ARGE DATEN
Österreichische Gesellschaft für Datenschutz
DB RECHT / STELL / Unser Zeichen: GES-STEL.DOC

[ADA] [BMSG] [3578] / [70.101/22-VII/B/10/02]

Herrn Bundesminister
Mag. Herbert HAUPT
BM FÜR SOZIALE SICHERHEIT UND GENERATIONEN (BMAS/BMSG)

Stubenring 1
1011 WIEN

Wien, 14. August 2002

Betreff: Ihr Zeichen: 70.101/22-VII/B/10/02
Stellungnahme der ARGE DATEN zu
Bundesgesetz betreffend Übertragungssicherheit beim elektronischen Austausch von Gesundheitsdaten und Einrichtung eines Informationsmanagement (Gesundheitstelematikgesetz) [BEGUTACHTUNG GESETZESENTWURF]

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

_____ _____
Dr. Hans G. Zeger (Obmann) Charlotte Schönherr (Schriftführerin)

Anlage:
Stellungnahme

Ergeht in Kopie an:
Parlamentsdirektion (☑ *begutachtungsverfahren@parlinkom.gv.at,* ☐ Druckversion)

Eine Kopie der Stellungnahme wird weiters an folgende Adresse(n) verschickt:
☑ herbert.haupt@bmsg.gv.at [electronic mail]
☑ telematik.gesundheit@bmsg.gv.at [electronic mail]

Alle Stellungnahmen werden unter http://www.argedaten.at/begutachtung veröffentlicht.

Stellungnahme der ARGE DATEN zu:

Bundesgesetz betreffend Übertragungssicherheit beim elektronischen Austausch von Gesundheitsdaten und Einrichtung eines Informationsmanagement (Gesundheitstelematikgesetz)

[BM FÜR SOZIALE SICHERHEIT UND GENERATIONEN (BMAS/BMSG) / 70.101/22-VII/B/10/02]

Grundsätzlich begrüßt die ARGE DATEN das Vorhaben bei der Verwendung von Gesundheitsdaten verpflichtende Mindeststandards zur Einhaltung von Sicherheitsmaßnahmen einzuführen.

Wie viele Anfragen von besorgten Menschen bei der ARGE DATEN bestätigen, stellt die Schaffung von Vertrauen bei der Übermittlung sensibler medizinischer Informationen ein wichtiges grundsatzpolitisches Anliegen dar.

Es wird damit versucht zumindest im Bereich des Gesundheitswesens eine geradezu unerträgliche Gesetzeslücke des DSG 2000 (das Fehlen jeglicher sicherheitstechnischer Mindeststandards) zu füllen.

Leider enthält der Entwurf eine Reihe problematischer Punkte, die es fraglich machen, ob das angestrebte Ziel erreicht werden kann. Darüber hinaus sieht der Entwurf mit der Schaffung des "Gesundheitsdiensteanbieter-Registers" eine unnötige bürokratische Maßnahme vor, die bestenfalls zusätzliche Kosten, möglicherweise aber auch zusätzliche Überwachung einzelner Einrichtungen bedeutet, ohne irgendeinen zusätzlichen Sicherheitsvorteil zu schaffen.

Die Problempunkte im Einzelnen:

(1.) UNKLARER BEGRIFF "GESUNDHEITSDATEN"

Im §2 Z1 werden zwar eine Reihe von Beispielen gegeben, was unter den Begriff "Gesundheit" verstanden werden könnte, doch ist die Liste weder vollständig, noch systematisch organisiert. So bleibt der Komplex Ernährung, Nahrungsmittel und Ernährungsgewohnheiten ebenso unerwähnt wie Sexualverhalten, der Bereich Umwelt und Umwelteinflüsse und deren Einwirkungen auf die Gesundheit, ebenso der Bereich Unfälle und Unfallursachen oder der Bereich gesundheitliche Auswirkungen von Wohnverhältnissen.

Der Begriff "Lebensgewohnheiten" muss ausdrücklich abgelehnt werden, da er zusehr auf das Verhalten der Einzelperson abzielt, viele "Lebensgewohnheiten" nicht oder nicht vordringlich gesundheitsrelevant sind und eine derartig unscharfe Begriffsdefinition einer

willkürlichen Auslegung Tür und Tor öffnet. Umgekehrt existieren viele vom Einzelnen nicht beeinflussbare Faktoren (Umweltfaktoren), die direkte Auswirkungen auf seine persönliche Gesundheit haben.

Im Ergebnis könnte eine derartige Definition dazu führen, dass auch privater Informationsausstausch über alltägliche Lebensverhältnisse durch dieses Gesetz reglementiert wird.

Als völlig missglückt muss die Begriffsbildung "Familiengeschichte" im Zusammenhang mit Gesundheit angesehen werden. Hier drängen sich Assoziationen zum unsäglichen "Arier-Nachweis" der NS-Zeit auf.

Die Definition für Gesundheitsdaten wird daher abgelehnt. Es wird empfohlen auf eine beispielhafte Aufzählung zu verzichten und die WHO-Gesundheitsdefinition als Basis für dieses Gesetz heranzuziehen.

(2.) IRREFÜHRENDER BEGRIFF "GESUNDHEITSDIENSTEANBIETER"

Der Begriff wird zwar durch eine umfangreiche taxative Auflistung im Anhang beschrieben, geht jedoch an der tatsächlichen Problematik vorbei.

Offenbar versuchte man alle Stellen zu identifizieren, die professionell (beruflich) Gesundheitsdaten verwenden, tatsächlich ist dieser Bereich wesentlich breiter anzusehen und umfasst nicht nur Stellen, die Gesundheitsdaten zu Heilzwecken verwenden, sondern zu anderen Zwecken, etwa zur Erbringung von Versicherungsleistungen, zur Feststellung von Qualifikationen und Fähigkeiten, zur Feststellung von Eintritts- und Zugangsrechten.

Ansatzweise wurde dieser Tatsache dadurch Rechnung getragen, dass unter Punkt 24 "Private Krankenversicherungen" angeführt werden. Niemand, auch nicht der Autor des Entwurfes kann damit meinen wollen, dass es sich hier um Einrichtungen zur Erbrinung von Gesundheitsleistungen handelt, sondern um Einrichtungen, die Gesundheitsleistungen finanzieren.

Gleichzeitig wurden jedoch private Lebensversicherer, sonstige Personenversicherer, Arbeitgeber, Arbeitsvermittler, Wellness- und Sporteinrichtungen, um nur einige zu nennen, vergessen. Genau in diesem Grenzbereich führt jedoch der schlampige Umgang mit Gesundheitsinformationen oft zu einem unzulässigen Eingriff in die Privatsphäre.

Ärzte und sonstige Personengruppen, die schon heute besonderen Geheimhaltungsverpflichtungen unterliegen, mit einem zusätzlichen Gesetz zu belasten, ist wenig zielführend. Hier würden allgemeine Richtlinien bzw. gezielte fachgesetzliche

Anpassungen, mit welchen technischen Mindeststandards diese besonderen Verschwiegenheitspflichten erfüllt werden müssen, genügen.

Informationen zur Gesundheit und über die eigene Gesundheit sind zentraler Bestandteil der Lebensgestaltung und daher in praktisch allen Bereichen, sei es Privatleben, Beruf, Freizeit, ... präsent. Ein Gesetz das den sicheren Umgang mit diesen Informationen regelt, sollte daher alle Personenkreise umfassen, die berufsmäßig mit Gesundheitsinformationen Dritter beschäftigt sind.

Es wird daher empfohlen den IRREFÜHRENDEN und im Ergebnis nichtssagenden Begriff "Gesundheitsdiensteanbieter" wegzulassen und stattdessen festzustellen, dass das Gesetz für alle Stellen gilt, die berufsmäßig Gesundheitsdaten Dritter verwenden.

(3.) VERPFLICHTUNG ZUR VERSCHLÜSSELUNG

Die Verpflichtung zur Verschlüsselung während der Übertragung wird ausdrücklich begrüßt. In diesem Sinn treffen §3 Abs.1 - 3 jedenfalls die im DSG 2000 vermissten notwendigen Klarstellungen.

Weitergehende Regelungen und Verpflichtungen zur Verschlüsselung sind jedoch entbehrlich. Auf dem Verordnungsweg bestimmte Methoden festzuhalten bringt bei einem sich derartig rasch entwickelnden Gebiet, wie der Verschlüsselung, bloß zusätzliche bürokratische Hemmnisse.

Die Wahl geeigneter, dem Stand der Technik entsprechender Methoden, ist eher als Schulungs- und Aufklärungsarbeit anzusehen und kann von verschiedensten Forschungs- und Beratungseinrichtungen übernommen werden.

Sinnvoll wäre allenfalls die Schaffung einer Möglichkeit für Organisationen, ihre verwendete Übertragungstechnik auf freiwilliger Basis prüfen bzw. zertifizieren zu lassen.

(4.) VERPFLICHTUNG ZUR SIGNATUR VON DATEN

Die unter dem Titel "Authentifizierung und Integrität" geführten Bestimmungen des §4 sind irreführend und verworren. Eine Verpflichtung zur "elektronischen Signatur" im SInne des SigG ist sachlich entbehrlich.

Sinnvoll ist jedenfalls die eindeutige Kennzeichnung übertragener Informationen und auch die Protokollierung der einzelnen Übertragungsvorgänge.

Diese Kennzeichnung kann auf den unterschiedlichsten technischen Ebenen stattfinden, wobei im gängigen Sprachgebrauch nur auf der Applikationsebene die Verknüpfung von Daten mit Prüf- und Hash-Werten, wie sie typisch für digitale Signaturen sind, als

"digitale Signatur" bezeichnet werden. In darunterliegenden technischen Layern werden derartige Verfahren schlicht als "Prüfsummen-Verfahren" bezeichnet.

Die vorgelegte Bestimmung würde eine Reihe von technisch sicheren Übertragungsmethoden ausschließen, weil die Verschlüsselung und die Authentisierung auf einem protokolltechnisch tieferen Ebene stattfindet. Sogenannte Virual Privat Network - Lösungen, die für die sichere Datenübertragung keine individuelle Verschlüsselung und Signatur benötigen, wären durch den vorgelegten Entwurf ausgeschlossen.

Tatsächlich wäre es aus sicherheitstechnischer Sicht begrüßenswert, dass übertragene Informationen nicht individuell auf Anwendungs- oder Datensatzebene verschlüsselt werden, sondern schon der gesamte Übertragungsweg, am besten hardwaretechnisch, abgesichert ist.

Werden Verschlüsselungsverfahren verwendet, müssen diese zwangsläufig, ansonsten ist eine Entschlüsselung der Daten nicht möglich, Prüfsummen- und Integritätsprüfverfahren enthalten.

Es wird empfohlen auf die Ausführungen des §4 zu verzichten und unter §3 festzuhalten, dass bei der Verschlüsselung Verfahren zu verwenden sind, die auch Integritätsprüfungen der übertragenen Daten vornehmen. Bezüglich der Authentifizierung siehe unten.

(5.) NACHVOLLZIEHBARKEIT UND EMPFANGSBESTÄTIGUNG

In den §§5f werden unter den unüblichen Bezeichnungen "Nachvollziehbarkeit und Empfangsbestätigung" Elemente zur Verpflichtung der Protokollierung vorgestellt.

Diese neuartige Begriffsbildung ist fachlich und rechtssystematisch abzulehnen. Beide Paragraphen sollten vollständig neu überarbeitet werden.

Unter den Titel "Protokollierung" sollte abschließend aufgezählt werden, welche Daten(arten) zu protokollieren sind, wie lange diese Daten aufzubewahren sind, welchen Datenaufbau die Empfangsbestätigungen haben, welche Daten zur Authentifizierung dienen und wie sichergestellt wird, dass der Betroffene dessen Daten übertragen wurden, seinen Auskunfts-, Informations- und Richtigstellungsrechten nachkommen kann.

Da Gesundheitsdaten vielfach unstrukturiert, etwa als Röntgenbilder, als Sammelbefunde oder als Abrechnungslisten für viele Betroffene gemeinsam übermittelt werden, müssen die Auskunftsrechte so gestaltet werden, dass jeder Betroffene zwar zuverlässig über seine Daten Auskunft erhält, jedoch keinesfalls Informationen über Dritte erfährt.

(6.) EU-WIDRIGES "REGISTER DER GESUNDHEITSDIENSTEANBIETER"

Eine grundsatzpolitische Zumutung stellt das angestrebte "Register der Gesundheitsdiensteanbieter" dar. Es ist in keiner Weise erkennbar, welchen neuen Zweck und welchen zusätzlichen Nutzen ein derartiges Register haben könnte. Tatsächlich sind alle im Anhang genannten möglichen Institutionen strengen Niederlassungs- und Zugangskriterien unterworfen und entsprechend registriert. Elektronische Datenverwendungen im sensiblen Bereich müssen gemäß DSG 2000 registriert werden.

Ein weiteres Register mag zwar persönliche Informations- und Überwachungswünsche des zuständigen Bundesministers befriedigen, innerhalb der österreichischen Rechtsordnung wäre es jedoch bloß eine zusätzliches bürokratisches Instrument.

Wie schon eingangs erwähnt wäre das Register auch unpraktikabel, da viel mehr Stellen, als im Anhang aufgezählt, Gesundheitsdaten verwenden und elektronisch übermitteln und daher von den Regelungen des Gesetzes erfasst sein sollten.

Weiters ist ein derartiges Register EU-widrig, da ausländische Einrichtungen (Ärzte, Labors, Versicherungen, ...) sicher auch berechtigt sein werden, Gesundheitsdaten zu übertragen und zu verwenden, nicht aber gezwungen werden können, sich in einem lokalen österreichischen Register einzutragen. Damit werden österreichische Einrichtungen diskriminiert, zumindest jedoch zusätzlichen bürokratischen Hemmnissen unterworfen.

Gerade um derartige Unterschiede innerhalb der EU auszuschließen, wurde die Datenschutz-Richtlinie beschlossen. Es ist ein Versäumnis, dass diese Richtlinie bisher von Österrreich nicht praxisorientiert umgesetzt wurde.

Eine Teilregelung, wie für den Gesundheitsbereich, muss sich trotzdem an den Rahmen der EU-Richtlinie enthalten und kann nicht zusätzliche Beschränkungen festlegen.

(7.) ZUSAMMENFASSUNG

Der Entwurf versucht eine längst überfällige Rechtslücke des DSG 2000 zu schließen und die vorhandene Rechtsunsicherheit zu beseitigen. Der Entwurf fällt jedoch unter das Kapitel "gut gemeint".

Inhaltlich bestehen missglückte Begriffsbestimmungen, im technischen Teil wird eine bestimmte technische Lösung unzulässigerweise bevorzugt und schränkt damit die Freiheit der Gestaltung von Unternehmen und Einrichtungen ein. Im grundsatzpolitischen Teil wird mit dem Aufbau eines EU-widrigen "Gesundheitsdiensteanbieter-Registers" ein unnötiger Schritt in Richtung mehr Überwachung vollzogen.