KNYRIM.TRIEB
RECHTSANWÄLTE

PER E-MAIL an:
Esch@seppmail.de
Stadlmair@seppmail.com

SEPPmail Deutschland GmbH
Ringstraße 1c
85649 Brunnthal b. München
DEUTSCHLAND

RA Dr. Rainer Knyrim
RA Dr. Gerald Trieb, LL.M.

RAA Jennifer Salomon, LL.M.
RAA Mag. Stephan Varga, BSc

Knyrim Trieb Rechtsanwälte OG
Mariahilfer Straße 89a
A-1060 Wien

T: +43 1 9093070
F: +43 1 9093639
E: kt@kt.at
W: www.kt.at

ERSTE BANK
BIC: GIBAATWWXXX
IBAN: AT652011182937766501
UID ATU71661837
FN 462250f HG Wien

25. Februar 2025
SEPPmail/GTelG/GT/SV/GB

Gutachten GTelG 2012 (Allgemeine Einschätzung der Rechtslage und Ausnahmeregelungen)

Sehr geehrter Herr Esch!
Sehr geehrter Herr Stadlmair!

Nachstehend finden Sie das beauftragte Gutachten über die Anforderungen an die Übermittlung von Gesundheitsdaten und genetischen Daten nach dem österreichischen Gesundheitstelematikgesetz 2012 (GTelG 2012). Das GTelG 2012 tritt als datenschutzrechtliches Spezialgesetz neben die Pflichten des datenschutzrechtlich für die Übermittlung dieser Daten Verantwortlichen (und des Auftragsverarbeiters) nach DSGVO und wird u.a. durch die (nationale) Gesundheitstelematikverordnung 2013 ergänzt. Es sieht insbesondere Regelungen zur Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten durch Gesundheitsdiensteanbieter vor. Da nach 20 Jahren die diesbezügliche „Faxausnahme" nicht mehr verlängert wurde, soll das Gutachten erörtern, welche Pflichten die Gesundheitsdiensteanbieter bei der elektronischen Übermittlung treffen und welche Ausnahmeregelungen (bis wann) greifen.

Wir behandeln daher zunächst den Kontext und die Historie des Gesundheitstelematikgesetzes (Punkt 1). Danach erläutern wir das Verhältnis zwischen DSGVO und GTelG 2012, die wesentlichen Begriffe des GTelG 2012 und den Anwendungsbereich des GTelG 2012 (Punkt 2). Anschließend führen wir aus, welche Datensicherheitsmaßnahmen ein Gesundheitsdiensteanbieter nach GTelG 2012 umsetzen muss (Punkt 3). Abschließend fassen wir die wesentlichen Inhalte des Gutachtens zusammen (Punkt 4).

Auftraggeber des Gutachtens ist die SEPPmail Deutschland GmbH (SEPPmail). SEPPmail bietet verschiedene Produkte im Bereich der E-Mail-Sicherheit an. Insbesondere können mit Produkten von SEPPmail E-Mails nicht nur elektronisch zur Sicherstellung der Integrität signiert, sondern auch E-Mails zur Sicherstellung der Vertraulichkeit verschlüsselt werden, ohne dass die Empfänger Verschlüsselungssoftware installiert haben müssen.

1. Kontext und Historie des Gesundheitstelematikgesetzes

Aufgrund der breiteren Verfügbarkeit und Nutzbarmachung des Internets erließ der österreichische Gesetzgeber 2004 das Gesundheitstelematikgesetz, um „Mindeststandards zur Gewährleistung der Datensicherheit beim elektronischen Transport von Gesundheitsdaten" festzulegen.[1] Insbesondere enthielt das Gesundheitstelematikgesetz daher Regelungen über die Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten. Die Übermittlung von Gesundheitsdaten per Fax (die die Anforderungen an die Datensicherheit nicht erfüllte) war jedoch insbesondere im Gesundheitsbereich noch weit verbreitet. Der Gesetzgeber sah über die Jahre daher verschiedene Ausnahmebestimmungen für die Übermittlung von Gesundheitsdaten über Fax vor, wenn die Einhaltung der Datensicherheitsmaßnahmen für den Gesundheitsdiensteanbieter technisch oder in Bezug auf den damit verbundenen wirtschaftlichen Aufwand unzumutbar war. Der Gesetzgeber begründete dies damit, dass die Verwendung von Faxgeräten „die einzige im Einsatz befindliche Kommunikationsinfrastruktur für die Übermittlung von Gesundheitsdaten [darstellte] und eine sofortige Ablöse nicht ohne Beeinträchtigung der Gesundheitsversorgung von Patientinnen und Patienten erfolgen [konnte]".[2]

Mit 31.12.2024 ist die letzte Übergangsregelung für die Übermittlung von Gesundheitsdaten und genetischen Daten über Fax ausgelaufen. Der Gesetzgeber führte diesbezüglich aus:

> „Sensible personenbezogene Daten per Fax zu übermitteln, galt noch vor einigen Jahren als relativ sichere Methode, allerdings hat sich die Situation zwischenzeitlich grundlegend geändert, da es sowohl bei den Endgeräten als auch bei den Transportwegen weitreichende Änderungen gab. In der Vergangenheit wurden beim Versand von Faxen exklusive Ende-zu-Ende-Telefonleitungen genutzt, jedoch sorgten technische Änderungen in den Telefonnetzen dafür, dass nunmehr keine exklusiven Leitungen mehr genutzt werden, sondern die Daten paketweise in Netzen transportiert werden, die auf Internet-Technologie beruhen. Zudem kann nicht mehr davon

[1] ErläutRV 693 BlgNR 22. GP 40.
[2] ErläutIA 1308/A BlgNR 24. GP 3.

ausgegangen werden, dass an der Gegenstelle der Faxübertragung auch ein reales Fax-Gerät existiert, denn meist werden Systeme genutzt, die ankommende Faxe automatisiert in ein E-Mail umwandeln und diese dann an bestimmte E-Mail-Postfächer weiterleiten.

Aufgrund dieser Umstände hat ein Fax hinsichtlich der Vertraulichkeit mittlerweile das gleiche Sicherheitsniveau wie ein unverschlüsseltes E-Mail. Fax-Dienste enthalten keinerlei Sicherungsmaßnahmen um die Vertraulichkeit der Daten zu gewährleisten. Sie sind daher in der Regel nicht für die Übertragung personenbezogener Daten, insbesondere nicht besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO, geeignet […].

Vor dem Hintergrund der technischen Entwicklungen der letzten Jahre ist davon auszugehen, dass die Unzumutbarkeit der Einhaltung [der Datensicherheitsmaßnahmen] nicht gegeben ist und **die Übermittlung von Gesundheitsdaten und genetischen Daten per Fax nicht zulässig ist**.

Der vorgeschlagene Entfall [der Ausnahmeregelung] stellt daher in rechtlicher Hinsicht nur eine formale Anpassung dar."[3]

2. Allgemeine Ausführungen zum und Anwendungsbereich des GTelG 2012

Das Gesundheitstelematikgesetz 2012 (GTelG 2012) enthält **Spezialbestimmungen** zur Verarbeitung personenbezogener elektronischer Gesundheitsdaten und genetischer Daten durch Gesundheitsdiensteanbieter. Auch nach In-Kraft-Treten der DSGVO darf der österreichische Gesetzgeber aufgrund einer Öffnungsklausel in der DSGVO zusätzliche Bedingungen (einschließlich Beschränkungen) für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten einführen oder aufrechterhalten.

Neben dem GTelG 2012 ist auf diese Datenverarbeitungen auch die **DSGVO** anwendbar, weshalb die Verantwortlichen (und die Auftragsverarbeiter) auch (zusätzlich) die DSGVO-Pflichten treffen. Insbesondere muss der Verantwortliche nach Art 32 Abs 1 DSGVO **geeignete technische und organisatorische Maßnahmen** umsetzen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Erfüllung der Bestimmungen über die Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten und

[3] ErläutRV 2530 BlgNR 27. GP 20.

genetischen Daten des GTelG 2012 führt nicht notwendigerweise und vollumfänglich[4] zu einer Erfüllung der Anforderungen des Art 32 Abs 1 DSGVO. Nachstehend werden die Pflichten nach DSGVO jedoch nicht erörtert, da Gegenstand des Gutachtens das GTelG 2012 ist. Das GTelG 2012 greift jedoch auf in der DSGVO definierte Begriffe zurück, weshalb diese Begriffe nach DSGVO auszulegen sind.[5]

Die **Verarbeitung** von Daten umfasst demnach u.a. das Speichern, das Verändern, das Auslesen und das Übermitteln von Daten. **Gesundheitsdaten** sind Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person (einschließlich der Erbringung von Gesundheitsdienstleistungen) beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Neben Entlassungsbriefen, Medikationsdaten und Laborbefunden können auch Arzt-Terminerinnerungen Gesundheitsdaten sein. Auch die Sozialversicherungsnummer kann (kontextbezogen) ein Gesundheitsdatum sein.

Gesundheitsdiensteanbieter sind Verantwortliche oder Auftragsverarbeiter, die regelmäßig in einer Rolle nach Gesundheitstelematikverordnung 2013 Gesundheitsdaten oder genetische Daten in elektronischer Form zu folgenden Zwecken verarbeiten:

a) medizinische Behandlung oder Versorgung oder

b) pflegerische Betreuung oder

c) Verrechnung von Gesundheitsdienstleistungen oder

d) Versicherung von Gesundheitsrisiken oder

e) Wahrnehmung von Patient/inn/en/rechten.

Nach den Gesetzesmaterialien zum GTelG 2012 können dies neben u.a. **Ärzten und Krankenanstalten** (siehe Anhang 1 dieses Gutachtens) auch **IT-Unternehmen**, die regelmäßig als Dienstleister für andere Gesundheitsdiensteanbieter auftreten, Patientenanwaltschaften oder auf Patientenrechte spezialisierte Rechtsanwälte sein.[6]

---

[4] Vgl. die Ausführungen in ErläutRV 1936 BlgNR 24. GP 17, nach denen die Vorgängerbestimmung von Art 32 DSGVO zu Datensicherheitsmaßnahmen (§ 14 DSG 2000) nicht restlos verdrängt wurde und in den nach GTelG 2012 nicht erfassten Bereichen weiterhin galt. Aufgrund des Anwendungsvorranges der DSGVO als Unionsrecht gilt dies umso mehr für die Bestimmungen der DSGVO, da (mangels einer Öffnungsklausel) nationales Recht im Widerspruch mit der DSGVO unangewendet bleiben muss.

[5] Vgl. die Ausführungen in ErläutRV 1936 BlgNR 24. GP 17, nach denen Begriffe im Zweifelsfall im Lichte des DSG 2000 auszulegen sind.

[6] ErläutRV 1936 BlgNR 24. GP 18.

Neben Regelungen über die elektronischen Gesundheitsakte (ELGA) enthält das GTelG 2012 im **zweiten Abschnitt** auch Bestimmungen über die **Datensicherheit** bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten. Diese Bestimmungen sind anwendbar, wenn Gesundheitsdaten und genetische Daten durch Gesundheitsdiensteanbieter elektronisch übermittelt werden. Von der Übermittlung umfasst ist daher die (elektronische) Übermittlung an andere Gesundheitsdiensteanbieter, aber auch die (elektronische) Übermittlung an Auftragsverarbeiter oder an andere Personen. Auch die Übermittlung von Daten an die betroffene Person (d.h. an jene Person, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen) kann vom Begriff der Übermittlung nach GTelG 2012 umfasst sein, wenn die übermittelten personenbezogenen Daten der betroffenen Person noch nicht bekannt sind.[7] Lokale Datenverarbeitungen innerhalb eines Gesundheitsdiensteanbieters und konzerninterne Übermittlungen in abgeschlossenen und abgesicherten Systemen unterliegen nur ausgewählten Verpflichtungen (Inhouse-Privileg; anwendbar bleiben: IT-Sicherheitskonzept, Übermittlung auf Basis einer Rechtsgrundlage nach DSGVO und Nachweis der Identität jener Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen).

3. Zulässigkeit der Übermittlung von Gesundheitsdaten und genetischen Daten nach dem zweiten Abschnitt des GTelG 2012

Nach dem zweiten Abschnitt des GTelG 2012 müssen für die Zulässigkeit der Übermittlung von Gesundheitsdaten und genetischen Daten mehrere Voraussetzungen **kumulativ** erfüllt sein. Auch mit Einwilligung der betroffenen Person kann von den (zwingenden) Bestimmungen des GTelG 2012 nicht abgewichen werden: Gesetzlich geforderte Datensicherheitsmaßnahmen sind vom Verantwortlichen zu erfüllen, ein Unterschreiten oder Nichterfüllen der Anforderungen ist einer Einwilligung nicht zugänglich. Da das GTelG 2012 ein datenschutzrechtliches Spezialgesetz ist, kann die Datenschutzbehörde Verstöße gegen den zweiten Abschnitt des GTelG 2012 nach den Bestimmungen der DSGVO sanktionieren[8], weshalb Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden können. Bei (anderen) Verstößen gegen die DSGVO können Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden.

---

[7] Auch die Arzt-Patienten-Kommunikation über Daten, die der betroffenen Person bekannt sind (z.B. Terminerinnerungen), muss (ungeachtet, ob diese unter das GTelG 2012 fällt), nach der DSGVO verschlüsselt erfolgen!

[8] ErläutRV 108 BlgNR 26. GP 76.

3.1. IT-Sicherheitskonzept

Technische und organisatorische Maßnahmen nach DSGVO und nach GTelG 2012 sind auf Basis eines IT-Sicherheitskonzepts **zu dokumentieren**. Aus dieser Dokumentation muss hervorgehen, dass sowohl der Zugriff als auch die Übermittlung der Daten ordnungsgemäß erfolgt und die Daten Unbefugten nicht zugänglich sind.

3.2. Zugriffs- und Berechtigungssystem

Die Verwendung von Gesundheitsdaten oder genetischen Daten innerhalb eines Gesundheitsdiensteanbieters muss durch ein Zugriffs- und Berechtigungssystem abgesichert sein, das eine **Authentifizierung der Benutzer/innen** voraussetzt. Dadurch können die unterschiedlichen Zugriffsberechtigungen der einzelnen Rollen (z.B. medizinisches Personal, Verwaltungspersonal, technisches Personal) sichergestellt werden.[9]

3.3. Zulässigkeit der Übermittlung nach Art 9 DSGVO

Es muss ein **Ausnahmetatbestand nach Art 9 Abs 2 DSGVO und (nach der Rechtsprechung des EuGH) zusätzlich eine Rechtsgrundlage nach Art 6 Abs 1 DSGVO** für die Übermittlung vorliegen.

3.4. Identität der betroffenen Person und der beteiligten Gesundheitsdiensteanbieter

Die Identität jener Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen, und die Identität der an der Übermittlung beteiligten Gesundheitsdiensteanbieter muss nachgewiesen werden. Bei Verwendung einer ungerichteten Kommunikation (dies ist dann der Fall, wenn die Empfänger der Gesundheitsdaten nicht abschließend im Vorhinein namentlich bekannt sind[10]) muss die **eindeutige Identität** von Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen, nachgewiesen und geprüft werden (z.B. mittels Patient/inn/enindex[11]). Bei Verwendung einer gerichteten Kommunikation (z.B. klassische Übermittlungsarten) muss hingegen „bloß" deren **Identität** (nicht deren eindeutige Identität) festgestellt und nachgewiesen werden. Unabhängig davon, ob die Kommunikation ungerichtet oder gerichtet ist, ist die **eindeutige Identität**

[9] ErläutRV 1936 BlgNR 24. GP 21.
[10] ErläutRV 1936 BlgNR 24. GP 21.
[11] Der Patient/inn/enindex enthält alle ELGA-Teilnehmer/inne/n und dient der Überprüfung der eindeutigen Identität natürlicher Personen.

der an der Übermittlung beteiligten Gesundheitsdiensteanbieter nachzuweisen und zu prüfen.

Der Nachweis der **eindeutigen Identität** (sowie der Rolle der beteiligten Gesundheitsdiensteanbieter) hat

1. durch Verwendung elektronischer Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen[12], sowie bereichsspezifische Personenkennzeichen oder

2. durch elektronischen Abgleich mit dem eHealth-Verzeichnisdienst[13] oder

3. durch elektronischen Abgleich mit dem Gesundheitsdiensteanbieterindex[14]

zu erfolgen.

Die eindeutige Identität ist mit Hilfe der **eindeutigen elektronischen Kennzeichen** gemäß § 8 E-GovG zu speichern.

Ausnahmeregelung: Ist der Nachweis der Identität und der Rolle der beteiligten Gesundheitsdiensteanbieter (sowie der Integrität) **mangels vorhandener technischer Infrastruktur nicht zumutbar** (zu berücksichtigen sind der Stand der Technik und die Implementierungskosten), dürfen Gesundheitsdaten und genetische Daten auch dann übermittelt werden, wenn zumindest die Identitäten und maßgeblichen Rollen der an der Übermittlung beteiligten Gesundheitsdiensteanbieter gegenseitig durch

1. persönlichen Kontakt oder

2. telefonischen Kontakt oder

3. Vertragsbestimmungen oder

4. Abfrage elektronischer Verzeichnisse

[12] Es ist daher zulässig, von einem qualifizierten Zertifikat abgeleitete Zertifikate zu verwenden (z.B., wenn ein Zustelldienst als Aussteller „normaler" Zertifikate, fungiert (ErläutRV 1936 BlgNR 24. GP 22)).

[13] Der eHealth-Verzeichnisdienst ist ein Verzeichnis aller in Österreich tätigen und registrierten Gesundheitsdiensteanbieter samt deren Rollen und Identifikation.

[14] Der Gesundheitsdiensteanbieterindex ist ein Verzeichnis aller Gesundheitsdiensteanbieter, die gesetzlich dazu berechtigt sind, in ELGA-Gesundheitsdaten ihrer Patientinnen und Patienten Einsicht zu nehmen.

a. der Österreichischen Ärztekammer oder

b. der Österreichischen Zahnärztekammer oder

c. des Österreichischen Hebammengremiums oder

d. der Österreichischen Apothekerkammer oder

e. des Dachverbandes oder

f. des für das Gesundheitswesen zuständigen Bundesministeriums

bestätigt sind.

Wird die Identität und die Rolle der an der Übermittlung beteiligten Gesundheitsdiensteanbieter **durch persönlichen oder telefonischen Kontakt bestätigt**, sind vor der erstmaligen Übermittlung der Gesundheitsdaten und genetischen Daten zwischen den beteiligten Gesundheitsdiensteanbietern

1. Datum und Art der Kontaktaufnahme,

2. die vollständigen Namen und maßgeblichen Rollen der an der Übermittlung beteiligten Gesundheitsdiensteanbieter,

3. die Angaben zur Erreichbarkeit der Gesundheitsdiensteanbieter sowie

4. die Angaben über die an der Kontaktaufnahme beteiligten natürlichen Personen

zu dokumentieren. Die Angaben zur Erreichbarkeit sind laufend aktuell zu halten.

Diese erleichterten Bedingungen gelten für alle beteiligten Gesundheitsdiensteanbieter, wenn für **zumindest einen** der beteiligten Gesundheitsdiensteanbieter diese erleichterten Bedingungen gelten („Einer-für-alle"-Prinzip).

3.5. Rolle der Gesundheitsdiensteanbieter

Mit der eindeutigen Identität der an der Übermittlung beteiligten Gesundheitsdiensteanbieter ist auch deren **Rolle** (siehe die Ausführungen zum Gesundheitsdiensteanbieter in

Punkt 2) nachzuweisen (z.B. Arzt/Ärztin für Allgemeinmedizin oder Krankenanstalt). Diesbezüglich (und auch zu den Ausnahmebestimmungen) wird auf die Ausführungen zur Identität in Punkt 3.4 oben verwiesen.

3.6. Integrität

Der Nachweis der Integrität (der Unverfälschtheit und der Echtheit[15]) elektronischer Gesundheitsdaten und genetischer Daten hat **durch die Verwendung fortgeschrittener oder qualifizierter elektronischer Signaturen oder fortgeschrittener oder qualifizierter elektronischer Siegel[16]** zu erfolgen. Die Integrität muss nicht nachgewiesen werden, wenn für die Übermittlung ein **abgesichertes Netzwerk** (siehe die Ausführungen zur Vertraulichkeit in Punkt 3.7) verwendet wird und der Zugang zu diesem Netzwerk ausschließlich für im Vorhinein bekannte Gesundheitsdiensteanbieter möglich ist.

Ausnahmeregelung: Ist der Nachweis der **Integrität mangels vorhandener technischer Infrastruktur nicht zumutbar** (zu berücksichtigen sind der Stand der Technik und die Implementierungskosten), dürfen Gesundheitsdaten und genetische Daten auch übermittelt werden, wenn zumindest die Identitäten und maßgeblichen Rollen der an der Übermittlung beteiligten Gesundheitsdiensteanbieter gegenseitig bestätigt werden (siehe erneut die diesbezüglichen Ausführungen zur Identität in Punkt 3.4).

3.7. Vertraulichkeit

Die Vertraulichkeit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten ist dadurch sicherzustellen, dass entweder

1. die elektronische Übermittlung von Gesundheitsdaten und genetischen Daten über **Netzwerke** durchgeführt wird, die gegenüber unbefugten Zugriffen **abgesichert** sind, indem sie zumindest

    a. die Absicherung der Übermittlung von Daten durch kryptographische[17] oder bauliche Maßnahmen,

[15] ErläutRV 1936 BlgNR 24. GP 24.
[16] Elektronische Siegel werden zum Nachweis des Ursprungs und der Unversehrtheit von Daten verwendet und können (im Unterschied zu elektronischen Signaturen) ausschließlich von juristischen Personen erstellt werden. In technischer Hinsicht unterscheiden sich elektronische Siegel nicht von elektronischen Signaturen.
[17] Eine Beschränkung der zulässigen Algorithmen ist in der derzeitigen Fassung der Gesundheitstelematikverordnung 2013 nicht mehr vorgesehen.

b. den Netzzugang ausschließlich für eine geschlossene oder abgrenzbare Benutzer/innen/gruppe sowie

c. die Authentifizierung der Benutzer/innen

vorsehen, oder

2. (bei Übermittlungen außerhalb dieser Netzwerke) **Protokolle und Verfahren** verwendet werden, die die **vollständige Verschlüsselung** der Gesundheitsdaten und genetischen Daten bewirken.

Die allenfalls von der Verschlüsselung ausgenommenen Informationen dürfen weder allfällige Authentifizierungsdaten noch Hinweise auf die betroffene(n) Person(en) (z.B. deren Namen oder deren Sozialversicherungsnummer), deren Gesundheitsdaten oder genetische Daten enthalten.

Werden Gesundheitsdaten und genetische Daten von einem Auftragsverarbeiter in der **Cloud** gespeichert, müssen die Daten mit einem dem aktuellen Stand der Technik entsprechenden Verfahren verschlüsselt worden sein.

Ausnahmeregelung: Bis 30. Juni 2026 darf die Sicherstellung der Vertraulichkeit abweichend erfolgen, wenn

1. Protokolle und Verfahren verwendet werden, die die vollständige Verschlüsselung der Gesundheitsdaten und genetischen Daten bei deren Bereitstellung („Transportverschlüsselung") bewirken,

2. die Sicherstellung der Vertraulichkeit mangels vorhandener technischer Infrastruktur nicht zumutbar ist,

3. an der Übermittlung der Gesundheitsdaten und genetischen Daten ausschließlich Gesundheitsdiensteanbieter beteiligt sind,

4. die Übermittlung der Gesundheitsdaten und genetischen Daten bis 31. Dezember 2024 **in der Regel per Fax** erfolgte und

5. die Drittanbieter, derer sich allenfalls bedient wird, eine Niederlassung in der EU aufweisen[18].

Die erleichterten Bedingungen gelten nicht, wenn Gesundheitsdaten und genetische Daten von einem Auftragsverarbeiter in der Cloud gespeichert werden, d.h. wenn Ressourcen oder Dienste über Netzwerke nicht dediziert einem Kunden zur Verfügung gestellt werden. Die erleichterten Bedingungen kämen jedoch bei der Verwendung eines dedizierten Servers eines Auftragsverarbeiters zur Anwendung.

Gelten **für einen** der an einer Übermittlung von Gesundheitsdaten und genetischen Daten beteiligten Gesundheitsdiensteanbieter diese erleichterten Bedingungen, so gelten sie für alle beteiligten Gesundheitsdiensteanbieter („Einer-für-alle"-Prinzip).

4. Zusammenfassung und Checkliste

Zusätzlich zu den Bestimmungen der DSGVO sind bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten durch Gesundheitsdiensteanbieter (z.B. durch Ärzte und durch Apotheken) die Datensicherheitsmaßnahmen nach Gesundheitstelematikgesetz 2012 (GTelG 2012) einzuhalten. Nach zwanzig Jahren ist bezüglich der im GTelG 2012 vorgesehenen Datensicherheitsmaßnahmen die Ausnahmeregelung für Faxe ausgelaufen, da die Nutzung sicherer Kommunikationsmittel nicht mehr unzumutbar ist (und sich die technischen Rahmenbedingungen der Faxübermittlung wesentlich verändert haben). **Die Übermittlung von Gesundheitsdaten und genetischen Daten durch Gesundheitsdiensteanbieter per Fax ist daher nicht mehr zulässig.**

Nach dem Inhouse-Privileg unterliegen lokale Datenverarbeitungen innerhalb eines Gesundheitsdiensteanbieters und konzerninterne Übermittlungen in abgeschlossenen und abgesicherten Systemen nur ausgewählten Verpflichtungen (IT-Sicherheitskonzept nach Punkt 3.1, Übermittlung auf Basis einer Rechtsgrundlage nach DSGVO nach Punkt 3.3 und Nachweis der Identität jener Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen, nach Punkt 3.4). Die Pflichten der Gesundheitsdiensteanbieter nach GTelG 2012, die kumulativ erfüllt werden müssen, sind in der folgenden Checkliste zusammengefasst.

[18] Nach § 27 Abs 20 Z 4 lit b gelten die erleichterten Bedingungen nur, „sofern Art. 3 Abs. 1 DSGVO eingehalten wird". Nach den Gesetzesmaterialien (ErläutRV 2530 BlgNR 27. GP 21) bedeutet diese sprachlich unglückliche Formulierung, dass „Drittanbieter, derer sich allenfalls bedient wird, dem räumlichen Anwendungsbereich gemäß Art. 3 Abs. 1 der DSGVO unterliegen" müssen. Art 3 Abs 1 DSGVO unterliegen Einrichtungen, die eine Niederlassung in der Union haben.

Checkliste für die elektronische Übermittlung von Gesundheitsdaten und genetischen Daten durch Gesundheitsdiensteanbieter

Stichwort	**Kurzbeschreibung**	**Erfüllt? (Ja/Nein)**
IT-Sicherheitskonzept (Punkt 3.1)	Wurde ein IT-Sicherheitskonzept erstellt und sind die auf diesem IT-Sicherheitskonzept basierenden Sicherheitsmaßnahmen dokumentiert?	
Zugriffs- und Berechtigungssystem (Punkt 3.2)	Wird innerhalb eines Gesundheitsdiensteanbieters ein Zugriffs- und Berechtigungssystem eingesetzt?	
Zulässigkeit der Übermittlung (Punkt 3.3)	Liegt für die Übermittlung ein Ausnahmetatbestand nach Art 9 Abs 2 DSGVO und eine Rechtsgrundlage nach Art 6 Abs 1 DSGVO vor?	
Identität der betroffenen Person und der beteiligten Gesundheitsdiensteanbieter (Punkt 3.4)	Kann die Identität der betroffenen Person (bei gerichteter Kommunikation) oder die eindeutige Identität der betroffenen Person (bei ungerichteter Kommunikation) und die eindeutige Identität der an der Übermittlung beteiligten Gesundheitsdiensteanbieter nachgewiesen werden?	
	Wenn nein: Ist der Nachweis der Identität der beteiligten Gesundheitsdiensteanbieter mangels vorhandener technischer Infrastruktur nicht zumutbar und können die Identitäten und maßgeblichen Rollen der an der Übermittlung beteiligten Gesundheitsdiensteanbieter gegenseitig bestätigt werden?	

Rolle der Gesundheitsdiensteanbieter (Punkt 3.5)	Kann die Rolle der an der Übermittlung beteiligten Gesundheitsdiensteanbieter nachgewiesen werden?	
	Wenn nein: Ist der Nachweis der Rolle der beteiligten Gesundheitsdiensteanbieter mangels vorhandener technischer Infrastruktur nicht zumutbar und können die Identitäten und maßgeblichen Rollen der an der Übermittlung beteiligten Gesundheitsdiensteanbieter gegenseitig bestätigt werden?	
Integrität (Punkt 3.6)	Werden fortgeschrittene oder qualifizierte elektronische Signaturen oder fortgeschrittene oder qualifizierte elektronische Siegel zum Nachweis der Integrität verwendet oder erfolgt die Übermittlung über ein abgesichertes Netzwerk?	
	Wenn nein: Ist der Nachweis der Integrität mangels vorhandener technischer Infrastruktur nicht zumutbar und können die Identitäten und maßgeblichen Rollen der an der Übermittlung beteiligten Gesundheitsdiensteanbieter gegenseitig bestätigt werden?	
Vertraulichkeit (Punkt 3.7)	Erfolgt die Übermittlung der Daten über abgesicherte Netzwerke oder über Protokolle und Verfahren, die die vollständige Verschlüsselung der Daten bewirken?	
	Wenn nein (bis 30. Juni 2026): Wird 1. eine Transportverschlüsselung verwendet, ist 2. die Sicherstellung der Vertraulichkeit mangels vorhandener technischer Infrastruktur nicht zumutbar, sind 3. an der Übermittlung ausschließlich	

	Gesundheitsdiensteanbieter beteiligt, erfolgte 4. die Übermittlung der Daten bis 31. Dezember 2024 in der Regel per Fax und haben 5. allfällige Dienstleister eine Niederlassung in der EU?	

Mit freundlichen Grüßen
Dr. Gerald Trieb, LL.M.

Anhang 1: Liste der Rollen nach Gesundheitstelematikverordnung 2013 (Stand: 25.2.2025)

Teil 1: Rollen für Personen

- Ärztin/Arzt für Allgemeinmedizin, gegebenenfalls unter Beifügung der gemäß Ärztinnen-/Ärzte-Ausbildungsordnung 2006 zutreffenden Zusatzbezeichnung des Additivfaches in runden Klammern
- Approbierte Ärztin/Approbierter Arzt
- Fachärztin/Facharzt, unter Beifügung der gemäß ÄAO 2006 zutreffenden Berufsbezeichnung (Sonderfach sowie als Zusatzbezeichnung das Additivfach/die Additivfächer in runden Klammern)
- Fachärztin/Facharzt, unter Beifügung der gemäß Ärztinnen-/Ärzte-Ausbildungsordnung 2015 zutreffenden Berufsbezeichnung (Sonderfach in runden Klammern)
- Fachärztin/Facharzt für Zahn-, Mund- und Kieferheilkunde
- Turnusärztin/Turnusarzt
- Ärztin/Arzt mit partiellem Berufszugang
- Zahnärztin/Zahnarzt

- Dentistin/Dentist
- Psychotherapeutin/Psychotherapeut
- Klinische Psychologin/Klinischer Psychologe
- Gesundheitspsychologin/Gesundheitspsychologe
- Musiktherapeutin/Musiktherapeut
- Hebamme
- Physiotherapeutin/Physiotherapeut
- Biomedizinische Analytikerin/Biomedizinischer Analytiker
- Radiologietechnologin/Radiologietechnologe
- Diätologin/Diätologe
- Ergotherapeutin/Ergotherapeut
- Logopädin/Logopäde
- Orthoptistin/Orthoptist
- Diplomierte Gesundheits- und Krankenpflegerin/Diplomierter Gesundheits- und Krankenpfleger
- Heilmasseurin/Heilmasseur
- Diplomierte Kardiotechnikerin/Diplomierter Kardiotechniker
- Pflegeassistenz
- Pflegefachassistenz
- Operationstechnische Assistenz

Teil 2: Rollen für Organisationen

- Allgemeine Krankenanstalt
- Sonderkrankenanstalt
- Pflegeanstalt
- Sanatorium
- Selbstständiges Ambulatorium
- Ärztliche Gruppenpraxis
- Zahnärztliche Gruppenpraxis
- Straf- und Maßnahmenvollzug
- Öffentliche Apotheke
- Pflegeeinrichtung
- Mobile Pflege
- Kuranstalt
- Untersuchungsanstalt
- Gewebebank
- Gewebeentnahmeeinrichtung
- Blutspendeeinrichtung
- Rettungsdienst
- Arbeitsmedizinisches Zentrum

- Augen- und Kontaktlinsenoptik
- Hörgeräteakustik
- Orthopädische Produkte
- Zahntechnik
- Gesundheitsmanagement
- Öffentlicher Gesundheitsdienst
- ELGA-Ombudsstelle
- eHealth-Servicestelle
- Widerspruchstelle
- Patientenvertretung
- Sozialversicherung
- Krankenfürsorge
- Gesundheitsversicherung
- Verrechnungsservice
- IKT-Gesundheitsservice
- Primärversorgungseinheit
- Medizinproduktehersteller
- Gesundheitsberatung 1450
- Ärztlicher Bereitschaftsdienst

- Ärztebereitstellungsdienst gemäß § 45 Abs. 3 Ärztegesetz 1998
- Telemedizinischer Dienst
- National Contact Point (NCP)
- Schulgesundheitspflege