www.manz.at/rdm

# RECHT DER MEDIZIN

RdM

mit Beilage Ökonomie & Gesundheit

*Schriftleitung* Christian Kopetzki

*Redaktion* Gerhard Aigner, Erwin Bernat, Daniel Ennöckl, Meinhild Hausreither, Thomas Holzgruber, Dietmar Jahnel, Matthias Neumayr, Magdalena Pöschl, Reinhard Resch, Hannes Schütz, Lukas Stärker, Karl Stöger, Felix Wallner, Johannes Zahrl

Oktober 2019 05

161 – 204



ISSN 1022-9434 Österreichische Post AG PZ 06Z036885 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

MANZ

# Rechtskonforme elektronische Übermittlung von Gesundheitsdaten und genetischen Daten

## Zum Anwendungsbereich des GTelG 2012

Die elektronische Übermittlung von personenbezogenen Daten ist in der heutigen Zeit selbstverständlich und das Thema Datenschutz spätestens seit Ingeltungtreten der DSGVO wohlbekannt. Weniger bekannt – aber nicht weniger bedeutend – ist, dass der österr Gesetzgeber im Gesundheitstelematikgesetz 2012 (GTelG 2012) nicht nur die Elektronische Gesundheitsakte, sondern auch Datensicherheitsmaßnahmen bei der Übermittlung elektronischer Gesundheitsdaten und genetischer Daten durch Gesundheitsdiensteanbieter regelt, deren Missachtung unter die Strafdrohung des Art 83 DSGVO fällt.

**Von Eva-Maria Pfandlsteiner, Claudia Gabauer und Gerald Trieb**

RdM 2019/103

Art 4, 9, 32 DSGVO; GTelG 2012; GTelV 2013

Gesundheitsdaten;
genetische Daten;
Gesundheitsdiensteanbieter;
Gesundheitstelematik;
Cloud Computing

Inhaltsübersicht:



## A. Der Anwendungsbereich des GTelG 2012

Gem § 1 Abs 1 ist Gegenstand des GTelG 2012[1] die Verarbeitung (Art 4 Z 2 DSGVO[2]) personenbezogener elektronischer Gesundheitsdaten und genetischer Daten (Art 4 Z 15 und Z 13 DSGVO) durch die Gesundheitsdiensteanbieter (GDA) gem § 2 Z 2. Es handelt sich beim GTelG 2012 um eine datenschutzrechtliche lex specialis, weshalb die Begriffe im Zweifelsfall im Lichte der DSGVO und des DSG[3] auszulegen sind.[4] Auch die Bestimmungen des 2. Abschnitts des GTelG 2012 betreffend die Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten gehen den allgemeinen Datensicherheitsmaßnahmen gem Art 32 DSGVO vor.[5] Die Zulässigkeit der nationalen Ausgestaltung von Datensicherheitsmaßnahmen im Rahmen der Verarbeitung von Gesundheitsdaten und genetischen Daten stützt sich auf die Öffnungsklausel des Art 9 Abs 4 DSGVO. Die Bestimmungen des GTelG 2012 sind nicht dispositiv und können daher auch nicht von den beteiligten Personen abbedungen werden.

**Praxistipp**

Die Praxis, eine unverschlüsselte Übermittlung von Befunden per E-Mail auf eine Einwilligung des Patienten zu stützen, ist rechtlich unzulässig. Nach zutreffender Ansicht der Datenschutzbehörde ist die Frage, ob eine Übermittlung in verschlüsselter oder unverschlüsselter Form erfolgt, eine Frage der Datensicherheitsmaßnahme und als solche allein vom Verantwortlichen zu beurteilen und keiner Einwilligung der betroffenen Person zugänglich.[6] Die Pflicht zur Verschlüsselung der Gesundheitsdaten und genetischen Daten im Fall einer Übermittlung

1) Gesundheitstelematikgesetz 2012 – GTelG 2012 BGBl I 2012/111 idF BGBl I 2018/100.
2) VO (EU) 2016/679 des Europäischen Parlaments und des Rates v 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1 idF ABl L 2016/314, 72.
3) Datenschutzgesetz – DSG BGBl I 1999/165 idF BGBl I 2019/14.
4) Vgl ErläutRV 1936 BlgNR 24. GP 17.
5) Vgl *Gabauer,* Datenschutzrechtliche Anforderungen im Gesundheitsbereich, RdM 2019, 84 (86).
6) Vgl DSB 16. 11. 2018, DSB-D213.692/0001-DSB/2018 RdM-LS 2019/73 = RdM 2019, 84 *(Gabauer)* = Dako 2019, 43 *(Haidinger)* = jusIT 2019, 128 *(Jahnel)* = MR 2019, 75 *(Knotzer).*

per E-Mail durch GDA resultiert bereits aus den Datensicherheitsbestimmungen des GTelG 2012, die nicht abbedungen werden können.[7]

Nach Ansicht des Gesetzgebers sind Verstöße gegen Bestimmungen des 2. Abschnitts des GTelG 2012 unter die Strafdrohung des Art 83 DSGVO zu subsumieren, weshalb die Verwaltungsstrafbestimmungen des § 25 GTelG 2012 idF BGBl I 2012/111 – bis auf eine Ausnahme[8] – mit dem 2. Materien-Datenschutz-Anpassungsgesetz 2018[9] gestrichen wurden.[10]

## 1. Elektronische Gesundheitsdaten und genetische Daten

### a) Gesundheitsdaten

Das GTelG 2012 idF BGBl I 2012/111 normierte in seinem § 2 Z 1 eine Definition von Gesundheitsdaten,[11] die aufgrund des unionsrechtlichen Transformationsverbots im Zuge des 2. Materien-Datenschutz-Anpassungsgesetzes 2018 durch einen Verweis auf die Definition in Art 4 Z 15 DSGVO ersetzt wurde.[12] Gem Art 4 Z 15 DSGVO sind Gesundheitsdaten personenbezogene 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. ErwGr 35 führt näher aus, welche Daten zu den personenbezogenen Gesundheitsdaten zählen sollen. Insgesamt gesehen ist die Definition sehr weit: Sobald Rückschlüsse auf die Gesundheit einer identifizierbaren Person gezogen werden können, liegt ein Gesundheitsdatum vor. Von der Definition umfasst sind daher nicht nur offensichtliche Fälle (Entlassungsbriefe, Medikationsdaten, Laborbefunde), sondern bspw auch Arzt-Terminerinnerungen oder Protokolldaten, die sowohl den Namen des Patienten als auch den des Arztes enthalten.

Ein Teil der Literatur[13] qualifiziert auch die Sozialversicherungsnummer (SVNR) als ein Gesundheitsdatum, da es sich dabei um eine Nummer handelt, die einer natürlichen Person zugeteilt wurde, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren (vgl ErwGr 35). Tatsächlich ist die SVNR eines der wichtigsten Identifikationsmerkmale im Gesundheitswesen,[14] allerdings gehen aus ihr per se keine Informationen über den Gesundheitszustand der betroffenen Person hervor.[15] Da der entsprechende Passus in ErwGr 35 im Wortlaut des Art 4 Z 15 DSGVO keine Deckung findet, stehen die rechtlich nicht verbindlichen[16] ErwGr im Widerspruch zum Normtext. Ein Teil der Literatur[17] versucht diesen Widerspruch dadurch aufzulösen, dass sie die Qualifikation der SVNR kontextbezogen beurteilt und das Vorliegen eines Gesundheitsdatums nur im Fall der Inanspruchnahme von Gesundheitsdienstleistungen bejaht. Dieser Ansicht schließt sich auch die Datenschutzbehörde in einem – nicht rechtskräftigen – Bescheid an.[18] Unabhängig von der Qualifikation als Gesundheitsdatum ist zu beachten, dass die SVNR nach stRsp nicht als „genereller Identifikator" – dh in Zusammenhängen, die mit sozialversicherungsrechtlichen Sachverhalten nichts zu tun haben – eingesetzt werden darf.[19]

### b) Genetische Daten

Genetische Daten waren vor dem Wirksamwerden der DSGVO den Gesundheitsdaten zuordenbar; da die DSGVO sie aber eigenständig in den Katalog besonderer Kategorien personenbezogener Daten iSd Art 9 Abs 1 DSGVO aufnimmt und sie in Art 4 Z 13 legaldefiniert, musste zum Erhalt der notwendigen Rechtsgrundlage für die elektronische Verarbeitung von genetischen Daten und entsprechend dem unionsrechtlichen Transformationsverbot deren Definition ins GTelG 2012 aufgenommen werden (vgl § 2 Z 1a GTelG 2012).[20] In der Praxis hat die Aufnahme der genetischen Daten ins GTelG 2012 jedoch keine Auswirkungen, weil die entsprechenden Bestimmungen des GTelG 2012 schon vor Wirksamwerden der DSGVO eingehalten werden mussten, wenn genetische Daten (als Gesundheitsdaten iSd § 2 Z 1 GTelG 2012 idF BGBl I 2012/111) verarbeitet wurden.

## 2. Elektronische Übermittlung

Die Bestimmungen des 2. Abschnitts betreffend die Datensicherheit gelten gem § 3 Abs 1 GTelG 2012 für alle Formen der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten (gerichtete[21] und ungerichtete[22] Kommunikation) durch GDA,

7) Vgl § 6 Abs 1 Z 2 GTelG 2012; *Gabauer,* RdM 2019, 86; *Jahnel,* DSB: Amtswegiges Prüfverfahren gegen eine Allergie-Tagesklinik, jusIT 2019, 128 (129).
8) Vgl § 25 GTelG 2012, wonach eine Schlechterstellung von Personen im Zugang zur medizinischen Versorgung oder hinsichtlich der Kostentragung entgegen § 16 Abs 3 GTelG 2012 eine Verwaltungsübertretung darstellt und mit bis zu € 10.000,– geahndet wird.
9) BGBl I 2018/37.
10) Vgl ErläutRV 108 BlgNR 26. GP 76.
11) „Gesundheitsdaten": personenbezogene Daten gem § 4 Z 1 DSG 2000 über die physische oder psychische Befindlichkeit eines Menschen, einschließlich der iZm der Erhebung der Ursachen für diese Befindlichkeit sowie der Vorsorge oder Versorgung, der Diagnose, Therapie- oder Pflegemethoden, der Pflege, der verordneten oder bezogenen Arzneimittel („Medikationsdaten"), Heilbehelfe oder Hilfsmittel, der Verrechnung von Gesundheitsdienstleistungen oder der für die Versicherung von Gesundheitsrisiken erhobenen Daten (vgl § 2 Z 1 GTelG 2012 idF BGBl I 2012/111).
12) Vgl ErläutRV 108 BlgNR 26. GP 74.
13) Vgl *Feiler/Forgó,* EU-DSGVO Kurzkommentar (2017) Art 4 Rz 35; *Kallab/Wozniak,* Datenschutzrechtliche Neuerungen und deren Auswirkungen im Gesundheitsbereich, ZfG 2018, 54 (FN 11); *Pilgermair,* Auswirkungen der Datenschutz-Grundverordnung auf den Gesundheits- und Sozialbereich (Teil I), ÖZPR 2017, 96 (97).
14) Vgl ErläutRV 1936 BlgNR 24. GP 31.
15) Vgl auch *Hörtnagl-Donner,* SVNR als Gesundheitsdatum? ZIIR 2018, 350 (350).
16) Siehe EuGH C-162/97, *Nilsson,* Rn 54.
17) Vgl *Hödl* in *Knyrim,* DatKomm Art 4 DSGVO Rz 157 (Stand 1. 12. 2018, rdb.at).
18) DSB 9. 4. 2019, DSB-D123.526/0001-DSB/2019 ZIIR 2019, 259 *(Schweiger).*
19) Vgl DSB 28. 6. 2017, DSB-D213.541/0005-DSB/2017 mwN; BVwG 11. 6. 2018, W211 2161456-1.
20) ErläutRV 108 BlgNR 26. GP 74.
21) Bei der gerichteten Kommunikation erfolgt die Datenübermittlung an im Vorhinein bestimmte Empfänger, vgl ErläutRV 1936 BlgNR 24. GP 5.
22) Bei der ungerichteten Kommunikation erfolgt die Datenübermittlung nicht direkt an bestimmte Empfänger, sondern über eine sog „Datendrehscheibe", wo Daten zur Verfügung gestellt und von Berechtigten abgerufen werden können, vgl ErläutRV 1936 BlgNR 24. GP 5.

nicht jedoch für die bloße (lokale) Verarbeitung dieser Datenkategorien.[23]

Und so wie die im 2. Abschnitt des GTelG 2012 normierten Datensicherheitsmaßnahmen keine Anwendung auf die lokale Verarbeitung von Gesundheitsdaten und genetischen Daten finden, sind sie auch nicht auf die nicht-elektronische Übermittlung von elektronischen Gesundheitsdaten und genetischen Daten anzuwenden. Eine gegenteilige Ansicht wird von *Burgstaller/Kolmhofer*[24] vertreten, die zur Argumentation § 6 GTelG 2012 heranziehen, der zur Sicherstellung der Vertraulichkeit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten entweder (Z 1) die Durchführung über ein entsprechendes Netzwerk oder (Z 2) außerhalb dieses Netzwerks die Verwendung bestimmter Protokolle und Verfahren fordert. Da die Übermittlung von Gesundheitsdaten und genetischen Daten außerhalb eines Netzwerks laut Ansicht der beiden Autoren zu einem bestimmten Zeitpunkt immer physisch erfolgen müsse, wäre die Differenzierung in § 6 Abs 1 GTelG 2012 sinnlos, würde der 2. Abschnitt des GTelG 2012 nicht auch auf die physische Übermittlung elektronischer Gesundheitsdaten und genetischer Daten anzuwenden sein.

Diese Ansicht ist entschieden abzulehnen. Aus der Systematik des GTelG 2012 ist ersichtlich, dass die Intention des Gesetzgebers die Regelung entsprechender Datensicherheitsmaßnahmen bei der elektronischen (im Gegensatz zur physischen) Übermittlung von Gesundheitsdaten und genetischen Daten war und ist: ZB ist eine Voraussetzung für das Vorliegen der GDA-Eigenschaft die Verarbeitung von Gesundheitsdaten und genetischer Daten in elektronischer Form (vgl § 2 Z 2 GTelG 2012). Werden die Gesundheitsdaten und genetischen Daten nicht durch GDA verarbeitet, ist der Anwendungsbereich des GTelG 2012 gar nicht erst eröffnet. Würde der Gesetzgeber also zwar die GDA-Eigenschaft an die Verarbeitung von Gesundheitsdaten und genetischen Daten in elektronischer Form knüpfen, gleichzeitig aber auch die Intention verfolgen, die nicht-elektronische Übermittlung von Gesundheitsdaten und genetischen Daten zu regeln, wäre dies ein Systembruch; eine diesbezügliche Unterstellung überzeugt daher nicht. Im Übrigen lautet die Überschrift des 2. Abschnitts „Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten (Art 4 Z 15 und Z 13 DSGVO)“ und regelt § 6 Abs 1 GTelG 2012 ja gerade die Vertraulichkeit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten (vgl Satz 1 leg cit) und kann diese auch durch bestimmte Protokolle und Verfahren „außerhalb eines Netzwerks“[25] sichergestellt werden. Ein Beispiel für die Sicherstellung der Vertraulichkeit durch Protokolle und Verfahren iSd § 6 Abs 1 Z 2 GTelG 2012 bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten ist die Verschlüsselung von E-Mails zwischen zwei GDA mit S/MIME.[26] Kein Beispiel ist die Übermittlung von verschlüsselten Gesundheitsdaten auf einem USB-Stick per Post, selbst wenn sowohl Absender als auch Empfänger GDA wären. Diese Übermittlung hat jedoch den allgemeinen Datensicherheitsanforderungen gem Art 32 DSGVO zu entsprechen.

Der Vollständigkeit halber sei erwähnt, dass eine Anwendung der im 2. Abschnitt des GTelG 2012 normierten Datensicherheitsmaßnahmen auf die nicht-elektronische Übermittlung von Gesundheitsdaten und genetischen Daten faktisch nicht möglich ist, da sie zwingend eine elektronische Übermittlung voraussetzen (vgl etwa § 4 Abs 4 GTelG 2012).[27]

## 3. Gesundheitsdiensteanbieter

Die Anwendbarkeit des 2. Abschnitts des GTelG 2012 setzt eine elektronische Übermittlung von Gesundheitsdaten und genetischen Daten „durch GDA“ voraus. Keine Voraussetzung ist, dass es sich beim Empfänger der übermittelten elektronischen Gesundheitsdaten und genetischen Daten ebenfalls um einen GDA handelt (dies ist allenfalls für die erleichterten Bedingungen gem § 27 Abs 10 bis 14 GTelG 2012 relevant), sodass die entsprechenden Bestimmungen des 2. Abschnitts auch bei der gerichteten Kommunikation zwischen Arzt und Patient einzuhalten sind.[28]

**Beispiele**

Die Bestimmungen des 2. Abschnitts des GTelG 2012 betreffend die Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten gelten zB für folgende Konstellationen:

- elektronische Übermittlung von Gesundheitsdaten oder genetischen Daten zwischen mehreren GDA als Verantwortlichen iSd Art 4 Z 7 DSGVO (zB Übermittlung eines Befunds eines Facharztes an den Hausarzt eines Patienten über das Gesundheitsinformationsnetz oder per E-Mail; Übermittlung von Entlassungsdokumenten durch eine Krankenanstalt an den Zuweiser im Rahmen von Befundkommunikationssystemen[29]);
- Offenlegung von Gesundheitsdaten oder genetischen Daten durch einen GDA an einen Auftragsverarbeiter iSd Art 4 Z 8 DSGVO (zB Speicherung von Patientendaten in der Cloud);
- Offenlegung von Gesundheitsdaten oder genetischen Daten durch GDA an Patienten (zB Übermittlung von Befunddaten per E-Mail oder via Plattform zum Download; Kommunikation zwischen Arzt und Patient via Plattform oder App; Erinnerung an Patienten zu Vorsorge- und Kontrolluntersuchungen; Impferinnerungen via Recall-Systemen).

23) ErläutRV 1936 BlgNR 24. GP 21.
24) *Burgstaller/Kolmhofer,* Die Anwendbarkeit der Vertraulichkeitsvorgaben aus dem GTelG: Elektronische Weitergabe von Gesundheitsdaten, ZIIR 2017, 261 (261 f).
25) *Burgstaller/Kolmhofer,* ZIIR 2017, 261.
26) Secure / Multipurpose Internet Mail Extensions.
27) *Gabauer,* Rechtliche Rahmenbedingungen von Mobile-Health-Diensten („mHealth“) (Wiener rechtswissenschaftliche Dissertation 2018) 194 f.
28) Vgl *Gabauer,* RdM 2019, 84 (86 mwN); im Ergebnis auch *Jahnel,* jusIT 2019, 129; *Kopetzki,* Editorial: Datenschutzrecht – Wohltat oder Plage? RdM 2019, 81.
29) Vgl ErläutRV 1936 BlgNR 24. GP 21.

### a) Zur Definition „GDA"

§ 2 Z 2 GTelG 2012 definiert GDA als Verantwortliche oder Auftragsverarbeiter (Art 4 Z 7 und 8 DSGVO), die regelmäßig Gesundheitsdaten oder genetische Daten in elektronischer Form, in einer in der Anlage 1 der GTelV 2013[30] festgelegten Rolle, zu einem der folgenden Zwecke verarbeiten:

- (lit a) medizinische Behandlung oder Versorgung,
- (lit b) pflegerische Betreuung,
- (lit c) Verrechnung von Gesundheitsdienstleistungen,
- (lit d) Versicherung von Gesundheitsrisiken,
- (lit e) Wahrnehmung von Patient/inn/en/rechten.

Dem Begriff der Gesundheitsdienstleistung ist ein weites Verständnis zu unterstellen. Ein Indiz für das Vorliegen der GDA-Eigenschaft ist das zugrunde liegende Berufsrecht: Ist dieses dem Gesundheitsrecht im weiteren Sinn zuzuordnen, liegt eine GDA-Eigenschaft vor.[31] Im Sinne dieses weiten Verständnisses ist eine unionsrechtliche Auslegung opportun: Gem Art 3 lit f der Patientenmobilitäts-RL 2011/24/EU[32] ist ein „Angehöriger der Gesundheitsberufe" nicht nur ein Arzt, eine Krankenschwester oder ein Krankenpfleger für allgemeine Pflege, ein Zahnarzt, eine Hebamme oder ein Apotheker iS der RL 2005/36/EG,[33] sondern auch eine andere Fachkraft, die im Gesundheitsbereich Tätigkeiten ausübt, die einem reglementierten Beruf iSv Art 3 Abs 1 lit a der RL 2005/36/EG vorbehalten sind, oder eine Person, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehörige der Gesundheitsberufe gilt.

GDA iSd § 2 Z 2 GTelG 2012[34] sind aus diesem Grund nicht nur Angehörige der „klassischen Gesundheitsberufe"[35] wie Ärzte, Apotheker, Hebammen, Logopäden, Physiotherapeuten udgl, sondern zB auch Medizinproduktehersteller, da es sich bei der Herstellung und Aufbereitung sowie dem Handel mit Medizinprodukten um ein reglementiertes Gewerbe[36] und um eine Tätigkeit im Gesundheitsbereich handelt.

Dass der Begriff GDA weit auszulegen ist, wird auch dadurch verdeutlicht, dass laut den Erläuternden Bemerkungen[37] sogar Rechtsanwälte und Notare als GDA anzusehen sind, wenn sie im Bereich der Patientenrechte spezialisiert sind. Von der Definition umfasst sind auch IT-Unternehmen, die im Auftrag eines GDA Gesundheitsdaten oder genetische Daten verarbeiten,[38] weil sie etwa Verrechnungs- oder Speicherdienstleistungen erbringen. Voraussetzung ist aber auch hier, dass das IT-Unternehmen regelmäßig Gesundheitsdaten oder genetische Daten verarbeitet (vgl § 2 Z 2 GTelG 2012), weswegen die bloße Möglichkeit, Gesundheitsdaten oder genetische Daten – etwa bei der Wartung des Softwareprodukts – unbeabsichtigt (und nicht vom Auftrag des verantwortlichen GDA gedeckt) einzusehen, wohl nicht zur Klassifikation als GDA führt.

### b) Rolle iSd GTelV 2013

Neben der regelmäßigen Verarbeitung der Gesundheitsdaten und genetischen Daten in elektronischer Form zu den festgelegten Zwecken ist eine weitere Voraussetzung für das Vorliegen der GDA-Eigenschaft, dass für die Verarbeitung eine Rolle iSd Anlage 1 der GTelV 2013 verwendet wird (vgl § 2 Z 2 GTelG 2012), da gem § 3 Abs 3 Satz 1 GTelG 2012 die Zulässigkeit, Gesundheitsdaten oder genetische Daten zu verarbeiten, mittels Rollen abzubilden ist. Eine Rolle ist gem § 2 Z 5 GTelG 2012 eine Klassifizierung von GDA nach der Art ihres Aufgabengebiets, ihrer Erwerbstätigkeit, ihres Betriebszwecks oder ihres Dienstleistungsangebots. Die GTelV 2013 differenziert zwischen „Rollen für Personen"[39] und „Rollen für Organisationen".[40]

Gem § 3 Abs 3 Satz 2 GTelG 2012 haben GDA technisch zu gewährleisten, dass es keine Verarbeitung von Gesundheitsdaten oder genetischen Daten außerhalb der zulässigen Rollen gibt. Die Rollen sind in Anlage 1 der GTelV 2013 abschließend aufgezählt (vgl § 2 Abs 1 GTelV 2013), allerdings haben gem § 3 Abs 1 GTelV 2013 Verantwortliche oder Auftragsverarbeiter, die zur Auffassung kommen, dass ihre Tätigkeit keiner Rolle der Anlage 1 zugeordnet werden kann, bei einer Registrierungsstelle gem § 9 Abs 3 GTelG 2012 die Eintragung einer neuen Rolle zu beantragen. So existiert derzeit zB keine entsprechende Rolle für Medizinproduktehersteller, was durch einen entsprechenden Antrag dieses Gesundheitsdienstleisters und einer damit einhergehenden Novellierung der GTelV 2013 zu ändern wäre.

**Praxistipp**

Die Bestimmungen des 2. Abschnitts des GTelG 2012 gelten auch für jene Gesundheitsdienstleister, deren Tätigkeit keiner Rolle der Anlage 1 der

30) Gesundheitstelematikverordnung 2013 – GTelV 2013 BGBl II 2013/506.
31) ErläutRV 1936 BlgNR 24. GP 18.
32) RL 2011/24/EU des Europäischen Parlaments und des Rates v 9. 3. 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung, ABl L 2011/88, 45 idF ABl L 2013/353, 8.
33) RL 2005/36/EG des Europäischen Parlaments und des Rates v 7. 9. 2005 über die Anerkennung von Berufsqualifikationen, ABl L 2005/255, 22 idF ABl L 2013/354, 132.
34) Allenfalls iVm § 3 Abs 1 GTelV 2013.
35) Vgl *BMASGK,* Gesundheitsberufe in Österreich 2019, https://broschuerenservice.sozialministerium.at//Home/Download?publicaHonId=489 (abgefragt am 1. 9. 2019).
36) Vgl § 94 Z 33 Gewerbeordnung 1994 – GewO 1994 BGBl 1994/194 idF BGBl I 2018/112; § 1 Medizinprodukteverordnung BGBl II 2003/129 idF BGBl II 2008/399.
37) ErläutRV 1936 BlgNR 24. GP 18.
38) ErläutRV 1936 BlgNR 24. GP 18.
39) Arzt für Allgemeinmedizin, Approbierter Arzt, Facharzt unter Beifügung der gemäß ÄAO 2006 zutreffenden Berufsbezeichnung, Facharzt für Zahn-, Mund- und Kieferheilkunde, Zahnarzt, Dentist, Psychotherapeut, Klinischer Psychologe, Gesundheitspsychologe, Musiktherapeut, Hebamme, Physiotherapeut, Biomedizinischer Analytiker, Radiologietechnologe, Diätologe, Ergotherapeut, Logopäde, Orthoptist, Diplomierter Gesundheits- und Krankenpfleger, Diplomierter Kinderkrankenpfleger, Diplomierter psychiatrischer Gesundheits- und Krankenpfleger, Heilmasseur, Diplomierter Kardiotechniker.
40) 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, Widerspruchstelle, Patientenvertretung, Sozialversicherung, Krankenfürsorge, Gesundheitsversicherung, Verrechnungsservice, IKT-Gesundheitsservice.

GTelV 2013 zugeordnet werden kann. Die Zulässigkeit der elektronischen Übermittlung von Gesundheitsdaten oder genetischen Daten durch diese Gesundheitsdienstleister setzt daher einen Antrag auf Eintragung einer neuen Rolle an das BMASGK als Registrierungsstelle iSd § 9 Abs 3 Z 3 GTelG 2012 und die Novellierung der GTelV 2013 voraus.

## B. Voraussetzungen für eine elektronische Übermittlung von Gesundheitsdaten und genetischen Daten

GDA dürfen Gesundheitsdaten und genetische Daten gem § 3 Abs 4 GTelG 2012 nur dann übermitteln, wenn

- (Z 1) die Übermittlung gem Art 9 DSGVO zulässig ist,
- (Z 2) die Identität jener Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen, nachgewiesen ist,
- (Z 3) die Identität der an der Übermittlung beteiligten GDA nachgewiesen ist,
- (Z 4) die Rollen der an der Übermittlung beteiligten GDA nachgewiesen sind,
- (Z 5) die Vertraulichkeit der übermittelten Gesundheitsdaten und genetischen Daten gewährleistet ist sowie
- (Z 6) die Integrität der übermittelten Gesundheitsdaten und genetischen Daten gewährleistet ist.

### 1. Zulässigkeit gem Art 9 DSGVO

Damit nicht der falsche Eindruck erweckt wird, dass die bloße Einhaltung der formellen Datensicherheitsmaßnahmen des 2. Abschnitts des GTelG 2012 für die Zulässigkeit der Verarbeitung von Gesundheitsdaten und genetischen Daten ausreichend sei,[41] normiert § 3 Abs 4 Z 1 GTelG 2012 die explizite Voraussetzung der Zulässigkeit der Übermittlung gem Art 9 DSGVO. Art 9 Abs 1 DSGVO statuiert ein generelles Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten, wie zB von Gesundheitsdaten und genetischen Daten. Art 9 Abs 2 DSGVO normiert taxativ Ausnahmetatbestände, für die das Verarbeitungsverbot des Abs 1 nicht gilt. Die Zulässigkeit der Verarbeitung von besonderen Kategorien personenbezogener Daten setzt nach der neueren Literatur[42] sowie nach Ansicht des Europäischen Datenschutzausschusses[43] zusätzlich zu einem Ausnahmetatbestand gem Art 9 Abs 2 DSGVO auch einen Erlaubnistatbestand gem Art 6 Abs 1 DSGVO voraus.

**Beispiele**

- Die Verarbeitung von Gesundheitsdaten im Rahmen der berufsrechtlichen Pflicht zur Führung einer ärztlichen Dokumentation[44] stützt sich auf Art 9 Abs 2 lit h iVm Art 6 Abs 1 lit c DSGVO.
- In medizinischen Notfällen ist eine Verarbeitung von Gesundheitsdaten im lebenswichtigen Interesse der betroffenen Person oder einer anderen natürlichen Person auf Grundlage von Art 9 Abs 2 lit c iVm Art 6 Abs 1 lit d DSGVO rechtmäßig, sofern die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu erteilen.
- Eine Übermittlung von Gesundheitsdaten aufgrund gesetzlicher Meldepflichten[45] zum Zweck öffentlicher Interessen im Bereich der öffentlichen Gesundheit beruht auf Art 9 Abs 2 lit i iVm Art 6 Abs 1 lit c DSGVO.
- Die Verarbeitung von Gesundheitsdaten und genetischen Daten zu wissenschaftlichen Forschungszwecken kann sich im Fall der Verfolgung von öffentlichen Interessen auf Art 9 Abs 2 lit j iVm Art 6 Abs 1 lit e DSGVO iVm § 7 DSG oder iVm den Bestimmungen des 2. Abschnitts des FOG[46] stützen.[47]
- Sofern keine andere Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten oder genetischen Daten in Betracht kommt, ist eine ausdrückliche Einwilligung der betroffenen Person gem Art 9 Abs 2 lit a iVm Art 6 Abs 1 lit a DSGVO erforderlich. Die Übermittlung von personenbezogenen Daten eines Patienten durch den behandelnden Arzt an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Patient steht, ist bereits aufgrund § 51 Abs 2 Z 2 ÄrzteG 1998 einwilligungsbedürftig.

### 2. Identitäts- und Rollennachweis

#### a) Identifikation der betroffenen Person

Die Verpflichtung zur Identifikation der betroffenen Person resultiert aus dem datenschutzrechtlichen Grundsatz der Richtigkeit gem Art 5 Abs 1 lit d DSGVO und soll Verwechslungen mit potenziell weitreichenden Konsequenzen nach Möglichkeit ausschließen.[48] Die konkreten Bestimmungen über die Feststellung der Identität sowie über den – im Fall der ungerichteten Kommunikation erforderlichen – Nachweis

41) Vgl ErläutRV 1936 BlgNR 24. GP 21.
42) Vgl *Bergauer,* Zur Rechtmäßigkeit der (Weiter-)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 2018, 231; *Jahnel/Pallwein-Prettner/Marzi,* Datenschutzrecht² (2018) 73 ff; *Petri* in *Simitis/Hornung/Spieker* (Hrsg), Datenschutzrecht DSGVO mit BDSG (2019) Art 9 Rz 2; *Braun/Hasenauer,* Die Rechtmäßigkeit der Verarbeitung gemäß Art 6 DSGVO, in *Jahnel* (Hrsg), Datenschutzrecht. Jahrbuch 18 (2018) 9 (10); vgl auch OGH 24. 7. 2019, 6 Ob 45/19 i RdM-LS 2019/110; aA *Goricnik,* Replik zu Bergauer, Zur Rechtmäßigkeit der (Weiter-)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 2018/83, jusIT 2019,158 (159 f); ebenfalls nur auf Art 9 Abs 2 DSGVO abstellend DSB 16. 11. 2018, DSB-D213.692/0001-DSB/2018, wonach sich die Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten ausschließlich nach Art 9 Abs 2 DSGVO richtet.
43) *EDSA,* Guidelines 3/2019 on processing of personal data through video devices (version for public consultation; adopted on 10. 7. 2019) Rz 66; *EDSA,* Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der DSGVO (Art 70 Abs 1 lit b) Rz 28, 34.
44) Vgl § 51 Abs 1 ÄrzteG 1998.
45) ZB Epidemiegesetz 1950 BGBl 1950/186 idF BGBl I 2018/37; Tuberkulosegesetz BGBl 1968/127 idF BGBl I 2016/63; Geschlechtskrankheitengesetz StGBl 1945/152 idF BGBl I 2001/98.
46) Forschungsorganisationsgesetz – FOG BGBl 1981/341 idF BGBl I 2018/31.
47) Vgl *Gabauer,* Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken (2019) 59, 89 f, 154.
48) Vgl ErläutRV 1936 BlgNR 24. GP 21.

und die Prüfung der „eindeutigen Identität" der betroffenen Person finden sich in § 4 Abs 1 bis 3 GTelG 2012, die auf das E-Government-Gesetz (E-GovG)[49] verweisen.

#### b) Identifikation der beteiligten GDA

Nachgewiesen und geprüft werden muss auch die Identität der an der Übermittlung beteiligten GDA, wobei § 4 Abs 4 GTelG 2012 eine „eindeutige Identität" iSd § 2 Z 2 E-GovG fordert. Der Nachweis und die Prüfung der eindeutigen Identität haben entweder

- (Z 1) durch Verwendung elektronischer Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen, sowie bereichsspezifische Personenkennzeichen (§ 9 E-GovG) oder
- (Z 2) durch elektronischen Abgleich mit dem eHealth-Verzeichnisdienst (§ 9 GTelG 2012) oder
- (Z 3) durch elektronischen Abgleich mit dem Gesundheitsdiensteanbieterindex (§ 19 GTelG 2012)

zu erfolgen.

Aus Gründen der Patientensicherheit sind gem § 4 Abs 5 GTelG 2012 sowohl die eindeutige Identität von Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen, als auch von GDA mit Hilfe der eindeutigen elektronischen Kennzeichen gem § 8 E-GovG zu speichern.

#### c) Nachweis der Rolle

Der Nachweis und die Prüfung der in der GTelV 2013 definierten Rollen haben gem § 5 Abs 1 iVm § 4 Abs 4 GTelG 2012 in derselben Form wie der Nachweis und die Prüfung der Identität der GDA zu erfolgen. Scheint ein Gesundheitsdienstleister nicht in Anlage 1 der GTelV 2013 auf, ist eine elektronische Übermittlung von Gesundheitsdaten und genetischen Daten bis zur Aufnahme dieser Rolle in die GTelV 2013 nicht zulässig, sofern er sonst in den Anwendungsbereich des GTelG 2012 fällt.

### 3. Gewährleistung der Vertraulichkeit und der Integrität

#### a) Vertraulichkeit

Die Anforderungen an die Vertraulichkeit finden sich in § 6 GTelG 2012, der unterschiedliche technische Lösungen und Rahmenbedingungen berücksichtigt.[50]

Die Vertraulichkeit kann entweder gem § 6 Abs 1 Z 1 GTelG 2012 dadurch sichergestellt werden, dass die elektronische Übermittlung von Gesundheitsdaten und genetischen Daten über Netzwerke durchgeführt wird, die entsprechend dem Stand der Technik in der Netzwerksicherheit gegenüber unbefugten Zugriffen abgesichert sind, indem sie zumindest kumulativ

- (lit a) die Absicherung der Übermittlung von Daten durch kryptographische oder bauliche Maßnahmen,
- (lit b) den Netzzugang ausschließlich für eine geschlossene oder abgrenzbare Benutzergruppe sowie
- (lit c) die Authentifizierung der Benutzer

vorsehen.

Alternativ können gem § 6 Abs 1 Z 2 GTelG 2012 auch Protokolle und Verfahren verwendet werden,

- (lit a) die die vollständige Verschlüsselung der Gesundheitsdaten und genetischen Daten bewirken und
- (lit b) deren kryptographische Algorithmen in der Anlage 2 der GTelV 2013 angeführt sind.

Die Erläuterungen verweisen iZm der zweiten Variante darauf, dass bei bestimmten Datenübermittlungen bzw bei großen Datenmengen (zB datenintensiven Röntgenbildern) auf die Verschlüsselung der eigentlichen Gesundheitsdaten (Bilddaten) verzichtet werden kann, wenn zumindest der Personenbezug so verschlüsselt ist, dass unbefugte Dritte keinen Hinweis auf die betroffene Person ableiten können.[51] § 6 Abs 2 GTelG 2012 normiert in diesem Zusammenhang, dass allenfalls von der Verschlüsselung ausgenommene Informationen weder Hinweise auf die betroffenen Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden, noch auf allfällige Authentifizierungsdaten enthalten dürfen.[52] Da die sicherste Verschlüsselung bei der Übermittlung wirkungslos ist, wenn die Daten an den Endpunkten der Kommunikation unverschlüsselt und für jedermann leicht zugänglich sind, müssen effektive Zugriffskontrollmechanismen (zB Berechtigungsregelungen, Zutrittsbeschränkungen, bauliche Vorkehrungen, verbindliche periodische Sicherheitsaudits) vorgesehen werden, die verhindern, dass die Daten vor Verschlüsselung oder nach Entschlüsselung Unbefugten bekannt werden.[53] Diese Maßnahmen sind gemeinsam mit den gem Art 32 DSGVO getroffenen Datensicherheitsmaßnahmen im IT-Sicherheitskonzept gem § 8 GTelG 2012 detailliert zu dokumentieren.[54] Als Mindestsicherheitsstandard im niedergelassenen ärztlichen Bereich sehen die Gesetzesmaterialien das Gesundheitsinformationsnetz (GIN) an.[55]

#### b) Cloud Computing

§ 6 Abs 3 GTelG 2012 enthält eine Sonderregelung für „Cloud Computing", worunter die Gesetzesmaterialien ganz allgemein das Anbieten bzw Nutzen von Ressourcen oder Diensten, die über Netzwerke zur Verfügung gestellt werden, verstehen.[56] Charakteristisch für Cloud Computing ist weiters, dass Ressourcen oder Dienste nicht unbedingt dediziert einem Kunden zugeordnet, sondern auch dynamisch je nach Bedarf und Vertragsmodell zur Verfügung gestellt werden.[57] Nach § 6 Abs 3 GTelG 2012 ist sicherzustellen, dass die Speicherung von Gesundheitsdaten und genetischen Daten in Datenspeichern, die einem Verantwortlichen (Art 4 Z 7 DSGVO) bedarfsorientiert von einem Auftragsverarbeiter (Art 4 Z 8 DSGVO) bereitgestellt werden („Cloud Computing"), nur dann erfolgt, wenn die Ge-

49) E-Government-Gesetz – E-GovG BGBl I 2004/10 idF BGBl I 2018/104.
50) Vgl ErläutRV 1936 BlgNR 24. GP 23.
51) Vgl ErläutRV 1936 BlgNR 24. GP 23.
52) Die Erläuterungen verweisen in diesem Zusammenhang auf den Namen, die SVNR oder sonstige Daten, aus denen ein direkter Personenbezug abgeleitet werden kann, vgl ErläutRV 1936 BlgNR 24. GP 23.
53) Vgl ErläutRV 1936 BlgNR 24. GP 24.
54) Vgl ErläutRV 1936 BlgNR 24. GP 24.
55) Vgl ErläutRV 1936 BlgNR 24. GP 24.
56) Vgl ErläutRV 1936 BlgNR 24. GP 24.
57) Vgl ErläutRV 1936 BlgNR 24. GP 24.

sundheitsdaten und genetischen Daten mit einem dem aktuellen Stand der Technik entsprechenden Verfahren gem § 6 Abs 1 Z 2 GTelG 2012 verschlüsselt worden sind. GDA, die Gesundheitsdaten und genetische Daten in einer Cloud speichern möchten, müssen daher Protokolle und Verfahren verwenden, die die vollständige Verschlüsselung der Daten bewirken und deren kryptographische Algorithmen der Anlage 2 der GTelV 2013 entsprechen.[58)]

#### c) Integrität

Integrität ist iSv „Unverfälschtheit" oder „Echtheit" der übermittelten Gesundheitsdaten und genetischen Daten zu verstehen.[59)] Nachweis und Prüfung der Integrität elektronischer Gesundheitsdaten und genetischer Daten haben gem § 7 Abs 1 GTelG 2012 durch die Verwendung fortgeschrittener oder qualifizierter elektronischer Signaturen oder fortgeschrittener oder qualifizierter Siegel gemäß VO (EU) 910/2014[60)] zu erfolgen. Diese Bestimmung ist gem § 7 Abs 2 GTelG 2012 nicht auf die elektronische Übermittlung von Gesundheitsdaten und genetischen Daten zwischen GDA anzuwenden, wenn hierzu ein entsprechend dem Stand der Technik abgesichertes Netzwerk gem § 6 Abs 1 Z 1 GTelG 2012 verwendet wird und der Zugang zu diesem Netzwerk ausschließlich für im Vorhinein bekannte GDA möglich ist.

### 4. Inhouse-Privileg

§ 3 Abs 2 GTelG 2012 normiert ein sog „Inhouse-Privileg", wonach bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten innerhalb eines GDA (zB Krankenanstalt, Ordination) die Bestimmungen des § 3 Abs 4 Z 3 bis 6 sowie die §§ 5 bis 7 GTelG 2012 nicht anzuwenden sind, wenn durch effektive und dem Stand der Technik entsprechende Datensicherheits- und Kontrollmaßnahmen unbefugte Dritte vom Zugriff auf Gesundheitsdaten und genetische Daten und somit deren Kenntnisnahme ausgeschlossen werden können. Nach den Gesetzesmaterialien wird diese Voraussetzung insb bei einem entsprechend abgesicherten Intranet gegeben sein.[61)] Im Fall des Inhouse-Privilegs weiterhin anwendbar bleiben etwa die Bestimmungen über die Zulässigkeit der Übermittlung gem Art 9 DSGVO (§ 3 Abs 4 Z 1 GTelG 2012) und über den Nachweis der Identität der betroffenen Person (§ 3 Abs 4 Z 2 iVm § 4 Abs 1 bis 3 und Abs 5 GTelG 2012).

### 5. Erleichterte Bedingungen

§ 27 Abs 10 und 12 GTelG 2012 normieren „erleichterte Bedingungen", wenn der Nachweis oder die Prüfung von Identität, Rollen oder Integrität nach den Bestimmungen des 2. Abschnitts insb mangels vorhandener technischer Infrastruktur nicht zumutbar sind. Diese erleichterten Bedingungen können jedoch nicht in Anspruch genommen werden, wenn die nach dem 2. Abschnitt erforderlichen Maßnahmen im Hinblick auf den Stand der Technik und die Implementierungskosten (Art 32 Abs 1 DSGVO) zumutbar sind.[62)] Im Regelfall wird die Anschaffung der für die Anwendung des 2. Abschnitts erforderlichen Infrastruktur zumutbar sein, sodass sich die Fälle der zulässigen Berufung auf die erleichterten Bedingungen auf wenige Ausnahmefälle beschränken werden.

Der für das Gesundheitswesen zuständige Bundesminister hat nach Anhörung der jeweils zuständigen gesetzlichen Interessenvertretungen mit Verordnung für bestimmte GDA jeweils den Zeitpunkt festzulegen, ab dem die Übermittlung von Gesundheitsdaten und genetischen Daten unter den erleichterten Bedingungen des § 27 Abs 10 und 12 GTelG 2012 jedenfalls nicht mehr zulässig ist (vgl § 28 Abs 4 GTelG 2012). Der Nichterlass dieser Verordnung darf jedenfalls nicht dahingehend interpretiert werden, dass eine Berufung auf die erleichterten Bedingungen per se zulässig wäre. Umgekehrt kann die Unzulässigkeit der Inanspruchnahme der erleichterten Bedingungen bereits aus dem aktuellen Stand der Technik und aus dem – aufgrund der besonderen Schutzbedürftigkeit der Gesundheitsdaten und genetischen Daten – erforderlichen hohen Schutzniveau resultieren (vgl Art 32 Abs 1 DSGVO).

Die erleichterten Bedingungen gelten bei der Übermittlung von Gesundheitsdaten und genetischen Daten für alle beteiligten GDA, wenn für zumindest einen der beteiligten GDA die jeweils erleichterten Bedingungen nach § 27 Abs 10 oder 12 GTelG 2012 gelten.[63)]

#### a) Erleichterter Nachweis der Identität und Rollen

Bei Vorliegen der erleichterten Bedingungen dürfen Gesundheitsdaten und genetische Daten nur übermittelt werden, wenn zumindest die Identitäten und maßgeblichen Rollen der an der Übermittlung beteiligten GDA gegenseitig durch

- (Z 1) persönlichen Kontakt oder
- (Z 2) telefonischen Kontakt oder
- (Z 3) Vertragsbestimmungen oder
- (Z 4) Abfrage elektronischer Verzeichnisse der ÖÄK, ÖÄZK, des Österreichischen Hebammengremiums, der Österreichischen Apothekerkammer, des Hauptverbands oder des BMASGK

bestätigt sind.[64)] Im Fall der Bestätigung über persönlichen oder telefonischen Kontakt sind vor der erstmaligen Übermittlung der Gesundheitsdaten und genetischen Daten zwischen den beteiligten GDA nach § 27 Abs 11 GTelG 2012 weitere Angaben zu dokumentieren und laufend zu aktualisieren. →

58) Vgl *Gabauer,* mHealth 199; nach *Burgstaller,* Gesundheitsdaten in der Cloud! ecolex 2016, 635 (637), liegt im Fall einer dedizierten Zurverfügungstellung von Datenkapazitäten an einen GDA keine rein dynamische Bedarfsorientierung vor, sodass keine Verpflichtung zur Verschlüsselung gegeben sei, sondern auch die Maßnahmen gem § 6 Abs 1 Z 1 GTelG 2012 ausreichend seien.
59) Vgl ErläutRV 1936 BlgNR 24. GP 24.
60) VO (EU) 910/2014 des Europäischen Parlaments und des Rates v 23. 7. 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der RL 1999/93/EG, ABl L 2014/257, 73 idF ABl L 2016/155, 44.
61) Vgl ErläutRV 1936 BlgNR 24. GP 21.
62) Vgl § 27 Abs 13 GTelG 2012.
63) Vgl § 27 Abs 14 GTelG 2012.
64) Vgl § 27 Abs 10 GTelG 2012.

### b) Übermittlung per Fax

Die Übermittlung von Gesundheitsdaten und genetischen Daten darf gem § 27 Abs 12 GTelG 2012 unter den Voraussetzungen des § 27 Abs 10 Z 1 bis 3 leg cit auch per Fax erfolgen, wenn kumulativ

- (Z 1) die Faxanschlüsse (einschließlich Ausdruckmöglichkeit zu Faxanschlüssen, die in EDV-Anlagen installiert sind) vor unbefugtem Zugang und Gebrauch geschützt sind,
- (Z 2) die Rufnummern, insb die verspeicherten Rufnummern, regelmäßig, insb nach Veränderungen der technischen Einrichtung sowie nach der Neuinstallation von Faxgeräten, nachweislich auf ihre Aktualität geprüft werden,
- (Z 3) automatische Weiterleitungen, außer an die jeweiligen GDA selbst, deaktiviert sind,
- (Z 4) die vom Gerät unterstützten Sicherheitsmaßnahmen genützt werden und
- (Z 5) allenfalls verfügbare Fernwartungsfunktionen nur für die vereinbarte Dauer der Fernwartung aktiviert sind.

## 6. IT-Sicherheitskonzept

Nach § 8 Abs 1 GTelG 2012 sind GDA verpflichtet, auf Basis eines IT-Sicherheitskonzepts alle gem Art 32 DSGVO und den Bestimmungen des GTelG 2012 getroffenen Datensicherheitsmaßnahmen 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.[65] Diese Bestimmung konkretisiert die bereits aus der Rechenschaftspflicht nach Art 5 Abs 2 DSGVO resultierende Dokumentationsverpflichtung des Verantwortlichen.[66] Insb die Inanspruchnahme sowie das Vorliegen der Voraussetzungen des Inhouse-Privilegs gem § 3 Abs 2 GTelG 2012 oder der in § 27 Abs 10 bis 12 GTelG 2012 normierten erleichterten Bedingungen müssen dokumentiert werden.[67]

Gem § 8 Abs 2 GTelG 2012 können bestimmte Einrichtungen standardisierte Formulare und Ausfüllhilfen für die Dokumentation zur Unterstützung jener GDA zur Verfügung stellen, für die sie als Registrierungsstelle gem § 2 Z 4 GTelG 2012 fungieren. Dem für das Gesundheitswesen zuständigen Bundesminister wird durch § 8 Abs 3 GTelG 2012 ein jederzeitiges Einsichtsrecht in die Dokumentation des IT-Sicherheitskonzepts eingeräumt.[68]

## C. Conclusio

Der Anwendungsbereich des GTelG 2012 beschränkt sich nicht nur auf ELGA (vgl 4. Abschnitt des GTelG 2012), sondern umfasst die Verarbeitung personenbezogener elektronischer Gesundheitsdaten und genetischer Daten durch GDA. Hinsichtlich der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten durch GDA normiert der 2. Abschnitt des GTelG 2012 spezifische Datensicherheitsbestimmungen, die den allgemeinen Datensicherheitsmaßnahmen gem Art 32 DSGVO als leges speciales vorgehen und weder durch die GDA noch durch die betroffenen Personen abbedungen werden können. Die Qualifikation als GDA iSd § 2 Z 2 GTelG 2012 setzt zum einen die regelmäßige Verarbeitung von Gesundheitsdaten oder genetischen Daten in elektronischer Form zu bestimmten festgelegten Zwecken voraus, weshalb die bloße gelegentliche elektronische Übermittlung per se noch nicht den Anwendungsbereich des GTelG 2012 eröffnet. Zum anderen dürfen GDA Gesundheitsdaten und genetische Daten nur in einer Rolle iSd Anlage 1 der GTelV 2013 verarbeiten. Kann ein Gesundheitsdienstleister keiner vordefinierten Rolle zugeordnet werden, muss dieser beim BMASGK die Eintragung einer neuen Rolle in die GTelV 2013 beantragen. Ein Verstoß gegen den 2. Abschnitt des GTelG 2012 ist nach Ansicht des Gesetzgebers unter die Strafdrohung des Art 83 DSGVO zu subsumieren, weshalb GDA eine rechtskonforme elektronische Übermittlung von Gesundheitsdaten und genetischen Daten anzuraten ist.

65) Vgl § 8 Abs 1 GTelG 2012.
66) Die Zulässigkeit einer nationalen – von den Vorgaben der DSGVO abweichenden – Bestimmung kann auf die Öffnungsklausel des Art 9 Abs 4 DSGVO gestützt werden.
67) Vgl ErläutRV 1936 BlgNR 24. GP 24.
68) Vgl ErläutRV 1936 BlgNR 24. GP 24.

### ➜ In Kürze

**Die elektronische Übermittlung von Gesundheitsdaten und genetischen Daten durch GDA unterliegt den Datensicherheitsbestimmungen des 2. Abschnitts des GTelG 2012, die den allgemeinen Datensicherheitsmaßnahmen gem Art 32 DSGVO als leges speciales vorgehen. Ein Verstoß gegen den 2. Abschnitt des GTelG 2012 ist nach Ansicht des Gesetzgebers unter die Strafdrohung des Art 83 DSGVO zu subsumieren.**

### ➜ Zum Thema

**Über die AutorInnen:**
Mag. Eva-Maria Pfandlsteiner, LL.M., ist Referentin in der Stabstelle Koordinierung ELGA-Ombudsstelle und Gesundheit Österreich GmbH und in der Abteilung VIII/A/4 Gesundheitstelematik im Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz.

Dr. Claudia Gabauer, LL.M., ist Rechtsanwaltsanwärterin bei Knyrim Trieb Rechtsanwälte OG. Kontaktadresse: Knyrim Trieb Rechtsanwälte OG, Mariahilfer Straße 89a, 1060 Wien. Tel: +43 (0) 1 909 30 70, E-Mail: cg@kt.at, Internet: www.kt.at

Dr. Gerald Trieb, LL.M., ist Partner und Rechtsanwalt bei Knyrim Trieb Rechtsanwälte OG. Kontaktadresse: Knyrim Trieb Rechtsanwälte OG, Mariahilfer Straße 89a, 1060 Wien. Tel: +43 (0) 1 909 30 70, E-Mail: gt@kt.at, Internet: www.kt.at