendig werden, welche dann in den Grundsätzen der Datenverarbeitung des jeweiligen Unterabschnitts anzuführen wären.

Zur – mittels Unionsrecht bereits geregelten und von der nationalen zu unterscheidenden – datenschutzrechtlichen Rollenverteilung auf Unionsebene siehe bereits die Erläuterungen zu § 24j Abs. 1. Abseits dieser allgemeinen und für alle Anwendungsfälle anwendbaren Rollenverteilung sieht **Abs. 2** eine spezielle Rollenverteilung für den Anwendungsfall der elektronischen Verschreibung und elektronischen Abgabe vor. Zu unterscheiden ist hier zwischen lit. a und lit. b je nach der Fallkonstellation. Im Falle Österreichs als Herkunftsmitgliedstaat erschöpft sich die Rollenverteilung in einer gemeinsamen Verantwortlichkeit des für das Gesundheitswesen zuständigen Bundesministers/der für das Gesundheitswesen zuständigen Bundesministerin als für die Infrastruktur Verantwortliche/n (§ 24j Abs. 1) und dem jeweils behandelnden Arzt oder der jeweils behandelnden Ärztin.

Im Falle Österreichs als Behandlungsmitgliedstaat ist zusätzlich zu dem für das Gesundheitswesen zuständigen Bundesministers/der für das Gesundheitswesen zuständigen Bundesministerin auch der jeweils den/die Bürger/in behandelnde, abgebende Apotheke als Verantwortliche anzusehen. Dies resultiert aus der Freiwilligkeit der Teilnahme der Apotheken sowie deren Eigenschaft als freier Beruf,

bei dessen Ausübung seitens des für das Gesundheitswesen zuständigen Bundesministers oder der zuständigen Bundesministerin keine inhaltlichen Vorgaben gemacht werden dürfen.

In beiden Fällen erfolgt die weitere Konkretisierung der Rollenverteilung mittels Verordnung des für das Gesundheitswesen zuständigen Bundesministers/der für das Gesundheitswesen zuständigen Bundesministerien, mit welcher die Anforderungen des Art. 26 DSGVO zu erfüllen sind.

Zu § 24s (Allgemeine Bestimmungen zur EU-Patientenkurzakte):

Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin hat nach **Abs. 1** eine grenzüberschreitende Anwendung zum Abruf der EU-Patientenkurzakte einzurichten und zu betreiben. Den in § 24t Abs. 2 angeführten österreichischen Gesundheitsdiensteanbietern wird der Zugang zu dieser Anwendung in einem ersten Schritt über die Plattform für Gesundheitsdiensteanbieter gemäß § 12b GTelG 2012 ermöglicht. In einem weiteren Schritt sollen auch Schnittstellen für die jeweilige Software der Gesundheitsdiensteanbieter ermöglicht werden. Die Anwendung regelt daher den Abruf der EU-Patientenkurzakte, welche von der Nationalen Kontaktstelle für digitale Gesundheit des jeweiligen Herkunftsmitgliedstaats abgerufen wird.

Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin ist nach **Abs. 2** berechtigt, die in § 24k Abs. 3 aufgezählten ELGA-Komponenten zu verwenden. Die Verwendung der ELGA-Komponenten durch den Bundesminister oder die Bundesministerin als Systempartner gemäß § 2 Z 11 entspricht der übrigen Systematik des GTelG 2012. Zur Klarstellung der Zugehörigkeit zur öffentlichen Gesundheitstelematik-Infrastruktur siehe bereits zu § 24j Abs. 1.

Zu § 24t (Österreich als Behandlungsmitgliedstaat):

Durch **Abs. 1** wird für die in § 2 Z 10 lit. a GTelG 2012 angeführten ELGA-Gesundheitsdiensteanbieter eine Möglichkeit geschaffen, zum Zwecke des Abrufs der EU-Patientenkurzakte an MyHealth@EU zu partizipieren. Hierdurch erfolgt keine Einschränkung oder Erweiterung des den Gesundheitsdiensteanbietern im jeweiligen Berufsrecht vorbehaltenen Tätigkeitsbereichs oder sonstiger berufsrechtlicher Bestimmungen:

Somit ist die Erfüllung der für die angeführten ELGA-Gesundheitsdiensteanbieter geltenden, berufsrechtlichen Anforderungen notwendige Bedingung für deren freiwillige Teilnahme an MyHealth@EU. Sofern aber eine Teilnahme erfolgt, haben die angeführten ELGA-Gesundheitsdiensteanbieter neben ihren berufsrechtlichen Pflichten auch die speziellen Pflichten des 3. Unterabschnitts und – soweit anwendbar – auch die Pflichten des 1. Unterabschnitts des 6. Abschnitts zu erfüllen.

Siehe bereits die Erläuterungen zu § 24l Abs. 3 bezüglich der Identifizierung von Bürger/inne/n anderer Mitgliedstaaten sowie zu § 24m bezüglich der gesteigerten Identifizierungspflicht für angeführten ELGA-Gesundheitsdiensteanbieter im Anwendungsfall des 3. Unterabschnitts. Zur Übermittlung der Daten zur EU-Patientenkurzakte siehe bereits die Erläuterungen zu § 24j.

Zu § 24u (Grundsätze der Datenverarbeitung):

Die Wiederholung der Anforderungen des § 24k in **Abs. 1** dient der klaren Festschreibung der Grundsätze auch für den Anwendungsfall der EU-Patientenkurzakte. Aufgrund der gleichzeitigen Erarbeitung sowohl der allgemeinen Bestimmungen als auch des Anwendungsfalls EU-Rezept und der EU-Patientenkurzakte sind diese deckungsgleich. Bei künftigen Anwendungsfällen können weiter Vorgaben notwendig werden, welche dann in den Grundsätzen der Datenverarbeitung des jeweiligen Unterabschnitts anzuführen wären.

Zur – mittels Unionsrecht bereits geregelten und von der nationalen zu unterscheidenden – datenschutzrechtlichen Rollenverteilung auf Unionsebene siehe bereits die Erläuterungen zu § 24j Abs. 1. Abseits dieser allgemeinen und für alle Anwendungsfälle anwendbaren Rollenverteilung sieht **Abs. 2** eine spezielle Rollenverteilung für den Anwendungsfall der EU-Patientenkurzakte vor. Im bislang einzig relevanten Falle Österreichs als Behandlungsmitgliedstaat erschöpft sich die Rollenverteilung in einer gemeinsamen Verantwortlichkeit des für das Gesundheitswesen zuständigen Bundesministers/der für das Gesundheitswesen zuständigen Bundesministerien als für die Infrastruktur Verantwortlichen (§ 24j Abs. 1) und dem jeweiligen angeführten ELGA-Gesundheitsdiensteanbieter. Die Verantwortlichkeit des angeführten ELGA-Gesundheitsdiensteanbieters resultiert aus der Freiwilligkeit dessen Teilnahme sowie dessen Eigenschaft als freier Beruf, bei dessen Ausübung seitens des für das Gesundheitswesen zuständigen Bundesministers oder der zuständigen Bundesministerin keine inhaltlichen Vorgaben gemacht werden dürfen.

Die Konkretisierung der Rollenverteilung erfolgt mittels Verordnung des für das Gesundheitswesen zuständigen Bundesministers/der für das Gesundheitswesen zuständigen Bundesministerien, mit welcher die Anforderungen des Art. 26 DSGVO zu erfüllen sind.

Zu Z 22 (§ 26 Abs. 19):

Diese Bestimmung soll das Inkrafttreten regeln.

Zu Z 22a (§ 28a Abs. 1 Z 3):

Es handelt sich um eine redaktionelle Anpassung.

Zu Art. 2 (Änderung des Allgemeinen Sozialversicherungsgesetzes)

Zu Z 1 (§ 31a Abs. 4 Z 10):

Die Verwendung der Anwendung „e-Rezept" als Teil der „ELSY"-Infrastruktur bedingt eine Verwendung für andere als Sozialversicherungszwecke, da die Abrechnung von österreichischen Verschreibungen bei deren Einlösung in einem anderen Mitgliedstaat mit dem jeweiligen Versicherungsträger (sofern überhaupt vorhanden) nicht Gegenstand der vorliegenden Gesetzesnovelle ist. Der neue Zweck der Erstellung von EU-Rezepten dient jedoch der sicheren Abgabe von österreichischen Verschreibungen in anderen Mitgliedstaaten, weshalb der neue Zweck als vereinbar mit den Zwecken des ELSY einzustufen ist. Die neue Z 10 zur Erstellung eines EU-Rezepts ist daher gemäß der Systematik des § 31a Abs. 4 zwar nicht notwendig, da dies auch alleine im Gesundheitstelematikgesetz 2012 erfolgen könnte, doch dient diese legistische Klarstellung auch der Rechtssicherheit sowie der Nachvollziehbarkeit für die Betroffenen. Gemäß Abs. 4 letzter Satz ASVG hat der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin dafür Sorge zu tragen, den dem Dachverband durch die Verarbeitung von Bestandteilen der ELSY entstehenden Aufwand nach Maßgabe einer vertraglichen Regelung zu vergüten.

Zu Z 2 (§ 31d Abs. 3 Z 3):

Der Betrieb des Zugangsportals soll nach geplanter Integration in das Gesundheitsportal (vgl. ErlRV 2310 BlgNR XXVII. GP, 19) nicht mehr durch den Dachverband der Sozialversicherungsträger im übertragenen Wirkungsbereich wahrgenommen werden. Aufgrund der damit einhergehenden erheblichen technischen Änderungen ist eine entsprechende Übergangsfrist notwendig. Diese Übergangsfrist soll verlängert werden.

Anlage

DATENSCHUTZ-FOLGENABSCHÄTZUNG

für die Datenverarbeitungen gemäß dem 6. Abschnitt GTelG 2012

Die folgende Datenschutz-Folgenabschätzung (DSFA) betrifft das EU-Rezept gemäß den §§ 24o ff sowie die EU-Patientenkurzakte gemäß §§ 24o ff des Gesundheitstelematikgesetzes 2012 (GTelG 2012).

Wesentlich für das Feststellen einer Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung ist die Auslegung von Art. 35 DSGVO, wie sie insbesondere durch die Art 29-Datenschutzgruppe (dem Vorgängergremium des Europäischen Datenschutzausschusses) ergangen ist (*Art-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" WP 248 Rev.01).

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 3 Buchstabe b DSGVO erforderlich, weil es zu einer Verarbeitung

- in großem Umfang (WP 248, 11),
- von sensiblen Daten sowie
- darüber hinaus Daten zu schutzbedürftigen Betroffenen, wie etwa Patient/innen (WP 248, 12)

kommt.

Außerdem ist die Datenschutz-Folgenabschätzung angezeigt, um das Risiko von erfolgreichen Schadenersatzverfahren gemäß Art. 82 DSGVO für die Verantwortlichen größtmöglich zu senken. Zwar hat der Europäische Gerichtshof im Mai 2023 festgestellt, dass die Verletzung von Bestimmungen der DSGVO für die Zuerkennung von Schadenersatz alleine nicht ausreicht und es daher unbedingt des Nachweises eines Schadens bedarf. Gleichzeitig hat er aber auch festgestellt, dass es keine Erheblichkeitsschwelle für die Geltendmachung immaterieller Schäden gibt (EuGH 4.5.2023, C-300/21 Rn. 51).

Zusammengefasst hat die vorliegenden Datenschutz-Folgenabschätzung folgendes Ergebnis gebracht:

Beschreibung	Bewertung	Risiken	Abhilfemaßnahmen	DS-Interessen
Art der Verarbeitung	festgelegter Zweck	Schäden	Minimierung	Datenschutzbeauftragter
Umfang der Verarbeitung	eindeutiger Zweck	Kontrollverlust	Pseudonymisierung	betroffene Personen
Kontext der Verarbeitung	legitimer Zwecke	Diskriminierung	Transparenz	
Zweck der Verarbeitung	Rechtmäßigkeit	Identitätsdiebstahl & -betrug	Überwachung	
personenbezogene Daten	Angemessenheit	finanzielle Verluste	Datensicherheits-maßnahmen	
Empfänger/innen	Erheblichkeit	unbef Aufhebung Pseudonymisierung		
Speicherdauer	Beschränktheit auf notwendiges Maß	Rufschädigung		
funktionelle Beschreibung	Speicherbegrenzung	Verlust Berufsgeheimnisse		
Hard- und Software	generelle Informationen	gesellschaftliche Nachteile		
Verhaltensregeln	Informationen (Art 13 DSGVO)			
	Informationen (Art 14 DSGVO)			
	Auskunft & Daten-übertragbarkeit			
	Berichtigung & Löschung			
	Widerspruch & Einschränkung			
	Auftrags-verarbeiter/innen		Legende	erfüllt
	Übermittlung in Drittländer			erfüllbar
	vorherige Konsultation			nicht erfüllt

SYSTEMATISCHE BESCHREIBUNG der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen Die Beschreibung hat nach Erwägungsgrund 90 sowie Art. 25 Abs. 7 Buchstabe a und Abs. 8 DSGVO sowie den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" der Artikel-29-Datenschutzgruppe (WP 248) zu enthalten.	
Art der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)	Die Verarbeitung erfolgt elektronisch im Rahmen einer Server-Client-Applikation. Aus Gründen der Datensicherheit gemäß Art. 32 DSGVO unterbleibt an dieser Stelle eine genaue Beschreibung der technischen Umsetzung, um potentielle Angreifer/innen nicht mit wertvollen Informationen über potentielle Schwachstellen (*Art-29-Datenschutzgruppe*, WP 248 Rev.01, 8) zu versorgen. Gemeinsam Verantwortliche im Sinne des Art. 4 Nr. 7 in Verbindung mit Art. 26 DSGVO sind Im Falle des EU-Rezepts: der für das Gesundheitswesen Bundesminister oder die zuständige Bundesministerin, die Apotheken (§ 24r Abs. 2 GTelG 2012). Im Falle der EU-Patientenkurzakte: der für das Gesundheitswesen Bundesminister oder die zuständige Bundesministerin, sowie der jeweils behandelnde Gesundheitsdiensteanbieter (§ 24u Abs. 2 GTelG 2012) **Die Anforderung "Beschreibung der Art der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Umfang der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)	Das EU-Rezept umfasst potenziell alle Personen, die mit dem österreichischen Gesundheitswesen – egal in welcher Rolle – in Berührung kommen. Es werden Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) und die erforderlichen Identitäts- bzw. Metadaten jener natürlichen Personen verarbeitet, die Im Patientenindex gemäß § 18 GTelG 2012 erfasst sind und somit jedenfalls jener Personen, die in den Datenverarbeitungen des Dachverbandes oder dem Ergänzungsregister gemäß § 6 Abs. 4 E-GovG erfasst sind, sowie Personen für die in ihrem Herkunftsland eine Verschreibung ausgestellt wurde, welche in Österreich im Rahmen des EU-Rezepts zu den vom jeweiligen Herkunftsstaat festgelegten Bedingungen einlöst werden sollen. Die EU-Patientenkurzakte umfasst potenziell alle Personen, für die in ihrem Herkunftsland eine Patientenkurzakte erstellt wurde, welche in Österreich im Rahmen der EU-Patientenkurzakte zu den vom jeweiligen Herkunftsstaat festgelegten Bedingungen lesend abgerufen werden soll. In inhaltlicher Sicht umfasst die gegenständliche Verarbeitung sämtliche Daten, die in den zentralen ELGA-Komponenten gemäß § 24k Abs. 3 GTelG 2012 aufgezählt sind sowie (im Falle des EU-Rezepts) Daten der Anwendung „e-Rezept" im elektronischen Verwaltungssystem des Dachverbands gemäß § 31a Abs. 4 Z 10 ASVG verarbeitet werden (siehe näher dazu, unten Feld „BESCHREIBUNG / Personenbezogene Daten"). In geografischer Sicht umfassen die Anwendungen das gesamte Gebiet der Europäischen Union. Sie stellen bereits aufgrund des geographischen

	Ausmaßes einen großen Umfang im Sinne der Art-29-Datenschutzgruppe (WP 248, 11) dar. Dies ist jedoch darauf beschränkt, dass ein Bürger oder eine Bürgerin tatsächlich die Einlösung eines österreichischen EU-Rezepts oder den Abruf der EU-Patientenkurzakte in einem Behandlungsmitgliedstaat anstößt, andernfalls keine (vor allem grenzüberschreitende) Datenverarbeitung erfolgt. **Die Anforderung "Beschreibung des Umfangs der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Kontext der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)	Die Verarbeitung erfolgt im Kontext der Zwecke des Art. 9 Abs. 2 Buchstabe g bis j DSGVO, genauer gesagt der grenzüberschreitenden Gesundheitsversorgung (zur rechtlichen Begründung – siehe unten: Feld „BEWERTUNG / Rechtsgrundlage"). Mit dem vorgeschlagenen Abschnitt 5 soll die grenzüberschreitende Gesundheitsversorgung eingeführt werden, die ein erhebliches öffentliches Interesse gemäß Art. 9 Abs. 2 Buchstaben g bis j DSGVO erfüllt. **Die Anforderung "Beschreibung des Kontexts der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Zweck der Verarbeitung (EG 90 sowie Art. 35 Abs. 7 Buchstabe a DSGVO; WP 248 Rev.01, 21 und 28)	Die Verarbeitung dient der grenzüberschreitenden Gesundheitsversorgung, die u.a. den freien Personenverkehr fördert, in dem die medizinische Versorgung im EU-Ausland erleichtert wird. Durch die Teilnahme an der MyHealth@EU-Infrastruktur sowie die Semantik-Services, werden vor allem Übersetzungs- und Kommunikationsfehler, die im grenzüberschreitenden Verkehr noch häufiger sind, vermieden, insbesondere im Vergleich zum aktuellen Prozess der Papierrezepte (Sprachbarrieren, Gefahr der Mehrfach-Abgabe, etc.). Außerdem hilft das EU-Rezept Kosten zu sparen, weil nicht vor Ort neue Rezepte ausgestellt werden müssen, sondern die „originalen" Rezepte unmittelbar eingelöst werden können. Im Falle der EU-Patientenkurzakte kann der für die Anamnese notwendige Zeit- und Personalaufwand drastisch reduziert werden. Die Steigerung der Prozess- und Ergebnisqualität von grenzüberschreitenden Gesundheitsdienstleistungen wird damit ebenso ermöglicht, wie eine verbesserte Behandlungskontinuität sowie integrierte Versorgung über die Landesgrenzen hinweg. Dass Verarbeitungen auch mehreren Zwecken gleichzeitig dienen, ist in Übereinstimmung mit der Datenschutz-Grundverordnung (Erwägungsgrund 32 DSGVO). **Die Anforderung "Beschreibung des Zwecks der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Personenbezogene Daten (WP 248 Rev.01, 21 und 28)	Die im Rahmen der Verarbeitungstätigkeit „EU-Rezept" verarbeiteten Daten umfassen: **Medikationsdaten**, d.h. Daten zu Verschreibungen und Abgaben von verschreibungspflichtigen und nicht verschreibungspflichtigen Arzneimitteln (§ 31a ASVG, insbesondere dessen Abs. 1 [bezüglich der Versicherten verschriebenen Heilmittel] in Verbindung mit dessen Abs. 4 Z 10 [bezüglich der Nichtversicherten verschriebenen Heilmittel] sowie § 2 Z 9 lit. b GTelG 2012); **Identitätsdaten**, d.h. Daten zur Identifikation der betroffenen Personen gemäß § 24k Abs. 3 Z 1 und 2 in Verbindung mit § 18 Abs. 2 GTelG 2012, d.h.: Namensangaben (Vorname[n], Familienname, Geburtsname, akademische Grade), Personenmerkmale (Geburtsdatum, Geburtsort [soweit verfügbar], Geschlecht, Sterbedatum [soweit verfügbar], Staatsangehörigkeit), Adressdaten, Identitätsdaten (Sozialversicherungsnummer, lokale Patient/inn/en/kennungen, bPK-GH, ID Austria); **Metadaten**, d.h. insbesondere Berechtigungsdaten sowie Protokollierungsdaten (§ 24k Abs. 3 Z 3 und 4 in Verbindung mit §§ 21 und 22 GTelG 2012), die zwar keine personenbezogenen Daten darstellen, aber der Vollständigkeit halber angeführt werden. Die im Rahmen der Verarbeitungstätigkeit „EU-Patientenkurzakte" verarbeiteten Daten umfassen jene Daten, welche im jeweiligen

	Herkunftsmitgliedstaat gemäß deren Vorgaben in der EU-Patientenkurzakte verarbeitet werden. Entsprechend den Umsetzungsrichtlinien des zugrundeliegenden EU-Projekts kann es sich hierbei maximal um die folgenden Datenarten handeln: 1. Angaben zur natürlichen Person (inklusive Identitätsdaten, Kontaktdaten, Angaben zur Versicherung), 2. Allergien, 3. Medizinische Warnungen, 4. Informationen über Impfungen/Prophylaxen, gegebenenfalls in Form eines Impfausweises, 5. Medizinische Probleme (aktuelle, gelöste, abgeschlossene oder inaktive Probleme, auch in einer internationalen Kodierung zur Klassifizierung), 6. Informationen in Textform zur medizinischen Vorgeschichte, 7. Medizinprodukte und Implantate, 8. Medizinische Verfahren oder Pflegeverfahren, 9. Funktionszustand, 10 Derzeitige und frühere Medikation, 11. Gesundheitsrelevante Beobachtungen zum sozialen Hintergrund (Konsum von Alkohol, Tabak, etc.), 12. Schwangerschaftshistorie, 13. von der natürlichen Person selbst zur Verfügung gestellte Daten, 14. Beobachteter Gesundheitszustand, 15. der aktuelle Versorgungsplan, 16. Angaben zu seltenen Krankheiten (zum Beispiel Einzelheiten über die Auswirkungen oder Merkmale der Krankheit, etc.) und 17. Ergebnisse von Untersuchungen. Der Umfang der Datenarten und deren Befüllungsgrad hängt daher im jeweiligen Einzelfall davon ab, welche Datenarten generell vom jeweiligen Herkunftsmitgliedstaat vorgegeben werden, und welche dieser Daten in der EU-Patientenkurzakte der jeweiligen Person tatsächlich befüllt sind. **Die Anforderung "Beschreibung der personenbezogenen Daten" ist aufgrund der gesetzlichen Determinierung im Gesundheitstelematikgesetz 2012, insbesondere dessen 4. und 5. Abschnitt, als erfüllt anzusehen.**
Empfänger/innen (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)	Die zulässigen Empfänger/innen sind: Im Fall des EU-Rezepts: **Gesundheitsdiensteanbieter** gemäß § 2 Z 2 GTelG 2012 (§ 24k Abs. 2 Z 1 lit. b GTelG 2012); **Apotheken** gemäß § 1 des Apothekengesetzes, RGBl. Nr. 5/1907 (§ 24r Abs. 2 Z 2 lit. b GTelG 2012); der für das **Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin** als Nationale Kontaktstelle für digitale Gesundheit gemäß § 24j GTelG 2012 (§ 24r Abs. 2 Z 1 lit. a sowie Z 2 lit. a GTelG 2012) bzw. ELGA- und eHealth-Supporteinrichtung gemäß § 17 GTelG 2012 (§ 24k Abs. 2 Z 2 lit. c GTelG 2012); der **Dachverband der österreichischen Sozialversicherungsträger** gemäß § 30 ASVG (§ 24r Abs. 2 GTelG 2012); **gesetzliche und bevollmächtigte Vertreter/innen der Bürger/innen** (§ 24k Abs. 2 Z 2 lit. b GTelG 2012);

	von den Verantwortlichen gegebenenfalls herangezogene **Auftragsverarbeiter/innen** gemäß Art. 28 DSGVO. Im Fall der EU-Patientenkurzakte: **Gesundheitsdiensteanbieter** gemäß § 2 Z 10 lit. a und b GTelG 2012 (§ 24k Abs. 2 lit. b GTelG 2012); der für das **Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin** als Nationale Kontaktstelle für digitale Gesundheit gemäß § 24j GTelG 2012 (§ 24r Abs. 2 Z 1 lit. a sowie Z 2 lit. a GTelG 2012) bzw. ELGA- und eHealth-Supporteinrichtung gemäß § 17 GTelG 2012 (§ 24k Abs. 2 Z 2 lit. c GTelG 2012); von den Verantwortlichen gegebenenfalls herangezogene **Auftragsverarbeiter/innen** gemäß Art. 28 DSGVO. **Die Anforderung "Beschreibung der Empfänger/innen" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Speicherdauer (WP 248 Rev.01, 21 und 28)	Vorweg ist festzuhalten, dass aufgrund der Reduktion der Verarbeitung auf die Weiterleitung („Kommunikation") der Medikationsdaten gemäß § 24j Abs. 2 GTelG 2012 keine Gesundheitsdaten bei der Nationalen Kontaktstelle gespeichert werden, sondern nur Protokollierungsdaten. Für diese gilt auch die in § 24j Abs. 3 GTelG 2012 vorgesehene Löschfrist. Eine Mindestspeicherdauer ist gesetzlich nicht vorgesehen. Die Löschfrist – bei der Nationalen Kontaktstelle – beträgt gemäß § 24j Abs. 3 GTelG 2012 10 Jahre. Die Frist beginnt nach Abschluss der Verarbeitung zu laufen, also sobald das EU-Rezept im Ausland erfolgreich eingelöst und die elektronische Abgabe erfolgreich rückübermittelt wurde, oder sobald die Abgabe durch eine österreichische Apotheke erfolgreich in den Herkunftsmitgliedstaat übermittelt wurde. Im Falle der EU-Patientenkurzakte beginnt die Frist ab Abruf der EU-Patientenkurzakte aus dem Herkunftsland der jeweiligen Person durch den Gesundheitsdiensteanbieter. Die Löschpflicht des § 24j Abs. 3 GTelG 2012 sorgt also dafür, dass die Nationalen Kontaktstellen nicht zu Datenfriedhöfen werden. Sollten Daten zu einem späteren Zeitpunkt – aufgrund einer neuerlichen Anforderung einer Nationalen Kontaktstelle eines anderen Mitgliedstaates – wieder benötigt werden, dürfen die erforderlichen Daten (siehe oben: Feld „SYSTEMATISCHE BESCHREIBUNG / Personenbezogene Daten") erneut angefordert werden. **Die Anforderung "Beschreibung der Speicherdauer" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Funktionelle Beschreibung der Verarbeitungsvorgänge (WP 248 Rev.01, 21 und 28)	Die Verarbeitungstätigkeit „EU-Rezept" umfasst folgende Funktionen: <u>Verschreibung eines österreichischen ELGA-GDA in e-Rezept speichern:</u> Im Zuge einer ärztlichen Behandlung in Österreich werden für alle ELGA-Teilnehmer/innen, die nicht gemäß § 16 Abs. 2 Z 2 GTelG 2012 situativ widersprochen haben, Verschreibungen von Arzneimitteln, d.h. Medikationsdaten im Sinne des § 2 Z 9 lit. b GTelG 2012, gespeichert (§ 13 Abs. 3 Z 4 GTelG 2012). Die Speicherung erfolgt zentral im Informationssystem „e-Rezept", das vom Dachverband im übertragenen Wirkungsbereich betrieben wird. Diese Funktion stellt für sich alleine betrachtet keine grenzüberschreitende Bereitstellung von Medikationsdaten (§ 2 Z 9 lit. b GTelG 2012) dar, ist aber eine conditio sine qua non für bestimmte Fälle der grenzüberschreitenden Gesundheitsversorgung, wenn nämlich in Österreich verschriebene Arzneimittel in anderen Mitgliedstaaten abgegeben werden sollen. Über die Ermächtigung des Dachverbandes zur Heranziehung der ELGA-Komponenten gemäß § 24k Abs. 3 GTelG 2012 in § 24o Abs. 2 GTelG 2012 ist die gegenständliche Funktion als Bestandteil

	der gegenständlichen Verarbeitungstätigkeit festgelegt. Verschreibung einer österreichischen ELGA-GDA/in für die Abgabe in anderem Mitgliedstaat bereitstellen: Soll die Abgabe von in Österreich verschriebenen Arzneimitteln in anderen Mitgliedstaaten erfolgen, fordert die Nationale Kontaktstelle des anderen Mitgliedstaats bei der österreichischen Nationalen Kontaktstelle die Bereitstellung der entsprechenden Verschreibungen an. Die österreichische Nationale Kontaktstelle leitet diese Anforderung – technisch oder organisatorisch – an den Dachverband als Betreiber des Informationssystems ELSY, und damit der Anwendung „e-Rezept", weiter und stellt die vom Dachverband bereitgestellten Verschreibungen der anfordernden Nationalen Kontaktstelle des anderen Mitgliedstaats bereit, die diese Verschreibungen wiederum den behandelnden Gesundheitsdienstleistern (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU), wie etwa Apotheken, in ihrem Mitgliedstaat für Zwecke der grenzüberschreitenden Gesundheitsversorgung bereitstellt. Verschreibung einer Gesundheitsdienstleister/in eines anderen Mitglied-staats für die Abgabe in Österreich bereitstellen: Soll die Abgabe von in anderen Mitgliedstaaten verschriebenen Arzneimitteln in Österreich erfolgen, so fordert die ELGA-Gesundheitsdiensteanbieter/in (§ 2 Z 10 GTelG 2012), die die Arzneimittel abgeben will, die Verschreibung aus dem anderen Mitgliedstaat an und erhält diese im Wege der Nationalen Kontaktstellen von Österreich bzw. des anderen Mitgliedstaats. Abgabe in Österreich für anderen Mitgliedstaat bereitstellen: Nach Abgabe von Arzneimitteln durch eine ELGA-Gesundheitsdiensteanbieter/in in Österreich wird die Abgabe der verschriebenen Arzneimittel im Wege der Nationalen Kontaktstellen von Österreich bzw. des anderen Mitgliedstaats der entsprechenden Anwendung des anderen Mitgliedstaats bereitgestellt. Die Verarbeitungstätigkeit „EU-Patientenkurzakte" umfasst folgende Funktionen: Abruf der EU-Patientenkurzakte: Soll im Zuge einer ärztlichen Behandlung in Österreich die EU-Patientenkurzakte einer Person durch einen Gesundheitsdiensteanbieter abgerufen werden, fordert die österreichische Nationale Kontaktstelle die EU-Patientenkurzakte bei der Nationalen Kontaktstelle des anderen Mitgliedstaats an. Die Nationale Kontaktstelle leitetet sodann die erhaltene EU-Patientenkurzakte der Person an den behandelnden Gesundheitsdiensteanbieter weiter, welcher einen lesenden Zugriff auf diese erhält. **Die Anforderung "Funktionelle Beschreibung der Verarbeitungsvorgänge" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Beschreibung der Hard- und Software bzw. sonstigen Infrastruktur (WP 248 Rev.01, 21 und 28)	Da die Verarbeitungstätigkeiten „EU-Rezept" und „EU-Patientenkurzakte noch einzurichten ist, sind hinsichtlich der genauen Beschreibung der Infrastruktur noch allfällige Ausschreibungen abzuwarten. **Die Anforderung "Beschreibung der Hard- und Software bzw. sonstigen Infrastruktur" ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.**
Eingehaltene, gemäß Art. 40 DSGVO genehmigte Verhaltensregeln (Art. 35 Abs. 8 DSGVO; WP 248 Rev.01, 21 und 28)	Das Instrument der Verhaltensregeln ist für Behörden und öffentliche Stellen nicht anwendbar (Art. 41 Abs. 6 DSGVO bzw. mwN *Schweinoch/Will* in *Ehmann/Selmayr*, DSGVO[2] Art. 40 Rn. 10). **Die Anforderung "Beschreibung der eingehaltenen, gemäß Art 40 genehmigten Verhaltensregeln" ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.**
BEWERTUNG	

der Notwendigkeit und Verhältnismäßigkeit *Die Bewertung hat nach Erwägungsgründen 90 und 96, Art. 35 Abs. 7 Buchstaben b und d DSGVO sowie den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" (WP 248) auf Maßnahmen* *– betreffend Notwendigkeit und Verhältnismäßigkeit (Art. 5 und 6 DSGVO) sowie* *– zur Stärkung der Rechte der betroffenen Personen (Art. 12 bis 21, 28, 36 und Kapitel V DSGVO) abzustellen.*	
Festgelegter Zweck (EG 90 und Art. 35 Abs. 7 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)	Die Zwecke der Verarbeitung sind in § 24i Abs. 1 GTelG 2012 sowie § 24k Abs. 2 GTelG 2012 wie folgt festgelegt: die Sicherstellung der Kontinuität der grenzüberschreitenden Gesundheitsversorgung durch eine verbesserte, schnellere Verfügbarkeit medizinischer Informationen, die zu einer Qualitätssteigerung diagnostischer und therapeutischer Entscheidungen sowie der Behandlung und Betreuung führt, die Erhöhung der Patient/innensicherheit in der grenzüberschreitenden Gesundheitsversorgung, die Steigerung der Prozess- und Ergebnisqualität von Gesundheitsdienstleistungen in der grenzüberschreitenden Gesundheitsversorgung, die Aufrechterhaltung einer qualitativ hochwertigen, ausgewogenen und allgemein zugänglichen grenzüberschreitenden Gesundheitsversorgung sowie der Stärkung der Patient/innenrechte, insbesondere in Bezug auf die Verfügbarkeit ihrer elektronischen Gesundheitsdaten und ihre Kontrolle über diese Daten in der grenzüberschreitenden Gesundheitsversorgung. **Die Anforderung "Bewertung der Festlegung des Zwecks" ist aufgrund der ausdrücklichen, gesetzlichen Festlegung der Zwecke in § 24i Abs. 1 GTelG 2012 sowie § 24k Abs. 2 GTelG 2012 als erfüllt anzusehen.**
Eindeutiger Zweck (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)	Die Zwecke sind in § 24i Abs. 1 GTelG 2012 sowie § 24k Abs. 2 GTelG 2012 eindeutig festgelegt. In Zusammenschau mit den noch zu veröffentlichenden Datenschutzerklärungen, Vereinbarungen gemäß Art. 26 DSGVO sowie der Verordnung gemäß § 24r Abs. 2 und § 24u Abs. 2 bzw. § 28c GTelG 2012 können betroffene Personen vorhersehen, wie ihre Daten verarbeitet werden. **Die Anforderung "Bewertung der Eindeutigkeit des Zwecks" ist aufgrund der ausdrücklichen, gesetzlichen Festlegung der Zwecke in § 24i Abs. 1 GTelG 2012 sowie § 24k Abs. 2 GTelG 2012 als erfüllt anzusehen.**
Legitimer Zweck (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)	Die eindeutig festgelegten Zwecke sind zudem legitim. Dies zeigt sich bereits auf unionsrechtlicher Ebene: Danach steht gemäß Art. 168 Abs. 7 AEUV die Verantwortung für die Festlegung ihrer Gesundheitspolitik sowie für die Organisation des Gesundheitswesens und der medizinischen Versorgung den Mitgliedstaaten zu. Dies umfasst auch die Verwaltung des Gesundheitswesens und der medizinischen Versorgung sowie die Zuweisung der dafür bereitgestellten Mittel. Auf verfassungsrechtlicher Ebene ergibt sich die Legitimität der Zwecke vor allem aus Art. 10 Abs. 1 Z 12 B-VG, wonach dem Bund die – grundsätzliche – Kompetenz im Gesundheitswesen zukommt. Es gibt somit einen klaren verfassungsrechtlichen Gestaltungsauftrag hinsichtlich des Gesundheitswesens. **Die Anforderung "Bewertung der Legitimität des Zwecks" ist aufgrund des Art. 168 Abs. 7 AEUV, des Art. 10 Abs. 1 Z 12 B-VG, der umfangreichen, ausdrücklichen, gesetzlichen Regelung zur Gesundheitsversorgung in Österreich sowie im Lichte der einschlägigen EuGH- und VfGH-Judikatur, als erfüllt anzusehen.**
Rechtmäßigkeit der Verarbeitung	Die Rechtmäßigkeit der Verarbeitung ergibt sich aus Art. 9 Abs. 2

(Art. 35 Abs. 7 Buchstabe b iVm Art. 6 und 9 DSGVO; WP 248 Rev.01, 21 und 28)	Buchstaben h und i DSGVO, weil die Verarbeitung für die grenzüberschreitende Gesundheitsversorgung erforderlich ist. Die in § 24i Abs. 2 GTelG 2012 verlangte Freiwilligkeit ist keine Einwilligung im Sinne des Art. 9 Abs. 2 Buchstabe a DSGVO, sondern eine zusätzliche Maßnahme mit der sichergestellt werden soll, dass sich die Patient/innen der Konsequenzen ihrer Handlungen bewusst sind. Rechtsgrundlage der grenzüberschreitenden Gesundheitsversorgung sind auf unionsrechtlicher Ebene vor allem Art. 168 und 114 AEUV, die Bestimmungen der Patientenmobilitätsrichtlinie 2011/24/EU sowie Art. 9 Abs. 2 Buchstaben h und i DSGVO. Dabei handelt es sich um eine Aufgabe, die zu einem „*funktionierenden Gesundheitswesen*“ beiträgt, d.h. im wichtigen öffentlichen Interesse liegt (VfSlg. 20.556/2022). **Die Anforderung “Bewertung der Rechtmäßigkeit der Verarbeitung” ist somit, insbesondere aufgrund der in Art. 9 Abs. 2 DSGVO enthaltenen Erlaubnistatbestände zur Gesundheitsversorgung sowie im Lichte der einschlägigen VfGH-Judikatur, als erfüllt anzusehen.**
Angemessenheit der Verarbeitung (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe c DSGVO; WP 248 Rev.01, 21 und 28)	Die Verarbeitung ist vor allem deswegen angemessen, weil die Verarbeitung der grenzüberschreitenden Gesundheitsversorgung dient und damit im wichtigen öffentlichen Interesse liegt (siehe oben: Feld „BEWERTUNG / Rechtmäßigkeit der Verarbeitung“). Außerdem dürfen Daten (siehe oben Feld „SYSTEMATISCHE BESCHREIBUNG / Personenbezogene Daten“) nur verarbeitet werden, wenn es die Behandlung oder Ausübung der Rechte der betroffenen Personen erfordert (§ 24k Abs. 2 GTelG 2012). Die Initiative geht auch in allen Fällen von den betroffenen Personen aus: entweder suchen sie ELGA-Gesundheitsdiensteanbieter/innen (in Österreich) oder Gesundheitsdienstleister gemäß Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie (in anderen Mitgliedstaaten) auf, um behandelt zu werden oder wenden sich an die ELGA- und eHealth-Supporteinrichtung bzw. rufen das Zugangsportal auf, um ihre Rechte wahrzunehmen. In beiden Fällen ist die Verarbeitung ihrer personenbezogenen Daten erforderlich, um ihren eigenen Wünschen entsprechen zu können. Was aber von den betroffenen Personen selbst verlangt wird, hat – nach dem Prinzip „volenti non fit iniuria“ – zumindest die Vermutung der Angemessenheit für sich (vgl. Schlussanträge zu C-693/22 Rn 65 bzw. C-667/21 Rn 102; VfSlg. 3424/1958). **Die Anforderung “Bewertung der Angemessenheit der Verarbeitung” ist insbesondere aufgrund des gesetzlich verpflichtenden Einsatzes von bereichsspezifischen Personenkennzeichen sowie des strafrechtlichen Schutzes vor Missbrauch, als erfüllt anzusehen.**
Erheblichkeit der Verarbeitung (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe c DSGVO; WP 248 Rev.01, 21 und 28)	Die Verarbeitung ist erheblich, weil die vorgesehene Verarbeitung conditio sine qua non für eine grenzüberschreitende Gesundheitsversorgung ist. Dabei handelt es sich um eine Aufgabe, die zu einem „*funktionierenden Gesundheitswesen*“ beiträgt, d.h. im wichtigen öffentlichen Interesse liegt (VfSlg. 20.556/2022). **Die Anforderung “Bewertung der Erheblichkeit der Verarbeitung” ist als erfüllt anzusehen, weil die Verarbeitungstätigkeit conditio sine qua non für eine grenzüberschreitende Gesundheitsversorgung ist.**
Beschränktheit der Verarbeitung auf das notwendige Maß (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe c DSGVO; WP 248 Rev.01, 21 und 28)	Die bloße Weiterleitung der Gesundheitsdaten an Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie) in anderen Mitgliedstaaten für Zwecke der grenzüberschreitenden Gesundheitsversorgung ist als auf das notwendige Maß beschränkt anzusehen (siehe oben auf Feld „BEWERTUNG / Erheblichkeit der Verarbeitung“), weil durch die Reduktion der Verarbeitung auf die Weiterleitung („Kommunikation“) der Medikationsdaten (EU-Rezepts) bzw. anderer relevanter Gesundheitsdaten (EU-Patientenkurzakte) gemäß § 24j Abs. 2 GTelG 2012 keine Gesundheitsdaten bei der Nationalen Kontaktstelle gespeichert werden, sondern nur Protokollierungsdaten. Für diese gilt auch die in § 24j Abs. 3 GTelG 2012 vorgesehene Löschfrist.

	Die Anforderung "Bewertung der Beschränktheit der Verarbeitung auf das notwendige Maß" ist als erfüllt anzusehen, insbesondere weil es zu keiner doppelten bzw. mehrfachen Speicherung der Daten – und damit einer Verarbeitung über das notwendige Maß hinaus – kommt.
Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe e DSGVO; WP 248 Rev.01, 21 und 28)	Wie bereits oben im Feld „SYSTEMATISCHE BESCHREIBUNG / Speicherdauer" ausgeführt, ist die Löschfrist in § 24j Abs. 3 GTelG 2012 so angegeben, dass die über die Nationale Kontaktstelle ausgetauschten Daten spätestens 10 Jahre nach Abschluss der Verarbeitung, also im Falle des EU-Rezepts nachdem die elektronische Abgabe an die Nationale Kontaktstelle für digitale Gesundheit im Behandlungsmitgliedstaat übermittelt oder von dieser erhalten wurde bzw. im Falle der EU-Patientenkurzakte nachdem die EU-Patientenkurzakte aus dem Herkunftsland der Person durch die Nationale Kontaktstelle abgerufen und vom behandelnden Gesundheitsdiensteanbieter erhalten wurde, zu löschen sind. **Durch diese ausdrückliche Löschpflicht ist die Anforderung "Bewertung der Speicherbegrenzung" als erfüllt anzusehen, weil Maßnahmen zur Begrenzung der Speicherdauer gesetzlich vorgeschrieben sind.**
Generelle Information der betroffenen Personen (Art. 12 DSGVO; WP 248 Rev.01, 21 und 28)	Eine Datenschutzerklärung ist für die gegenständliche Verarbeitung in Ausarbeitung und wird als Patient Information Notice (PIN) den Bürger/innen zur Verfügung gestellt werden. **Die Anforderung "Bewertung der Information der betroffenen Personen bei Erhebung" ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.**
Information der betroffenen Personen bei Erhebung (Art. 13 DSGVO; WP 248 Rev.01, 21 und 28)	Eine Datenschutzerklärung liegt für die gegenständliche Verarbeitung noch nicht vor. Zur Einhaltung der klaren und einfachen Sprache – siehe oben: Feld „BEWERTUNG / Generelle Informationen der betroffenen Personen". **Die Anforderung "Bewertung der Information der betroffenen Personen bei Erhebung" ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.**
Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden (Art. 14 DSGVO; WP 248 Rev.01, 21 und 28)	Siehe oben: Feld „BEWERTUNG / Information der betroffenen Personen bei Erhebung". **Die Anforderung "Bewertung der Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden" ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.**
Auskunftsrecht der betroffenen Personen und Recht auf Datenübertragbarkeit (Art. 15 und 20 DSGVO; WP 248 Rev.01, 21 und 28)	Das Recht auf Auskunft kann elektronisch durch einen Zugang über das des Zugangsportals (§ 23 GTelG 2012) oder postalisch, physisch sowie elektronisch gegenüber der ELGA- und eHealth-Supporteinrichtung (§ 17 GTelG 2012) wahrgenommen werden. Elektronisch kann das Auskunftsrecht jederzeit, weltweit durch Einloggen mit der E-ID (ID Austria) und Aufruf der Seite https://www.elga-online.gv.at/web-gui/protected/protokolle.xhtml wahrgenommen werden. Bei der ELGA- und eHealth-Supporteinrichtung kann das Auskunftsrecht physisch an den unter https://www.gesundheit.gv.at/gesundheitsleistungen/elga/elga-ombudsstelle.html angegeben Standorten während der angeführten Öffnungszeiten wahrgenommen werden. Voraussetzung ist der Identitätsnachweis mittels amtlichem Lichtbildausweis sowie eine dokumentierte Vollmacht zur Wahrnehmung dieses Rechts gemäß Kapitel III DSGVO. Das Recht auf Datenübertragbarkeit steht gemäß Art. 20 Abs. 1 Buchstabe a DSGVO nicht zu, weil die Verarbeitung weder aufgrund einer Einwilligung (Art. 6 Abs. 1 Buchstabe a oder Art. 9 Abs. 2 Buchstabe a DSGVO) noch aufgrund eines Vertrags (Art. 6 Abs. 1 Buchstabe b DSGVO), sondern aufgrund des Rechts eines Mitgliedstaats, nämlich des Gesundheitstelematikgesetzes 2012 erfolgt. **Die Anforderung "Bewertung des Auskunftsrechts der betroffenen Personen und ihres Rechts auf Datenübertragbarkeit" ist aufgrund der elektronischen und physischen Infrastruktur, insbesondere des**

	Zugangsportals (§ 23 GTelG 2012) sowie der ELGA- und eHealth-Supporteinrichtung (§ 17 GTelG 2012), als erfüllt anzusehen.
Recht auf Berichtigung und Löschung (Art. 16, 17 und 19, WP 248 Rev.01, 21 und 28)	Das Recht auf Berichtigung kann postalisch, physisch sowie elektronische gegenüber der ELGA- und eHealth-Supporteinrichtung (§ 17 GTelG 2012) wahrgenommen werden. Bei der ELGA- und eHealth-Supporteinrichtung kann das Recht auf Berichtigung physisch an den unter https://www.gesundheit.gv.at/gesundheitsleistungen/elga/elga-ombudsstelle.html angegeben Standorten während der angeführten Öffnungszeiten wahrgenommen werden. Voraussetzung ist der Identitätsnachweis mittels amtlichem Lichtbildausweis sowie eine dokumentierte Vollmacht zur Wahrnehmung dieses Rechts gemäß Kapitel III DSGVO. Das Recht auf Löschung steht gemäß Art. 17 Abs. 3 Buchstabe b DSGVO nicht zu, weil die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der – zumindest die innerstaatlichen – Verantwortlichen unterliegen, erforderlich ist. Die *rechtlichen Verpflichtungen nach dem Recht eines Mitgliedstaats* sind die Bestimmungen des 6. Abschnitts des Gesundheitstelematikgesetzes 2012 über die grenzüberschreitende Gesundheitsversorgung. **Die Anforderung "Bewertung des Rechts auf Berichtigung und Löschung" ist aufgrund der elektronischen und physischen Infrastruktur, insbesondere des Zugangsportals (§ 23 GTelG 2012) sowie der ELGA- und eHealth-Supporteinrichtung (§ 17 GTelG 2012), als erfüllt anzusehen.**
Widerspruchsrecht und Recht auf Einschränkung der Verarbeitung (Art. 18, 19 und 21; WP 248 Rev.01, 21 und 28)	Das Widerspruchsrecht steht nicht zu, weil die Verarbeitung weder aufgrund öffentlicher Interessen (Art. 6 Abs. 1 Buchstabe e DSGVO) noch aufgrund berechtigter Interessen (Art. 6 Abs. 1 Buchstabe f DSGVO) noch zu Zwecken der Direktwerbung oder der Statistik erfolgt. Die Verarbeitung erfolgt – wie oben in Feld „BEWERTUNG / Rechtmäßigkeit der Verarbeitung" näher ausgeführt – aufgrund von Art. 9 Abs. 2 Buchstaben g, h und i DSGVO, d.h. ist aufgrund *„des Rechts eines Mitgliedstaats [...] aus Gründen eines erheblichen öffentlichen Interesses erforderlich"*, *„für [...] die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich [...] erforderlich"* oder *„aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit [...] erforderlich"*. Das Recht auf Einschränkung der Verarbeitung kann postalisch, physisch sowie elektronisch gegenüber der ELGA- und eHealth-Supporteinrichtung (§ 17 GTelG 2012) wahrgenommen werden. Bei der ELGA- und eHealth-Supporteinrichtung kann das Recht auf Berichtigung physisch an den unter https://www.gesundheit.gv.at/gesundheitsleistungen/elga/elga-ombudsstelle.html angegeben Standorten während der angeführten Öffnungszeiten wahrgenommen werden. Voraussetzung ist der Identitätsnachweis mittels amtlichem Lichtbildausweis sowie eine dokumentierte Vollmacht zur Wahrnehmung dieses Rechts gemäß Kapitel III DSGVO. **Die Anforderung "Bewertung des Widerspruchsrechts und des Rechts auf Einschränkung der Verarbeitung" ist aufgrund der elektronischen und physischen Infrastruktur, insbesondere des Zugangsportals (§ 23 GTelG 2012) sowie der ELGA- und eHealth-Supporteinrichtung (§ 17 GTelG 2012), als erfüllt anzusehen.**
Verhältnis zu Auftragsverarbeiter/innen (Art. 28 DSGVO; WP 248 Rev.01, 21 und 28)	Da das EU-Rezept noch umzusetzen bzw. zu errichten ist und zwar Anfang 2026 (siehe: Allgemeiner Teil der Erläuterungen), sind hinsichtlich der genauen Festlegung der Auftragsverarbeiter/innen noch allfällige Ausschreibungen abzuwarten. Dabei sind die Anforderungen des Art. 28 DSGVO einzuhalten. Da es kein *„anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht eines Mitgliedstaates"* (Art. 28 Abs. 3 DSGVO), d.h. insbesondere keine Bestimmung im Gesundheitstelematikgesetz 2012 oder in einer darauf basierenden Verordnung, gibt, die die Anforderungen des Art. 28 Abs. 3 DSGVO erfüllt, sind Auftragsverarbeitungsvereinbarungen

	abzuschließen. Dies hat gemäß Art. 28 Abs. 9 DSGVO schriftlich zu erfolgen. Die Verantwortung für den Abschluss der Auftragsverarbeitungsvereinbarungen tragen die Verantwortlichen. Gleiches gilt für die Anwendung „EU-Patientenkurzakte“, die ebenso Anfang 2026 umzusetzen ist. **Die Anforderung “Bewertung des Verhältnisses zu Auftragsverarbeiterinnen und Auftragsverarbeitern” ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.**
Schutzmaßnahmen bei der Übermittlung in Drittländer (Kapitel V DSGVO; WP 248 Rev.01, 21 und 28)	Eine Übermittlung in Drittländer ist nicht vorgesehen. Es sind daher keine spezifischen Schutzmaßnahmen für die Übermittlung in Drittländer vorgesehen. **Die Anforderung “Bewertung der Schutzmaßnahmen bei der Übermittlung in Drittländer” ist aufgrund der nicht vorgesehenen Übermittlung in Drittländer als erfüllt anzusehen.**
Vorherige Konsultation (Art. 36 und EG 96 DSGVO; WP 248 Rev.01, 21 und 28)	Die vorherige Konsultation der Datenschutzbehörde ist nicht erforderlich, weil folgende Maßnahmen zur Eindämmung der Risiken getroffen wurden: die Sicherstellung der Freiwilligkeit der Teilnahme (§ 24i Abs. 2 GTelG 2012); die ausdrückliche Einschränkung der erlaubten Zwecke auf grenzüberschreitende Gesundheitsversorgung und die Wahrnehmung der Bürger/innenrechte, d.h. insbesondere der Betroffenenrechte gemäß Kapitel III DSGVO (§ 24k Abs. 2 Z 1 GTelG 2012); die Regelung einer ausdrücklichen Löschfrist für die Nationale Kontaktstelle (§ 24j Abs. 3 GTelG 2012); Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „*geeignete technische und organisatorische Maßnahmen*“ zu treffen sind; Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter/innen für „*ein dem Risiko angemessenes Schutzniveau*“ zu sorgen haben und der – zumindest im privaten Bereich – mit Geldstrafen bis 10 Mio. EUR sanktioniert ist (Art. 83 Abs. 4 Buchstabe a DSGVO); Art. 82 DSGVO, wonach auch immaterielle Schäden, ohne Erheblichkeitsschwelle und zwar auch gegenüber öffentlichen Stellen verschuldensunabhängig ersatzfähig sind; strafrechtliche Bestimmungen zur „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB); das für Beamt/innen bei den beteiligten öffentlichen Stellen, wie etwa der Nationalen Kontaktstelle, geltende Disziplinarrecht; das für Ärzt/innen geltende Standesrecht; die Bestimmungen des 2. Abschnittes des Gesundheitstelematikgesetzes 2012 zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist, die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister

	(Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012; die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Die Anforderung "Bewertung der vorherigen Konsultation" ist aufgrund der durchgeführten vorherigen Konsultation als erfüllt anzusehen.**
RISIKEN *Die Risiken sind nach ihrer Ursache, Art, Besonderheit, Schwere und Eintrittswahrscheinlichkeit zu bewerten (Erwägungsgründe 76, 77, 84 und 90 DSGVO). Als Risiken werden in den Erwägungsgründen 75 und 85 DSGVO unter anderem genannt:*	
Physische, materielle oder immaterielle Schäden (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Im Fall des EU-Rezepts: Ursache: Physische, materielle oder immaterielle Schäden können für die betroffenen Personen durch das Bekanntwerden bzw. Offenlegen von – aus den Medikationsdaten ableitbaren – Krankheiten sowie die Änderung bzw. Löschung von Medikationsdaten entstehen. Im Fall der EU-Patientenkurzakte: Ursache: Physische, materielle oder immaterielle Schäden können für die betroffenen Personen durch das Bekanntwerden bzw. Offenlegen von aus der EU-Patientenkurzakte abgelesenen oder ableitbaren Krankheiten oder sonstigen personenbezogenen Daten entstehen. In beiden Fällen: Art: **Physische Schäden** sind insbesondere bei Änderung der Medikationsdaten zu erwarten. Vor allem Änderungen in der Dosierung

	können zu physischen Schäden, d.h. Beeinträchtigungen der Gesundheit bis hin zum Tod führen, weil derartige Änderungen leichter übersehen werden können, als beispielsweise Änderungen, die den Namen des verschriebenen Arzneimittels betreffen und daher leichter auffallen. Als **materielle Schäden** können finanzielle Verluste etwa aufgrund des Verlust des Arbeitsplatzes oder sonstiger beruflicher bzw. geldwerter Chancen, etwa auf Versicherungs-, Miet- oder sonstige Vertragsverhältnisse auftreten. An **immateriellen Schäden** in Folge entdeckter Krankheiten sind vor allem Ängste vor den negativen Auswirkungen der Offenlegung, Änderung oder Löschung von Medikationsdaten zu erwarten. Immaterielle Schäden sind insbesondere auch aufgrund der Angst vor weiteren Datenschutzverletzungen ("Vertrauensverlust") sowie vor Stigmatisierung oder anderen Formen der Diskriminierung denkbar. Im Falle der EU-Patientenkurzakte ist dieses spezifische Risiko mangels schreibenden Zugriff nicht gegeben. Besonderheit: Das gegenständliche Risiko für physische, materielle oder immaterielle Schäden weist folgende Besonderheiten auf: Mit Medikationsdaten und der EU-Patientenkurzakte werden welche der sensibelsten Daten überhaupt verarbeitet. Die Liste der verschriebenen und verabreichten Arzneimittel stellt eine Zusammenfassung des Gesundheitszustands der betreffenden Person dar, aus der – bei entsprechender Medikation mit Psychopharmaka – sogar psychische Beeinträchtigungen abgelesen werden können. Durch den grenzüberschreitenden Charakter besteht ein geographisch außerordentlich großer Umfang der Verarbeitung, der sogar das Bundesgebiet übersteigt. Der grenzüberschreitende Charakter bedingt nicht nur einen ungewöhnlich großen (geographischen) Umfang der Verarbeitung, sondern erfordert auch das Zusammenspiel vieler unterschiedlicher technischer Systeme in zumindest zwei Mitgliedstaaten. Als weitere Besonderheit ist das gemäß § 54 des Ärztegesetzes 1998 sowie gemäß § 121 des Strafgesetzbuches besonders geschützte Vertrauensverhältnis zwischen Ärzt/innen und Patient/innen („ärztliche Schweigepflicht") zu nennen. Schwere: Fehlerhafte Medikationsdaten oder fehlende oder falsche Daten in der EU-Patientenkurzakte können mitunter zu schweren **physischen Schäden**, d.h. Beeinträchtigungen der Gesundheit bis hin zum Tod führen. Auch die materiellen Schäden können beträchtlich und mit langfristigen negativen Konsequenzen für die betroffenen Personen verbunden sein. Auch die **immateriellen Schäden** können erheblich sein, weil betroffene Personen keine Angst vor der Verarbeitung ihrer Gesundheitsdaten haben sollten, sondern sich ohne Angst auf die notwendige Behandlung konzentrieren können sollten. Eintrittswahrscheinlichkeit: Es ist nicht zu erwarten, dass es zu den angeführten Schäden für die betroffenen Personen kommt (die bereits jetzt bestehen und durch die Anwendungen des 2. und 3. Abschnitts durchwegs gemindert statt erhöht werden), weil es strenge Vorkehrungen und Maßnahmen gibt, die vor einer fehlerhaften bzw. missbräuchlichen Verarbeitung schützen sollen, wie insbesondere: die Sicherstellung der Freiwilligkeit der Teilnahme (§ 24i Abs. 2 GTelG 2012); die ausdrückliche Einschränkung der erlaubten Zwecke auf grenzüberschreitende Gesundheitsversorgung und die Wahrnehmung der Bürger/innenrechte, d.h. insbesondere der Betroffenenrechte gemäß Kapitel III DSGVO (§ 24k Abs. 2 Z 1 GTelG 2012); die Regelung einer ausdrücklichen Löschfrist für die Nationale Kontaktstelle (§ 24j Abs. 3 GTelG 2012); Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „*geeignete technische und organisatorische Maßnahmen*" zu treffen sind;

	Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter/innen für „*ein dem Risiko angemessenes Schutzniveau*“ zu sorgen haben und der – zumindest im privaten Bereich – mit Geldstrafen bis 10 Mio. EUR sanktioniert ist (Art. 83 Abs. 4 Buchstabe a DSGVO); Art. 82 DSGVO, wonach auch immaterielle Schäden, ohne Erheblichkeitsschwelle und zwar auch gegenüber öffentlichen Stellen verschuldensunabhängig ersatzfähig sind; strafrechtliche Bestimmungen zur „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB); das für Beamt/innen bei den beteiligten öffentlichen Stellen, wie etwa der Nationalen Kontaktstelle, geltende Disziplinarrecht; das für Ärzt/innen geltende Standesrecht; die Bestimmungen des 2. Abschnittes des Gesundheitstelematikgesetzes 2012 zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist, die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012; die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); die Heranziehung der BRZ GmbH als Ausfallrechenzentrum zur Sicherstellung der Verfügbarkeit, wobei die BRZ GmbH über Zertifizierungen gemäß ISO 27001, 22301 und 9001 verfügt (siehe BMSGPK-Sicherheitskonzept vom 7.6.2024 [in der Folge: SIKO], 16); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Aufgrund der Rahmenbedingungen, insbesondere der bereits bestehenden strengen rechtlichen Konsequenzen bei Verstößen sowie der Heranziehung von nach internationalen Standards zertifizierten Auftragsverarbeitern ist nicht von einem substanziellen Risiko für das**

	Auftreten physischer, materieller und immaterieller Schäden auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.
Verlust der Kontrolle über personenbezogene Daten (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Der Verlust der Kontrolle über personenbezogene Daten kann für die betroffenen Personen grundsätzlich durch jede Verarbeitung entstehen und ist bei gesetzlich vorgesehenen Verarbeitungen höher als bei Verarbeitungen aufgrund von Einwilligungen, weil bei gesetzlich vorgesehenen Verarbeitungen die Mitwirkung der betroffenen Personen oftmals nicht erforderlich bzw. vorgesehen ist. Art: Beim Verlust der Kontrolle über personenbezogene Daten haben die betroffenen Personen keinerlei Möglichkeit auf die Verarbeitung Einfluss zu nehmen und sind ihrer Betroffenenrechte beraubt. Besonderheit: Die Besonderheit des gegenständlichen Risikos für den Verlust der Kontrolle über personenbezogene Daten ergibt sich vor allem aus dem Umfang der verarbeiteten Daten. Dass die gesetzliche vorgesehene Verarbeitung aber nicht unzulässig ist, zeigen die Rechtsgrundlagen (siehe oben Feld „BEWERTUNG / Rechtmäßigkeit der Verarbeitung“) sowie die Öffnungsklauseln in der Datenschutz-Grundverordnung, die die Verarbeitung aufgrund nationaler Bestimmungen erlauben. Schwere: Von ihrer Schwere ist der Verlust der Kontrolle über personenbezogene Daten nicht von vergleichbaren Risiken aufgrund anderer gesetzlich vorgesehener Verarbeitungen zu unterscheiden. Eintrittswahrscheinlichkeit: Es ist nicht zu erwarten, dass es zum Verlust der Kontrolle über personenbezogene für die betroffenen Personen kommt, weil es zahlreiche Vorkehrungen gibt, die die Transparenz der Verarbeitung, die Wahrung der Betroffenenrechte sowie den (datenschutzrechtlichen) Rechtsschutz der betroffenen Personen sicherstellen, wie etwa: die Veröffentlichung des 6. Abschnitts des Gesundheitstelematikgesetzes 2012 sowie der darauf basierenden Verordnungen im Rahmen des Rechtsinformationssystems des Bundes im Internet; die Veröffentlichung der zugrundeliegenden, parlamentarischen Materialien auf dem Server des Parlaments; die umfassende Möglichkeit zur Wahrnehmung der Betroffenenrechte gemäß § 24n GTelG 2012; die Sicherstellung der Freiwilligkeit der Teilnahme durch § 24i Abs. 2 GTelG 2012. **Aufgrund der gegenständlichen Verarbeitung, insbesondere der vorgesehenen Maßnahmen zur Einhaltung der Transparenz und Sicherstellung der Betroffenenrechte ist nicht von einem nennenswerten Risiko für den Verlust der Kontrolle über personenbezogene Daten auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Diskriminierung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Nachteile aus Diskriminierung können für die betroffenen Personen grundsätzlich durch jede Verarbeitung personenbezogener Daten entstehen, weil die (automationsunterstützte) Verarbeitung personenbezogener Daten die Filterung nach gewissen Merkmalen erlaubt und für die so durch Filterung ermittelten betroffenen Personen (rechtswidriger Weise) negative Konsequenzen entstehen können. Ursache für Nachteile aus Diskriminierung sind einerseits technischer Natur, wenn es beispielsweise zu Datenschutzverletzungen kommt, und andererseits gesellschaftlicher Natur, wenn die Daten wegen fehlendem Verständnis oder aufgrund bestimmter Vorurteile zum Nachteil der betroffenen Person eingesetzt werden. Art: Denkbar sind Nachteile aus Diskriminierung insbesondere am Arbeitsplatz, wenn Arbeitnehmer/innen aufgrund ihrer Gesundheitsdaten bei Beförderungen oder Einstellungen benachteiligt oder ihre Arbeitsverhältnisse ungerechtfertigter Weise gekündigt werden. Auch Nachteile bei Versicherungen sind dankbar, etwa in Form höherer Prämien oder verweigerter Leistungen oder Versicherungsabschlüsse. Schließlich könnten betroffene Personen aufgrund bestimmter Diagnosen – insbesondere

	betreffend Psychopharmaka – sozial ausgegrenzt werden. Besonderheit: Das gegenständliche Risikos für Diskriminierungen weist folgende Besonderheiten auf: Mit Medikationsdaten werden eine der sensibelsten Daten überhaupt verarbeitet. Die Liste der verschriebenen und verabreichten Arzneimittel stellt eine Zusammenfassung des Gesundheitszustands der betreffenden Person dar, aus der – bei entsprechender Medikation mit Psychopharmaka – sogar psychische Beeinträchtigungen abgelesen werden können. Durch den grenzüberschreitenden Charakter besteht ein geographisch außerordentlich großer Umfang der Verarbeitung, der sogar das Bundesgebiet übersteigt. Der grenzüberschreitende Charakter bedingt nicht nur einen ungewöhnlich großen (geographischen) Umfang der Verarbeitung, sondern erfordert auch das Zusammenspiel vieler unterschiedlicher technischer Systeme in zumindest zwei Mitgliedstaaten. Als weitere Besonderheit ist das gemäß § 54 des Ärztegesetzes 1998 sowie gemäß § 121 des Strafgesetzbuches besonders geschützte Vertrauensverhältnis zwischen Ärzt/innen und Patient/innen („ärztliche Schweigepflicht") zu nennen. Schwere: Es sind leichte und schwere Fälle denkbar. Leichte Fälle können subtile Formen der Benachteiligung, wie zum Beispiel Ausschluss von bestimmten beruflichen Weiterbildungen, umfassen. Schwere Fälle können soziale Stigmatisierung und Isolation, Jobverlust oder Verlust des Versicherungsschutzes umfassen. Eintrittswahrscheinlichkeit: Es ist nicht zu erwarten, dass es zu den angeführten Schäden für die betroffenen Personen kommt, weil es strenge Vorkehrungen und Maßnahmen gibt, die vor einer fehlerhaften bzw. missbräuchlichen Verarbeitung schützen sollen, wie insbesondere: die Sicherstellung der Freiwilligkeit der Teilnahme (§ 24i Abs. 2 GTelG 2012); die ausdrückliche Einschränkung der erlaubten Zwecke auf grenzüberschreitende Gesundheitsversorgung und die Wahrnehmung der Bürger/innenrechte, d.h. insbesondere der Betroffenenrechte gemäß Kapitel III DSGVO (§ 24k Abs. 2 Z 1 GTelG 2012); die Regelung einer ausdrücklichen Löschfrist für die Nationale Kontaktstelle (§ 24j Abs. 3 GTelG 2012); Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „*geeignete technische und organisatorische Maßnahmen*" zu treffen sind; Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter/innen für „*ein dem Risiko angemessenes Schutzniveau*" zu sorgen haben und der – zumindest im privaten Bereich – mit Geldstrafen bis 10 Mio. EUR sanktioniert ist (Art. 83 Abs. 4 Buchstabe a DSGVO); Art. 82 DSGVO, wonach auch immaterielle Schäden, ohne Erheblichkeitsschwelle und zwar auch gegenüber öffentlichen Stellen verschuldensunabhängig ersatzfähig sind; strafrechtliche Bestimmungen zur „Verletzung von Berufsgeheimnissen" (§ 121 StGB), „Amtsmissbrauch" (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses" (§ 310 StGB); das für Beamt/innen bei den beteiligten öffentlichen Stellen, wie etwa der Nationalen Kontaktstelle, geltende Disziplinarrecht; das für Ärzt/innen geltende Standesrecht; die Bestimmungen des 2. Abschnittes des Gesundheitstelematikgesetzes 2012 zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist,

	die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012; die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); die Heranziehung der BRZ GmbH als Ausfallrechenzentrum zur Sicherstellung der Verfügbarkeit, wobei die BRZ GmbH über Zertifizierungen gemäß ISO 27001, 22301 und 9001 verfügt (siehe BMSGPK-Sicherheitskonzept vom 7.6.2024 [in der Folge: SIKO], 16); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einem substanziellen Risiko für Diskriminierung der betroffenen Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Identitätsdiebstahl oder -betrug (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Identitätsdiebstahl oder -betrug treten typischerweise in der Folge von Datenschutzverletzungen (Art. 4 Nr. 12 DSGVO) auf, wenn personenbezogene Daten, wie insbesondere Personenkennzeichen, E-Mail-Adressen, Nutzerkennungen, Passwörter oder Kreditkarteninformationen gestohlen oder offengelegt werden. Ursache für Datenschutzverletzungen können Schwachstellen in der IT-Sicherheit, wie ungenügende Verschlüsselung oder schlecht gesicherte Datenbanken sein, die es Hacker/innen erleichtern, Zugriff auf sensible Daten zu erlangen. Auch menschliches Fehlverhalten kann zu Datenschutzverletzungen führen, weshalb in sensiblen Bereichen (der Systemadministration) jedenfalls ein 4-Augen-Prinzip erforderlich ist. Art: Identitätsdiebstahl oder -betrug können zu hohen, finanziellen Schäden bei den betroffenen Personen führen, insbesondere wenn mit den gestohlenen Identitäten kostenpflichtige Services (im Internet) in Anspruch genommen werden. Die betroffenen Personen entdecken den Identitätsdiebstahl oder -betrug oft erst, wenn ihnen nicht bezogene Leistungen in Rechnung gestellt werden. Es sind aber nicht nur finanzielle Schäden für die betroffenen Personen, sondern auch für Dritte denkbar, wenn beispielsweise mit gestohlenen Identitäten nicht zustehende Gesundheits- bzw. Versicherungsleistungen abgerufen werden. Nicht nur aus diesem Grund ist es daher im eigenen, vitalen Interesse der Verantwortlichen, für eine entsprechende Datensicherheit zu sorgen.

	Besonderheit: Die Besonderheit des gegenständlichen Risikos für Identitätsdiebstahl oder -betrug ergibt sich vor allem aus der gesetzlichen Regelung, die der Verarbeitungstätigkeit „EU-Rezept“ zugrunde liegt, dem großen Umfang, der Komplexität der zugrundeliegenden IT-Systeme sowie der potentiellen Mächtigkeit gestohlener Identitäten. Die Aussicht in den Genuss gesetzlicher Sozialversicherungsleistungen zu kommen, könnte einen erheblichen Anreiz für Identitätsdiebstahl und -betrug darstellen. Eine weitere Besonderheit ist, dass – vor allem der medizinische Identitätsdiebstahl oder -betrug, lange Zeit oft nicht erkannt werden kann, weil anders als beim finanziellen Identitätsdiebstahl oder -betrug monatliche Abrechnungen, wie etwa Kreditkartenabrechnungen, und deren Kontrolle nicht gängige Praxis sind. Schwere: Identitätsdiebstahl oder -betrug können – wie bereits ausgeführt – zu hohen, finanziellen Schäden führen. Verlust der Kreditwürdigkeit und hohe Schulden durch rechtswidrige Transaktionen können auf Seiten der betroffenen Personen und hohe, ungerechtfertigte Transferleistungen können auf Seiten der Verantwortlichen nicht ausgeschlossen werden. Nicht unerwähnt bleiben sollen medizinische Risiken, wenn es durch Identitätsdiebstahl oder -betrug möglicherweise zu Fehlbehandlungen kommt. Eintrittswahrscheinlichkeit: Datenschutzverletzungen können nie zur Gänze ausgeschlossen werden. Es ist daher wichtig durch geeignete Prozesse sicherzustellen, dass sie soweit als möglich verhindert werden bzw. im Fall des Falles rasch reagiert wird. Insbesondere sollen typische technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung gemäß Art. 32 DSGVO vorgesehen werden, wie etwa zur zeitlichen Verfügbarkeit, zu Sicherheitsanforderungen und Zugriffsschutz, zu Beauftragten für die Informationssicherheit, zum Risikomanagement, zu Sicherheitsanforderungen an Prozesse, zu technische Sicherheitsanforderungen, zu Sicherheitsanforderungen an die Authentifizierung, zu Sicherheitsanforderungen für Testumgebungen, zu baulichen Sicherheitsanforderungen sowie zu Sicherheitsanforderungen an das Personal. Dass weder Passwörter noch Nutzerkennungen oder Kreditkarteninformationen verarbeitet werden, senkt das Risiko für Identitätsdiebstahl oder -betrug. Auch durch die folgenden bereits im Entwurf enthaltenen technischen und organisatorischen Maßnahmen soll die Sicherheit der Verarbeitung erhöht und das Risiko für Identitätsdiebstahl oder -betrug gesenkt werden: die ausdrückliche Einschränkung der erlaubten Zwecke auf grenzüberschreitende Gesundheitsversorgung und die Wahrnehmung der Bürger/innenrechte, d.h. insbesondere der Betroffenenrechte gemäß Kapitel III DSGVO (§ 24k Abs. 2 Z 1 GTelG 2012); die Regelung einer ausdrücklichen Löschfrist für die Nationale Kontaktstelle (§ 24j Abs. 3 GTelG 2012); Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „*geeignete technische und organisatorische Maßnahmen*“ zu treffen sind; Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter/innen für „*ein dem Risiko angemessenes Schutzniveau*“ zu sorgen haben und der – zumindest im privaten Bereich – mit Geldstrafen bis 10 Mio. EUR sanktioniert ist (Art. 83 Abs. 4 Buchstabe a DSGVO); Art. 82 DSGVO, wonach auch immaterielle Schäden, ohne Erheblichkeitsschwelle und zwar auch gegenüber öffentlichen Stellen verschuldensunabhängig ersatzfähig sind; strafrechtliche Bestimmungen zur „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB);

	das für Beamt/innen bei den beteiligten öffentlichen Stellen, wie etwa der Nationalen Kontaktstelle, geltende Disziplinarrecht; das für Ärzt/innen geltende Standesrecht; die Bestimmungen des 2. Abschnittes des Gesundheitstelematikgesetzes 2012 zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist, die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012; die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); die Heranziehung der BRZ GmbH als Ausfallrechenzentrum zur Sicherstellung der Verfügbarkeit, wobei die BRZ GmbH über Zertifizierungen gemäß ISO 27001, 22301 und 9001 verfügt (siehe BMSGPK-Sicherheitskonzept vom 7.6.2024 [in der Folge: SIKO], 16); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einem substanziellen Risiko für Identitätsdiebstahl oder -betrug auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Finanzielle Verluste (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Auch finanzielle Verluste treten typischerweise in der Folge von Datenschutzverletzungen (Art. 4 Nr. 12 DSGVO) auf, wenn personenbezogene Daten, wie insbesondere Personenkennzeichen, E-Mail-Adressen, Nutzerkennungen, Passwörter oder Kreditkarteninformationen gestohlen oder offengelegt werden. Finanzielle Verluste können sich aber auch als nachteilige Folgen von Diskriminierung ergeben. Art: Finanzielle Verluste sind geldwerte Schäden und können insbesondere im Entgang von Verdienstmöglichkeiten liegen. Besonderheit: Die Besonderheit des gegenständlichen Risikos für finanzielle Verluste ergibt sich vor allem aus der gesetzlichen Regelung, die der

	Verarbeitungstätigkeit „EU-Rezept“ zugrunde liegt, dem großen Umfang, der Komplexität der zugrundeliegenden IT-Systeme sowie der potentiellen Mächtigkeit gestohlener Identitäten. Die Aussicht in den Genuss gesetzlicher Sozialversicherungsleistungen zu kommen, könnte einen erheblichen Anreiz für Hacking bieten. Schwere: Identitätsdiebstahl oder -betrug sowie Diskriminierung können – wie bereits oben ausgeführt – zu hohen, finanziellen Schäden bei den betroffenen Personen führen. Eintrittswahrscheinlichkeit: Es ist nicht zu erwarten, dass es zu finanziellen Verlusten für die betroffenen Personen kommt, weil zahlreiche Vorkehrungen bestehen, die die Rechtmäßigkeit der Verarbeitung sicherstellen sollen, wie etwa: die Sicherstellung der Freiwilligkeit der Teilnahme (§ 24i Abs. 2 GTelG 2012); die ausdrückliche Einschränkung der erlaubten Zwecke auf grenzüberschreitende Gesundheitsversorgung und die Wahrnehmung der Bürger/innenrechte, d.h. insbesondere der Betroffenenrechte gemäß Kapitel III DSGVO (§ 24k Abs. 2 Z 1 GTelG 2012); die Regelung einer ausdrücklichen Löschfrist für die Nationale Kontaktstelle (§ 24j Abs. 3 GTelG 2012); Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „*geeignete technische und organisatorische Maßnahmen*“ zu treffen sind; Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter/innen für „*ein dem Risiko angemessenes Schutzniveau*“ zu sorgen haben und der – zumindest im privaten Bereich – mit Geldstrafen bis 10 Mio. EUR sanktioniert ist (Art. 83 Abs. 4 Buchstabe a DSGVO); Art. 82 DSGVO, wonach auch immaterielle Schäden, ohne Erheblichkeitsschwelle und zwar auch gegenüber öffentlichen Stellen verschuldensunabhängig ersatzfähig sind; strafrechtliche Bestimmungen zur „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB); das für Beamt/innen bei den beteiligten öffentlichen Stellen, wie etwa der Nationalen Kontaktstelle, geltende Disziplinarrecht; das für Ärzt/innen geltende Standesrecht; die Bestimmungen des 2. Abschnittes des Gesundheitstelematikgesetzes 2012 zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist, die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012; die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); die Heranziehung der BRZ GmbH als Ausfallrechenzentrum zur

	Sicherstellung der Verfügbarkeit, wobei die BRZ GmbH über Zertifizierungen gemäß ISO 27001, 22301 und 9001 verfügt (siehe BMSGPK-Sicherheitskonzept vom 7.6.2024 [in der Folge: SIKO], 16); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von finanziellen Verlusten für die betroffenen Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Unbefugte Aufhebung der Pseudonymisierung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Eine Pseudonymisierung ist für die gegenständliche Verarbeitungstätigkeit nicht vorgesehen, da für die vorgesehenen Zwecke nicht praxistauglich, weshalb dieses Kriterium nicht anwendbar ist. **Die Anforderung "Unbefugte Aufhebung der Pseudonymisierung" ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.**
Rufschädigung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Nachteile aus Rufschädigung sind theoretisch und – wie viele andere Risiken auch – als Folge von Datenschutzverletzungen, etwa durch Hacking oder menschliches Fehlverhalten denkbar. Art: Nachteile aus Rufschädigung können sich für betroffene Personen als auch die Verantwortlichen selbst ergeben. Besonderheit: Die Besonderheit des gegenständlichen Risikos für Rufschädigungen ergibt sich vor allem aus der gesetzlichen Regelung, die der Verarbeitungstätigkeit „EU-Rezept" zugrunde liegt, dem großen Umfang, der Komplexität der zugrundeliegenden IT-Systeme sowie der potentiellen Mächtigkeit gestohlener Identitäten. Die Aussicht in den Genuss gesetzlicher Sozialversicherungsleistungen zu kommen, könnte einen erheblichen Anreiz für Hacking – und damit Datenschutzverletzungen – bieten. Schwere: Die Schwere des Risikos kann theoretisch – je nach Art der potentiellen Rufschädigung – auch hoch sein. Eintrittswahrscheinlichkeit: Nachteile durch Rufschädigung sind eher nicht zu erwarten, weil den typischerweise mit einer Rufschädigung verbundenen Nachteilen durch technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit und insbesondere Minimierung der Daten begegnet wird. Zu diesen Maßnahmen zählen etwa: die ausdrückliche Einschränkung der erlaubten Zwecke auf grenzüberschreitende Gesundheitsversorgung und die Wahrnehmung der Bürger/innenrechte, d.h. insbesondere der Betroffenenrechte gemäß Kapitel III DSGVO (§ 24k Abs. 2 Z 1 GTelG 2012); die Regelung einer ausdrücklichen Löschfrist für die Nationale Kontaktstelle (§ 24j Abs. 3 GTelG 2012); Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „*geeignete technische und organisatorische Maßnahmen*" zu treffen sind; Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter/innen für „*ein dem Risiko angemessenes Schutzniveau*" zu sorgen haben und der – zumindest im privaten Bereich – mit Geldstrafen bis 10 Mio. EUR sanktioniert ist (Art. 83 Abs. 4 Buchstabe a DSGVO); Art. 82 DSGVO, wonach auch immaterielle Schäden, ohne Erheblichkeitsschwelle und zwar auch gegenüber öffentlichen Stellen

	verschuldensunabhängig ersatzfähig sind; strafrechtliche Bestimmungen zur „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB); das für Beamt/innen bei den beteiligten öffentlichen Stellen, wie etwa der Nationalen Kontaktstelle, geltende Disziplinarrecht; das für Ärzt/innen geltende Standesrecht; die Bestimmungen des 2. Abschnittes des Gesundheitstelematikgesetzes 2012 zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist, die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012; die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); die Heranziehung der BRZ GmbH als Ausfallrechenzentrum zur Sicherstellung der Verfügbarkeit, wobei die BRZ GmbH über Zertifizierungen gemäß ISO 27001, 22301 und 9001 verfügt (siehe BMSGPK-Sicherheitskonzept vom 7.6.2024 [in der Folge: SIKO], 16); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einer Rufschädigung für betroffene Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Verlust der Vertraulichkeit bei Berufsgeheimnissen (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Der Verlust der Vertraulichkeit bei Berufsgeheimnissen ist theoretisch denkbar, wenn es zu Offenlegung durch Personen, die etwa dem Amts- oder einem anderen Berufsgeheimnis unterliegen, kommt. Vor allem mangelnde Abschreckung von Sanktionen begünstigen derartiges Verhalten. Abgesehen davon ist aber auch die rechtswidrige Offenlegung im Zuge von Datenschutzverletzungen, etwas aufgrund von Sicherheitslücken, denkbar.

	Art: Der Verlust der Vertraulichkeit bei Berufsgeheimnissen kann andere Risiken, wie etwa finanzielle Verluste oder Nachteile aus Diskriminierung zur Folge haben. Besonderheit: Die Besonderheit des gegenständlichen Risikos für den Verlust der Vertraulichkeit von Berufsgeheimnissen ergibt sich vor allem aus der gesetzlichen Regelung, die der Verarbeitungstätigkeit zugrunde liegt, dem großen Umfang, der Komplexität der zugrundeliegenden IT-Systeme sowie der potentiellen Mächtigkeit gestohlener Identitäten. Die Aussicht in den Genuss gesetzlicher Sozialversicherungsleistungen zu kommen, könnte einen erheblichen Anreiz für Hacking – und damit Datenschutzverletzungen – bieten. Schwere: Die Schwere des Risikos ergibt sich vor allem aus den anschließenden Risiken, wie etwa finanziellen Verlusten oder Nachteilen aus Diskriminierung. Eintrittswahrscheinlichkeit: Den typischerweise mit dem Verlust der Vertraulichkeit bei Berufsgeheimnissen verbundenen Nachteilen ist durch technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit zu begegnen. Zu diesen Maßnahmen zählen etwa: die ausdrückliche Einschränkung der erlaubten Zwecke auf grenzüberschreitende Gesundheitsversorgung und die Wahrnehmung der Bürger/innenrechte, d.h. insbesondere der Betroffenenrechte gemäß Kapitel III DSGVO (§ 24k Abs. 2 Z 1 GTelG 2012); die Regelung einer ausdrücklichen Löschfrist für die Nationale Kontaktstelle (§ 24j Abs. 3 GTelG 2012); Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „*geeignete technische und organisatorische Maßnahmen*“ zu treffen sind; Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter/innen für „*ein dem Risiko angemessenes Schutzniveau*“ zu sorgen haben und der – zumindest im privaten Bereich – mit Geldstrafen bis 10 Mio. EUR sanktioniert ist (Art. 83 Abs. 4 Buchstabe a DSGVO); Art. 82 DSGVO, wonach auch immaterielle Schäden, ohne Erheblichkeitsschwelle und zwar auch gegenüber öffentlichen Stellen verschuldensunabhängig ersatzfähig sind; strafrechtliche Bestimmungen zur „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB); das für Beamt/innen bei den beteiligten öffentlichen Stellen, wie etwa der Nationalen Kontaktstelle, geltende Disziplinarrecht; das für Ärzt/innen geltende Standesrecht; die Bestimmungen des 2. Abschnittes des Gesundheitstelematikgesetzes 2012 zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist, die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012;

	die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); die Heranziehung der BRZ GmbH als Ausfallrechenzentrum zur Sicherstellung der Verfügbarkeit, wobei die BRZ GmbH über Zertifizierungen gemäß ISO 27001, 22301 und 9001 verfügt (siehe BMSGPK-Sicherheitskonzept vom 7.6.2024 [in der Folge: SIKO], 16); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einem Verlust der Vertraulichkeit bei Berufsgeheimnissen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Erhebliche wirtschaftliche oder gesellschaftliche Nachteile (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Erhebliche wirtschaftliche oder gesellschaftliche Nachteile sind theoretisch und – wie viele andere Risiken auch – als Folge von Datenschutzverletzungen, etwa durch Hacking oder menschliches Fehlverhalten denkbar. Art: Wirtschaftliche Nachteile können für die betroffenen Personen vor allem in Kosten durch Identitätsdiebstahl und -betrug (siehe oben Felder „RISIKEN / Identitätsdiebstahl und -betrug“ bzw. „RISIKEN / Finanzielle Verluste“) bestehen. Für die Verantwortlichen können Kosten durch Betrugsfälle, Haftungsschäden und Wiederherstellung der Datensicherheit aufgrund von Datenschutzverletzungen entstehen. Gesellschaftliche Nachteile sind insbesondere als Vertrauensverlust in das Gesundheitssystem, Diskriminierung von betroffenen Personen (siehe oben Feld „RISIKEN / Diskriminierung“) und generelle Ängste und Unsicherheiten der betroffenen Personen denkbar. Besonderheit: Die Besonderheit des gegenständlichen Risikos für erhebliche wirtschaftliche oder gesellschaftliche Nachteile ergibt sich vor allem aus der gesetzlichen Regelung, die der Verarbeitungstätigkeit zugrunde liegt, dem großen Umfang, der Komplexität der zugrundeliegenden IT-Systeme sowie der potentiellen Mächtigkeit gestohlener Identitäten bzw. Daten, die als großer Anreiz für Hacking dienen können. Schwere: Die Schwere des Risikos kann theoretisch – je nach Art der potentiellen, erheblichen wirtschaftlichen oder gesellschaftlichen Nachteile – auch hoch sein. Eintrittswahrscheinlichkeit: Es ist nicht zu erwarten, dass es zu erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen für die betroffenen Personen kommt, weil zahlreiche technische und organisatorische Maßnahmen vorgesehen sind, die die Vertraulichkeit der Verarbeitung sicherstellen sollen, wie etwa: die ausdrückliche Einschränkung der erlaubten Zwecke auf grenzüberschreitende Gesundheitsversorgung und die Wahrnehmung der Bürger/innenrechte, d.h. insbesondere der Betroffenenrechte gemäß Kapitel III DSGVO (§ 24k Abs. 2 Z 1 GTelG 2012); die Regelung einer ausdrücklichen Löschfrist für die Nationale Kontaktstelle (§ 24j Abs. 3 GTelG 2012);

	Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „*geeignete technische und organisatorische Maßnahmen*“ zu treffen sind; Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter/innen für „*ein dem Risiko angemessenes Schutzniveau*“ zu sorgen haben und der – zumindest im privaten Bereich – mit Geldstrafen bis 10 Mio. EUR sanktioniert ist (Art. 83 Abs. 4 Buchstabe a DSGVO); Art. 82 DSGVO, wonach auch immaterielle Schäden, ohne Erheblichkeitsschwelle und zwar auch gegenüber öffentlichen Stellen verschuldensunabhängig ersatzfähig sind; strafrechtliche Bestimmungen zur „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB); das für Beamt/innen bei den beteiligten öffentlichen Stellen, wie etwa der Nationalen Kontaktstelle, geltende Disziplinarrecht; das für Ärzt/innen geltende Standesrecht; die Bestimmungen des 2. Abschnittes des Gesundheitstelematikgesetzes 2012 zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist, die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012; die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); die Heranziehung der BRZ GmbH als Ausfallrechenzentrum zur Sicherstellung der Verfügbarkeit, wobei die BRZ GmbH über Zertifizierungen gemäß ISO 27001, 22301 und 9001 verfügt (siehe BMSGPK-Sicherheitskonzept vom 7.6.2024 [in der Folge: SIKO], 16); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von erheblichen**

	wirtschaftlichen oder gesellschaftlichen Nachteilen für die betroffenen Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.
ABHILFEMASSNAHMEN *Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in den Erwägungsgründen 28, 78 und 83 DSGVO genannt:*	
Minimierung der Verarbeitung personenbezogener Daten (EG 78 und Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Die Minimierung der Daten erfolgt im Fall des EU-Rezepts insbesondere durch die Beschränkung der Datenarten gemäß § 24o Abs. 2 GTelG 2012, wonach nicht mehr als die in den ELGA-Komponenten und dem elektronischen Verwaltungssystem des Dachverbands enthaltenen Daten zu Verschreibungen aus dem e-Rezept verarbeitet werden dürfen sowie die Beschränkung der Verarbeitungsdauer durch § 24j Abs. 3 GTelG 2012. Im Falle der EU-Patientenkurzakte beschränken sich die Datenarten auf jene, die im jeweiligen Herkunftsmitgliedstaat vorgesehen sind und in der jeweiligen EU-Patientenkurzakte auch tatsächlich eingetragen sind. Außerdem dürfen die Daten nur für die Zwecke grenzüberschreitenden Gesundheitsversorgung sowie der Wahrnehmung der Bürger/innenrechte verarbeitet werden. **Die Anforderung "Abhilfe durch Minimierung der Verarbeitung personenbezogener Daten" ist insbesondere aufgrund der Beschränkung auf in ELGA vorhandene Daten sowie die Zweckbeschränkung als erfüllt anzusehen.**
Schnellstmögliche Pseudonymisierung personenbezogener Daten (EG 28 und 78 sowie Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Die Pseudonymisierung ist für die (grenzüberschreitende) Gesundheitsversorgung nicht möglich, weil eine konkrete natürliche Person behandelt werden soll bzw. muss. **Die Anforderung "Abhilfe durch schnellstmögliche Pseudonymisierung" ist – aufgrund der notwendigerweise personenbezogenen Gesundheitsversorgung – für die gegenständliche Verarbeitungstätigkeit nicht anwendbar und daher bloß als erfüllbar anzusehen.**
Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten (EG 78 DSGVO und Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Durch die Publikation der vorgeschlagenen Novelle als Bundesgesetz im Bundesgesetzblatt sowie der parlamentarischen Materialien im Zuge des Gesetzgebungsprozesses können die Hintergründe von der Öffentlichkeit kostenlos nachvollzogen werden. Außerdem wird die erforderliche Datenschutzerklärung im Internet zur Verfügung gestellt werden. Auch die allfällige Einrichtung einer Anlaufstelle gemäß Art. 26 DSGVO iVm § 24r Abs. 2 GTelG 2012 und § 24u Abs. 2 GTelG 2012 würde die Transparenz für die betroffenen Personen erhöhen. **Die Anforderung "Abhilfe durch Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten" ist aufgrund der bereits im Gesetzgebungsprozess bereitzustellenden Informationen bzw. der grundsätzlichen Machbarkeit einer zukünftigen Datenschutzerklärung jedenfalls als erfüllbar anzusehen.**
Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen (EG 78 DSGVO und Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Auf Grundlage der Datenschutz-Grundverordnung stehen den betroffenen Personen bezüglich der gegenständlichen Verarbeitung folgende Rechte gegenüber den gemeinsamen Verantwortlichen zu: das Recht auf Auskunft (Art. 15 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO), das Recht auf Löschung (Art. 17 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie die Pflicht zur Mitteilung (Art. 19 DSGVO). Diese Rechte können durch einen Zugang über das Zugangsportals bzw. gegenüber der ELGA- und eHealth-Supporteinrichtung geltend gemacht werden (§ 24n Abs. 1 GTelG 2012). **Die Anforderung "Abhilfe durch Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen" ist aufgrund der grundsätzlichen Machbarkeit als erfüllbar anzusehen.**
Datensicherheitsmaßnahmen (EG 78 und 83 DSGVO sowie Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Aufgrund des BMSGPK-Sicherheitskonzepts sind unter anderem folgende technische und organisatorische Maßnahmen vorgesehen bzw. bereits umgesetzt: die im 2. Abschnittes des Gesundheitstelematikgesetzes 2012 vorgesehenen

	Maßnahmen zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten, wie insbesondere § 3 Abs. 4 GTelG 2012, wonach Gesundheitsdaten nur dann übermittelt werden dürfen, wenn die Übermittlung gemäß Art. 9 DSGVO zulässig ist, die Identität der Patient/innen nachgewiesen ist, die Identität der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen ist, die Rollen der an der Übermittlung beteiligten Gesundheitsdienstleister (Art. 3 Buchstabe g der Patientenmobilitätsrichtlinie 2011/24/EU) nachgewiesen sind und Vertraulichkeit und Integrität der übermittelten Gesundheitsdaten gewährleistet sind; die verpflichtende eindeutige Identifikation von betroffenen Personen (§ 24k Abs. 1 Z 1 in Verbindung mit § 24l GTelG 2012) und involvierten Gesundheitsdiensteanbietern (§ 24k Abs. 1 Z 3 in Verbindung mit § 24m GTelG 2012); Einsatz der höchsten Qualität von Identifikatoren in Form bereichsspezifischer Personenkennzeichen gemäß den §§ 9 ff des E-Government-Gesetzes sowie § 4 Abs. 6 GTelG 2012; die verpflichtende, namentliche Protokollierung sämtlicher Verarbeitungsvorgänge (§ 24k Abs. 3 Z 4 in Verbindung mit § 22 GTelG 2012); die Heranziehung der BRZ GmbH als Ausfallrechenzentrum zur Sicherstellung der Verfügbarkeit, wobei die BRZ GmbH über Zertifizierungen gemäß ISO 27001, 22301 und 9001 verfügt (siehe BMSGPK-Sicherheitskonzept vom 7.6.2024 [in der Folge: SIKO], 16); weitere umfangreiche Sicherheitsmaßnahmen, wie etwa die Sicherheitsüberprüfung der IT-Administrator/innen (SIKO, 16); die Einschränkung von Drittkomponenten (SIKO, 33); Prüfung- und Validierungsverfahren (SIKO, 34); Passwortsicherheit (SIKO, 39); Systemtrennung (SIKO, 41); Systemhärtung (SIKO, 41); Systemisolierung (SIKO, 44); Update- und Patch-Management (SIKO, 45); Transportverschlüsselung (SIKO, 49); Datensicherung (SIKO, 52); sicherheitsrelevante Abnahmekriterien und Tests (SIKO, 57); System- und Prozessaudits (SIKO, 60); starke Authentifizierung für Fernwartungszugänge (SIKO, 62); Meldung von Sicherheitsvorfällen und Datenschutzverletzungen (SIKO, 65). **Die Anforderung "Abhilfe durch Datensicherheitsmaßnahmen" ist aufgrund der umfangreichen geplanten sowie bereits umgesetzten Datensicherheitsmaßnahmen jedenfalls als erfüllbar anzusehen.**
BERÜCKSICHTIGUNG VON DATENSCHUTZINTERESSEN *Gemäß Art. 35 Abs. 2 und 9 sowie Art. 36 Abs. 4 DSGVO ist – wenn möglich – der Rat des Datenschutzbeauftragten einzuholen und sind die betroffenen Personen anzuhören:*	
Stellungnahme des Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO; WP 248 Rev.01, 21 und 29)	Die datenschutzbeauftragten Personen der Verantwortlichen sind eingeladen zum vorgeschlagenen Entwurf Stellung zu nehmen. **Die Anforderung "Stellungnahme des Datenschutzbeauftragten" ist aufgrund der grundsätzlichen Machbarkeit jedenfalls als erfüllbar anzusehen.**
Stellungnahme betroffener Personen (Art. 35 Abs. 9 DSGVO; WP 248 Rev.01, 21 und 29)	Betroffene Personen werden im Rahmen einer noch einzurichtenden zentralen Anlaufstelle (§ 24r Abs. 2 und § 24 Abs. 2 in Verbindung mit § 28c GTelG 2012 sowie Art. 26 Abs. 1 DSGVO) die Möglichkeit haben zu der vorliegenden Verarbeitungstätigkeit Stellung zu nehmen. **Die Anforderung "Stellungnahme betroffener Personen" ist aufgrund der grundsätzlichen Machbarkeit der Einholung von Stellungnahmen**

53 von 53

	jedenfalls als erfüllbar anzusehen.