

An das
Bundesministerium für
Gesundheit

Per Mail:
clemens.auer@bmg.gv.at
*Begutachtung.SLI@bmg.gv.at

Betrifft: Entwurf einer Verordnung des Bundesministers für Gesundheit, mit der nähere Regelungen für die Gesundheitstelematik getroffen werden – Gesundheitstelematikverordnung 2013 (GTelV 2013)

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **218. Sitzung am 25. November 2013 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines:

Mit dem **Entwurf einer Gesundheitstelematikverordnung 2013 (GTelV 2013)** sollen Bestimmungen des zweiten und dritten Abschnittes des Gesundheitstelematikgesetzes 2012 (GTelG 2012), BGBl. I Nr. 111/2012, konkretisiert bzw. operationalisiert werden. Dies ist insbesondere deshalb notwendig, weil einige Bestimmungen im GTelG 2012 gegenüber früheren Bestimmungen geändert wurden. Sie ersetzt die Gesundheitstelematikverordnung 2012 (GTelV 2012), BGBl. II Nr. 483/2012, zur Gänze, da die Novellierung mit einem ähnlichen Aufwand verbunden, jedoch der Lesbarkeit nicht förderlich gewesen wäre.

Das Begleitschreiben zum Begutachtungsentwurf nimmt auf die Anhörung des Datenschutzrates nach § 31a Abs. 4 ASVG Bezug. Nach dieser Bestimmung ist der Datenschutzrat im Zusammenhang mit dem Elektronischen Verwaltungssystem und der Elektronischen Gesundheitsakte sowie den

Grundlagen des Elektronischen Verwaltungssystems (ELSY) zu Fragen der Unvereinbarkeit neuer Verwendungszwecke sowie zu Fragen der Speicherung von Daten auf den innerhalb des ELSY zu verwendenden Chipkarten unter Setzung einer angemessenen Frist anzuhören.

2) Datenschutzrechtlich relevante Bestimmungen:

Zu den §§ 2 und 3 sowie der Anlage 1:

a.) Nach § 2 Abs. 1 haben **Gesundheitsdiensteanbieter** bei der elektronischen Verwendung von **Gesundheitsdaten** ausschließlich die in der Anlage 1 definierten Rollen zu verwenden. Gesundheitsdiensteanbieter, die **in mehreren Rollen tätig** werden, haben jeweils die auf den konkreten Verwendungsvorgang zutreffende Rolle zu verwenden. Der Bundesminister für Gesundheit kann nach Abs. 2 im **Internet** sowie im **Amtsblatt der Wiener Zeitung** eine nähere Beschreibung der in der Anlage 1 genannten Rollen veröffentlichen, in der insbesondere einzelne Rollen erläutert oder Abgrenzungen der Rollen vorgenommen werden. § 3 sieht Möglichkeiten zur **Aktualisierung des Rollenkataloges** vor. Insbesondere kann ein **Antrag auf Eintragung einer neuen Rolle** gestellt werden.

Vorweg ist anzumerken, dass die Festlegung von „**Rollen**“, in welchen Auftraggeber und Dienstleister tätig werden, bei der Verwendung von Gesundheitsdaten schon aus **Datensicherheitsgründen** (§ 14 DSGVO 2016) unbedingt erforderlich ist. In einem komplexen System für die Übermittlung von Gesundheitsdaten müssen Rollen und Berechtigungen daher vorweg derart präzise festgelegt werden, dass nur solche Auftraggeber und Dienstleister Gesundheitsdaten verwenden können, die diese auch tatsächlich benötigen. Dazu ist insbesondere eine ausreichende Anzahl an **Unterteilungen im Rollensystem** sowie eine klare **Abgrenzung der Rollen** erforderlich.

Im Lichte dieser Vorgaben erscheint es nicht ausreichend, in einer Verordnung bloß grundsätzlich die Rollen festzulegen und erst zu einem späteren Zeitpunkt im Internet sowie im Amtsblatt der Wiener Zeitung einzelne Rollen zu erläutern oder notwendige Abgrenzung der Rollen vorzunehmen. Es sollten daher erforderliche Präzisierungen bereits in der vorgeschlagenen Verordnung sowie allfällig notwendige spätere Anpassungen in Form einer Novelle zur Verordnung vorgenommen werden.

Insbesondere sollte in der Verordnung bzw. der Anlage 1 klargestellt werden, **welche Funktion die Beifügung der Fächer in den Rollen** der Anlage 1 Teil 1 Z 1 („Ärztin/Arzt der Allgemeinmedizin“) und Z 4 („Fachärztin/Facharzt“) hat bzw. ob damit eine Untergliederung dieser Rollen geschaffen werden soll und was unter der Rolle „**Gesundheitsversicherung**“ gemäß Anlage 1 Teil 2 Z 27 zu verstehen ist. Unklar ist schließlich auch die terminologische Abgrenzung der Rolle der „**Rettung**“ in der Anlage 1 Teil 2 Z 15, insbesondere ob davon auch etwa die Flug- oder Bergrettung umfasst sein soll.

b.) Hinsichtlich der Prüfung von Anträgen auf Eintragung einer neuen Rolle sollte in § 3 Abs. 4 **nicht auf die Zweckmäßigkeit**, sondern darauf abgestellt werden, ob neue Rollen – vor allem im Hinblick auf notwendige Datensicherheitsmaßnahmen – tatsächlich **erforderlich** sind. Auch in § 3 Abs. 6 sollte für die Aufnahme neuer Rollen auf die Erforderlichkeit aus Gründen der Datensicherheit abgestellt werden.

Zu § 4 und der Anlage 2:

§ 4 legt fest, dass die in der **Anlage 2** angeführten **Algorithmen jedenfalls** die Voraussetzungen des § 6 GTelG 2012 erfüllen. Die Anlage 2 sieht als zulässige Algorithmen unter anderem **AES (Advanced Encryption Standard)** mit einer **Schlüssellänge von 128, 192 oder 256 Bit** [FIPS 197] sowie **TDEA (Triple Data Encryption Algorithm)** mit einer **effektiven Schlüssellänge von mindestens 112 Bit** [NIST 800-67] jeweils in CBC oder CTR Modus [NIST 800-38A] vor.

Nach § 14 Abs. 1 DSG 2000 müssen **alle Organisationseinheiten** eines Auftraggebers oder Dienstleisters, die Daten verwenden, **Maßnahmen zur Gewährleistung der Datensicherheit** zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

Nachdem **Gesundheitsdaten** zu den besonders schützenswerten, sensiblen Daten zählen, muss die Verschlüsselung dieser Daten dem derzeitigen Stand der technischen Möglichkeiten entsprechen. Diesbezüglich erscheint es fraglich, ob die Festlegung eines **breiten Spektrums an zulässigen Schlüssellängen** tatsächlich noch dem derzeitigen Stand der Technik entspricht, zumal auch die Erläuterungen

„zur Erhöhung der kryptografischen Sicherheit“ **die Verwendung der höchstmöglichen Schlüssellänge empfehlen.**

Aufgrund der Sensibilität der Verwendung von Gesundheitsdaten sollte zum Schutz vor Missbrauch dieser Daten daher nochmals geprüft werden, welche Algorithmen tatsächlich dem derzeitigen Stand der Technik für die Verwendung von Gesundheitsdaten entsprechen, und nur die Verwendung ausreichend sicherer Schlüssel erlaubt sein.

Nach Ansicht des Datenschutzrates sollte geprüft werden, ob der Algorithmus AES (Advanced Encryption Standard) als bevorzugter Algorithmus festgelegt werden sollte.

Zu den §§ 5 bis 9:

a.) Die §§ 5 bis 9 legen die Grundlagen für die Eintragungen in den **eHealth-Verzeichnisdienst (eHVD)** sowie Übermittlungen an diesen und die Verwendung der Daten fest.

Hinsichtlich der Übermittlung von Daten nach den §§ 6 bis 9 lässt die Verordnung – mit Ausnahme des in § 8 Abs. 2 vorgesehenen Falls der Übermittlung im Wege des Unternehmensserviceportals – offen, **in welcher Form** (zB per verschlüsseltem E-Mail oder im Wege einer elektronischen Schnittstelle) diese Übermittlung jeweils vorgenommen werden soll bzw. welche **Datensicherheitsmaßnahmen** im Falle einer elektronischen Übermittlung getroffen werden müssen. Die bloße Veröffentlichung von Spezifikationen, welche nach § 5 Abs. 3 ua. auch **Art und Umfang der zu meldenden Daten** umfassen, im Internet sowie im Amtsblatt der Wiener Zeitung erscheint dahingehend nicht ausreichend. **Stattdessen sollten die technischen Möglichkeiten für die Meldung sowie die Datenarten bereits in der Verordnung festgelegt werden.** Siehe diesbezüglich die Anmerkungen zu den §§ 2 und 3 sowie der Anlage 1.

b.) Die Erläuterungen zu § 6 nehmen Bezug darauf, dass mit dem derzeit in parlamentarischer Behandlung befindlichen **Gesundheitsberuferegister-Gesetz (GBRegG)** im Falle der Beschlussfassung ein **weiteres Berufsregister vergleichbar mit dem eHVD** entsteht. **Es ist fraglich, wozu zwei vergleichbare Berufsregister überhaupt benötigt werden.**

c.) Nachdem § 9 Abs. 2 Z 1 bis 3 für die Übermittlung der Daten aus dem eHVD auf den Umfang der Daten, den Zweck der Verwendung und die Art der technischen Inanspruchnahme der Daten abstellt, ist nicht nachvollziehbar, weshalb sodann nach § 9 Abs. 3 die Daten des eHVD **ausschließlich in Form eines Gesamtdatenbestandes** übermittelt werden dürfen. **Stattdessen sollten iSd in § 1 Abs. 2 DSG 2000 verankerten Verhältnismäßigkeitsgrundsatzes nur jene Daten übermittelt werden, die der Interessent für den angegebenen Zweck tatsächlich benötigt.**

26. November 2013
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt