

27. März 2018

Bundesministerium für Arbeit, Soziales,

Gesundheit und Konsumentenschutz

per E-Mail an:

vera.pribitzer@bmg.gv.at

sowie

Präsidium des Nationalrats

per E-Mail an:

begutachtung@parlament.gv.at

Stellungnahme zum Entwurf

Datenschutz-Anpassungsgesetz 2018 – Gesundheit

Sehr geehrte Damen und Herren!

Zum Ministerialentwurf „Datenschutz-Anpassungsgesetz 2018 – Gesundheit“ nehmen wir wie folgt Stellung:

1. Zu Artikel 22 (Änderung des Bundesgesetzes über Krankenanstalten und Kuranstalten)

1.1 § 9a Abs 2 Satz 2 KAKuG

Die vorgeschlagene Fassung (§ 9a KAKuG) lautet wie folgt:

§ 9a. (1) Rechtsträger von Krankenanstalten sind ermächtigt, die im Rahmen des Betriebes einer Krankenanstalt nach den Bestimmungen dieses Bundesgesetzes erforderlichen personenbezogenen Daten zum Zwecke der

- 1. Dokumentation und Auskunftserteilung (§ 10), und*
- 2. Abrechnung (§§ 27 bis, 30 und 40 Abs. 3)*

unter Einhaltung der Datenschutz-Grundverordnung zu verarbeiten.

(2) Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 sind die Pflichten und Rechte gemäß Art. 13, 14, 18 und 21 Datenschutz-Grundverordnung ausgeschlossen. Personenbezogene Daten gemäß Abs. 1 Z 2, die der Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen dienen, dürfen jedenfalls bis zu 30 Jahre gespeichert und gegebenenfalls verarbeitet werden.

Durch den Verweis in § 9a Abs 2 Satz 2 KAKuG lediglich auf Abs 1 Z 2 sind von der vorgeschlagenen Fassung „Dokumentation und Auskunftserteilung (§ 10)“ nicht umfasst. Gerade auch die Dokumentation und die Auskunftserteilung können aber Gegenstand von Rechtsstreitigkeiten sein und auch diese Daten der „Verteidigung von Rechtsansprüchen“ dienen (etwa der Abwehr von Schadenersatzansprüchen, welche grundsätzlich bis zum Ablauf von 30 Jahren nach der Behandlung möglich sind).

§ 9a KAKuG sollte daher wie folgt lauten¹:

§ 9a. (1) Rechtsträger von Krankenanstalten sind ermächtigt, die im Rahmen des Betriebes einer Krankenanstalt nach den Bestimmungen dieses Bundesgesetzes oder der gemäß diesem Bundesgesetz erlassenen Verordnungen erforderlichen personenbezogenen Daten insbesondere zum Zwecke der

1. Dokumentation und Auskunftserteilung (§ 10), und
2. Abrechnung (§§ 27 bis, 30 und 40 Abs. 3)

unter Einhaltung der Datenschutz-Grundverordnung zu verarbeiten.

(2) Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 sind die Pflichten und Rechte gemäß Art. 13, 14, 17, 18 und 21 Datenschutz-Grundverordnung ausgeschlossen. Personenbezogene Daten gemäß Abs. 1, die der Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen dienen, dürfen jedenfalls bis zu 30 Jahre gespeichert und gegebenenfalls verarbeitet werden.

1.2 § 10 Abs 1 Z 4a KAKuG

Die bestehende Bestimmung in § 10 Abs 1 Z 4a KAKuG lautet wie folgt:

§ 10. (1) Durch die Landesgesetzgebung sind die Krankenanstalten zu verpflichten:

- 4a. Pfleglingen Einsicht in ihre Krankengeschichte zu gewähren und gegen Kostenersatz die Herstellung von Kopien zu ermöglichen;

Diese Bestimmung erlaubt es, für die Herstellung von Kopien von Krankengeschichten Kostenersatz zu verlangen. Diese Möglichkeit sollte gesichert bleiben.

Der Gesetzestext sollte daher in § 10 Abs 1 Z 4a KAKuG um einen Halbsatz ergänzt werden und wie folgt lauten:

§ 10. (1) Durch die Landesgesetzgebung sind die Krankenanstalten zu verpflichten:

- 4a. Pfleglingen Einsicht in ihre Krankengeschichte zu gewähren und gegen Kostenersatz die Herstellung von Kopien zu ermöglichen; *im Hinblick auf die im Rahmen des Betriebes einer Krankenanstalt nach den Bestimmungen dieses Bundesgesetzes oder der gemäß diesem Bundesgesetz erlassenen Verordnungen erforderlichen personenbezogenen Daten ist Art. 15 Abs 3 Datenschutz-Grundverordnung ausgeschlossen;*

¹ Zur Ergänzung der Wortfolge „oder der gemäß diesem Bundesgesetz erlassenen Verordnungen“ und des Wortes „insbesondere“ in Abs 1 siehe unten Punkt 3.1; zur Ergänzung des Artikels „17“ in Abs 2 Satz 1 siehe unten Punkt 3.2.

2. Zu Artikel 45 (Änderung des Gesundheitstelematikgesetzes 2012)

2.1 § 3 Abs 2 GTelG 2012

Die vorgeschlagene Fassung (§ 3 Abs 2 GTelG 2012) lautet wie folgt:

(2) Abs. 4 Z 3 bis 6 sowie die §§ 5 bis 7 sind auf die elektronische *Übermittlung* von Gesundheitsdaten *und genetischen Daten* innerhalb eines Gesundheitsdiensteanbieters nicht anzuwenden, 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.

Aufgrund der bisherigen wie auch der vorgeschlagenen neuen Bestimmung in § 3 Abs 2 GTelG 2012 gelten die Regelungen zur Datensicherheit bei der elektronischen Weitergabe von Gesundheitsdaten innerhalb eines Gesundheitsdiensteanbieters (GDA), also etwa innerhalb eines Trägers von Krankenanstalten als Verantwortlicher, nur beschränkt (GDA-Privileg). Diese Privilegierung sollte auf alle Gesundheitsdiensteanbieter ausgeweitet werden, die nach den unternehmensrechtlichen Bestimmungen verbundene Unternehmen darstellen, und zwar dahingehend, dass die Privilegierung im gesamten Unternehmensverbund gilt. Dies würde die nach § 10 Abs 5 KAKuG² vorgesehene Möglichkeit, die Speicherung, Verarbeitung und Aufbewahrung von Krankengeschichten anderen Rechtsträgern zu übertragen, im Konzern wesentlich erleichtern bzw. überhaupt erst eröffnen.

Darüber hinaus sei angemerkt, dass der vorgeschlagene § 6 Abs 3 GTelG 2012 (siehe unten Punkt 2.2.), auf welchen § 3 Abs 2 GTelG 2012 Bezug nimmt, nicht die Übermittlung von Gesundheitsdaten und genetischen Daten zum Inhalt hat, sondern deren Speicherung. Das GDA-Privileg sollte also auch diese Verarbeitungskategorie (Speicherung) umfassen.

Die Bestimmung in § 3 Abs 2 GTelG 2012 sollte daher wie folgt lauten:

(2) Abs. 4 Z 3 bis 6 sowie die §§ 5 bis 7 sind auf die elektronische *Übermittlung und Speicherung* von Gesundheitsdaten *und genetischen Daten* innerhalb eines Gesundheitsdiensteanbieters nicht anzuwenden, 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. *Dasselbe gilt für einen unternehmensrechtlichen Unternehmensverbund von Gesundheitsdiensteanbietern bzw. zwischen Gesundheitsdiensteanbietern, die nach den unternehmensrechtlichen Bestimmungen verbundene Unternehmen darstellen.*

² § 10 Abs 5 KAKuG lautet wie folgt: „Die Landesgesetzgebung kann die Rechtsträger von Krankenanstalten ermächtigen, die Speicherung, Verarbeitung und Aufbewahrung von Krankengeschichten anderen Rechtsträgern zu übertragen, wenn für diese Rechtsträger und die in ihnen beschäftigten Personen eine gesetzliche Verschwiegenheitspflicht besteht oder durch die Landesgesetzgebung auferlegt wird. Die Ermächtigung kann auch die Speicherung, Verarbeitung und Aufbewahrung mittels automationsunterstützter Datenverarbeitung beinhalten. Weitergaben von personenbezogenen Daten durch Rechtsträger, denen die Speicherung, Verarbeitung und Aufbewahrung übertragen wurde, sind nur an Ärzte oder Zahnärzte oder Krankenanstalten zulässig, in deren Behandlung der Betroffene steht.“

2.2 § 6 Abs 3 GTelG 2012

Die vorgeschlagene Fassung in § 6 Abs 3 GTelG 2012 lautet wie folgt:

(3) Es ist sicherzustellen, dass die Speicherung von Gesundheitsdaten *und genetischen Daten* in Datenspeichern, die einem *Verantwortlichen* (Art. 4 Z 7 DSGVO) bedarfsoorientiert von einem *Auftragsverarbeiter* (Art. 4 Z 8 DSGVO) bereitgestellt werden („Cloud Computing“), nur dann erfolgt, wenn die Gesundheitsdaten *und genetischen Daten* mit einem dem aktuellen Stand der Technik entsprechenden Verfahren (Abs. 1 Z 2) verschlüsselt worden sind.

Die Bestimmung war bereits bisher unklar und ist es weiterhin. Eine Klarstellung – zumindest in den Erläuterungen – wäre hilfreich, etwa ob unter dem Begriff „Cloud Computing“ im Sinne dieser Bestimmung nur die bloße Bereitstellung von „Cloud-Speicher“ gemeint ist.³

Es sollte jedenfalls (auch) klargestellt werden, dass durch diese Bestimmung die Möglichkeiten eines Gesundheitsdiensteanbieters (§ 2 Z 2 GTelG 2012), Gesundheitsdaten und genetischen Daten zu speichern, nicht beschränkt werden, 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 (vgl. die Erweiterung des GDA-Privilegs gemäß § 3 Abs 2 GTelG 2012, wie oben im Punkt 2.1. angeregt).

3. Weitere Anregungen

3.1 Gesetzliche Ermächtigung zum Verarbeiten von personenbezogenen Daten

Die vorgeschlagene Fassung in § 3b Abs 1 ÄrzteG lautet wie folgt:

§ 3b. (1) Personenbezogene Daten dürfen nur zu Zwecken, die in diesem Bundesgesetz oder in gemäß diesem Bundesgesetz erlassenen Verordnungen festgelegt sind, unter Einhaltung der 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 4.5.2016 S. 1, und des Datenschutzgesetzes (DSG), BGBL. I Nr. 165/1999, verarbeitet werden.

Im Hinblick auf die zulässigen Verarbeitungszwecke beinhaltet die im ÄrzteG vorgesehene Bestimmung demnach eine Generalklausel. Davon abweichend findet sich in den neuen Regelungen zu den Berufsgesetzen (siehe z.B. die vorgeschlagenen Fassungen in § 2b Abs 1 GuKG, § 61d Abs 1 HebG, § 1c Abs 1 MTD-G, § 3a Abs 1 MABG) oder zum Kranken- und Kuranstaltengesetz (siehe die vorgeschlagene Fassung in § 9a Abs 1 KAKuG) keine solche Generalklausel, sondern jeweils eine taxative Aufzählung.

³ Dabei wäre wohl auch zu hinterfragen, welche sinnvollen Verarbeitungen verschlüsselt verspeicherter Daten überhaupt möglich wären.

Beispiel aus GuKG:

§ 2b. (1) *Angehörige der Gesundheits- und Krankenpflegeberufe sind ermächtigt, die im Rahmen der Berufsausübung nach den Bestimmungen dieses Bundesgesetzes erforderlichen personenbezogenen Daten zum Zweck*

1. *der Dokumentation (§ 5),*
2. *der Honorarabrechnung (§ 6 Abs. 2 Z 3),*
3. *der Anzeige oder Meldung (§§ 7 und 8),*
4. *der Auskunftserteilung (§ 9)*

unter Einhaltung der 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 4.5.2016 S. 1, und des Datenschutzgesetzes (DSG), BGBL. I Nr. 165/1999, zu verarbeiten.

Beispiel aus KAKuG:

§ 9a. (1) *Rechtsträger von Krankenanstalten sind ermächtigt, die im Rahmen des Betriebes einer Krankenanstalt nach den Bestimmungen dieses Bundesgesetzes erforderlichen personenbezogenen Daten zum Zwecke der*

1. *Dokumentation und Auskunftserteilung (§ 10), und*
2. *Abrechnung (§§ 27 bis, 30 und 40 Abs. 3)*

unter Einhaltung der Datenschutz-Grundverordnung zu verarbeiten.

Die restriktive, weil taxative, Regelung in § 2b Abs 1 GuKG würde dazu führen, dass etwa die Verarbeitung personenbezogener Daten zum Zweck einer notwendigen Offenbarung von Geheimnissen gemäß § 6 Abs 2 Z 2 GuKG nicht (mehr) zulässig wäre. Anders als die ebenfalls als Durchbrechung der Verschwiegenheitspflicht in § 6 Abs 2 Z 3 GuKG normierten Mitteilungen des Angehörigen eines Gesundheits- und Krankenpflegeberufes zum Zweck der Honorarabrechnung (vgl § 2b Abs 1 Z 2 GuKG) wurde die Verarbeitung zum Zweck einer für die nationale Sicherheit etc notwendigen Offenbarung (vgl § 6 Abs 2 Z 2 GuKG) – möglicherweise aus Versehen – nicht in den Katalog in § 2b Abs 1 GuKG aufgenommen. Ähnliches gilt für die anderen Berufsgesetze und für das KAKuG.

Es können sich aus diesen Gesetzen auch noch andere mögliche oder erforderliche Verarbeitungen ergeben. Um zu vermeiden, dass solche erforderlichen Verarbeitungszwecke, die sich aus den Bestimmungen der vom Gesetzesentwurf umfassten Gesetze und den darauf basierenden Verordnungen ergeben, nicht von der gesetzlichen Erlaubnis zur Verarbeitung umfasst sind (und über einen Gegen schluss zu den taxativen Aufzählungen möglicherweise auch rechtswidrig würden), sollte auch in diesen Gesetzen eine Generalklausel, wie in § 3b Abs 1 ÄrzteG vorgesehen, normiert werden. Nur so wäre sichergestellt, dass alle – insbesondere für Zwecke der Gesundheitsvorsorge, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheitsbereich und für die Verwaltung von Systemen und Diensten im Gesundheitsbereich (vgl. Art 9 Abs 2 lit h DSGVO) – erforderlichen Verarbeitungen umfasst sind. Dies könnte alternativ auch durch eine Ergänzung des Wortes „*insbesondere*“ be werkstelligt werden, womit eine (bloß) beispielhafte Aufzählung zum Ausdruck gebracht wird.

§ 2b Abs 1 GuKG könnte demnach etwa wie folgt lauten:

§ 2b. (1) *Angehörige der Gesundheits- und Krankenpflegeberufe sind ermächtigt, die im Rahmen der Berufsausübung nach den Bestimmungen dieses Bundesgesetzes oder der gemäß diesem Bundesgesetz erlassenen Verordnungen erforderlichen personenbezogenen Daten insbesondere zum Zweck*

1. der Dokumentation (§ 5),
2. der Honorarabrechnung (§ 6 Abs. 2 Z 3),
3. der Anzeige oder Meldung (§§ 7 und 8),
4. der Auskunftserteilung (§ 9)

unter Einhaltung der 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 4.5.2016 S. 1, und des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, zu verarbeiten.

§ 9a Abs 1 KAKuG könnte etwa wie folgt lauten:

§ 9a. (1) *Rechtsträger von Krankenanstalten sind ermächtigt, die im Rahmen des Betriebes einer Krankenanstalt nach den Bestimmungen dieses Bundesgesetzes oder der gemäß diesem Bundesgesetz erlassenen Verordnungen erforderlichen personenbezogenen Daten insbesondere zum Zwecke der*

1. Dokumentation und Auskunftserteilung (§ 10), und
2. Abrechnung (§§ 27 bis, 30 und 40 Abs. 3)

unter Einhaltung der Datenschutz-Grundverordnung zu verarbeiten.

3.2 Ausschluss des Rechts auf Löschung

Die vom Gesetzesentwurf umfassten Berufsgesetze schließen die Anwendbarkeit von Art 13 und 14 DSGVO (Informationspflichten des/der Verantwortlichen bei der Erhebung von personenbezogenen Daten) sowie Art 18 DSGVO (Recht des/der Betroffenen auf Einschränkung der Verarbeitung) und 21 DSGVO (Widerspruchsrecht des/der Betroffenen) ausdrücklich aus (siehe zB die vorgeschlagenen Fassungen in § 2b Abs 3 GuKG, § 3b Abs 2 Ärztegesetz). Dasselbe gilt für das KAKuG (siehe die vorgeschlagene Fassung in § 9a Abs 2 erster Satz KAKuG).

Beispiel § 2b Abs 3 GuKG:

(3) Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 und 2 sind die Rechte und Pflichten gemäß Artikel 13, 14, 18 und 21 DSGVO ausgeschlossen.

Beispiel § 9a Abs 2 erster Satz KAKuG:

(2) Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 sind die Pflichten und Rechte gemäß Art. 13, 14, 18 und 21 Datenschutz-Grundverordnung ausgeschlossen.

Im Hinblick auf Art 17 DSGVO (Recht auf Löschung) beinhalten zwar die Erläuterungen zu den betreffenden Gesetzen jeweils den (zu befürwortenden) Hinweis, dass dieses Recht auf Löschung bereits durch Artikel 17 Abs 3 lit b DSGVO ausgeschlossen sei, „da die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung nach dem nationalen Recht erfolgt“. Diese in den Gesetzen enthaltenen „rechtlichen Verpflichtungen“ sehen aber nur Mindestfristen vor (vgl. § 5 Abs 4 GuKG „mindestens zehn

Jahre“; § 51 Abs 3 ÄrzteG „*mindestens zehn Jahre*“; § 10 Abs 1 Z 3 erster Halbsatz KAKuG „*mindestens 30 Jahre*“; § 10 Abs 1 Z 3 zweiter Halbsatz KAKuG „*mindestens jedoch zehn Jahre*“).

Wie in den Erläuterungen zu einigen Berufsgesetzen zutreffend dargelegt (siehe etwa auf Seite 2 der Erläuterungen die Ausführungen zum GuKG), besteht gemäß Art 17 Abs 3 lit e DSGVO auch nach den in den Berufsgesetzen festgelegten Fristen „*insbesondere im Hinblick auf die zivilrechtliche Verjährungsfrist, die Möglichkeit, von der Löschung zum Zweck der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen abzusehen*“.

Da die „Erfüllung einer rechtlichen Verpflichtung“ im Sinne von Art 17 Abs 3 lit b DSGVO streng genommen nur die Einhaltung der Mindestfrist bedeutet, würde der Ausschluss des Rechts auf Löschung möglicherweise nur für diese Mindestfristen gelten und das Recht auf Löschung nach Ablauf der Mindestfristen wieder auflieben. Angesichts solcher Unsicherheiten, sollte der Ausschluss des Rechts auf Löschung (auch) in den Gesetzestext Eingang finden.

§ 2b Abs 3 GuKG sollte daher wie folgt lauten (für die anderen Berufsgesetze gilt das analog):

(3) *Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 und 2 sind die Rechte und Pflichten gemäß Artikel 13, 14, 17, 18 und 21 DSGVO ausgeschlossen.*

§ 9a Abs 2 erster Satz KAKuG sollte wie folgt lauten:

(2) *Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 sind die Pflichten und Rechte gemäß Art. 13, 14, 17, 18 und 21 Datenschutz-Grundverordnung ausgeschlossen.*

3.3 Ergänzung der Erläuterungen betreffend das ÄrzteG und das KAKuG

In den Erläuterungen zu den Änderungen im GuKG (siehe Seite 2 der Erläuterungen) steht unter Bezugnahme auf die Verpflichtung, die Pflegedokumentation mindestens zehn Jahre nach Beendigung des Behandlungs-/Betreuungsverhältnisses aufzubewahren, folgende (zu befürwortende) Klausel: „Gemäß Artikel 17 Abs. 3 lit e DSGVO besteht auch nach dieser Frist, insbesondere im Hinblick auf die zivilrechtliche Verjährungsfrist, die Möglichkeit, von der Löschung zum Zweck der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen abzusehen.“ Auch in den Erläuterungen zu anderen Berufsgesetzen (zB HebG: Seite 4 der Erläuterungen; MTD-Gesetz: Seite 8 der Erläuterungen; MMHmG: Seite 11 der Erläuterungen) findet sich diese Klausel. Da der Gesetzgeber angehalten ist, sachlich vergleichbare Problemlagen auch rechtlich (sowohl im Gesetz als auch in den Erläuterungen) gleich zu behandeln, sollte diese Klausel auch in den das ÄrzteG und das KAKuG betreffenden Erläuterungen aufgenommen werden. Dort fehlen nämlich derartige Klarstellungen.

Mit freundlichen Grüßen

Oö. Gesundheits- und Spitals-AG (gespag)

i.A. Dr. Kurt Reindl
Referent Rechtsabteilung