GESELLSCHAFT
FÜR INFORMATIK

Berlin, 5. Juni 2020

Stellungnahme

des Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“
der Gesellschaft für Informatik e.V.

zum Referentenentwurf des Bundesministeriums für Gesundheit

einer „Datentransparenzverordnung (DaTraV)“

GESELLSCHAFT
FÜR INFORMATIK

Unzureichende Sicherheitsqualität der Datentransparenz-verordnung (DaTraV) des BMG

Das „Digitale-Versorgung-Gesetz (DVG) für eine bessere Versorgung durch Digitalisierung und Innovation im Forschungsbereich des Gesundheitswesens“ vom 19. Dezember 2019 enthält zur Regelung weiterer Details eine Datentransparenzverordnung (DaTraV) – Referentenentwurf vom 13. Mai 2020.

Dieser Entwurf sieht die Sammlung der Versicherungs- und Behandlungsdaten aller 73 Mio. Pflichtversicherten vor. Jedoch werden elementare Sicherheits-bedürfnisse zum Schutz der Gesundheitsdaten aller Versicherten (private und zudem hochsensible Daten) nicht oder nur unzureichend berücksichtigt.

- Vorgesehen ist die zentrale Sammlung der Daten sämtlicher gesetzlich Versicherter ohne Widerspruchsmöglichkeit. Versicherte müssen auf Grundlage dieser Verordnung die Hoheit über ihre Daten vollständig aufgeben.
- Mithilfe sogenannter Lieferpseudonyme und späterer sogenannter periodenübergreifender Pseudonyme werden vermeintlich Maßnahmen zur Wahrung des Rechts auf Datenschutz ergriffen. Diese sind jedoch bei weitem nicht ausreichend, wie aus der Aufstellung der erhobenen Daten hervorgeht. Die Lieferpseudonyme ermöglichen eine eindeutige Identifizierung der Versicherten – mit dem Ziel, die Daten auf Vollständigkeit, Plausibilität und Konsistenz zu prüfen. Das Verfahren stellt sicher, dass Versicherten – unabhängig von Randbedingungen wie Kassenzugehörigkeit etc. – dasselbe Pseudonym zugeordnet wird. Periodenübergreifende Pseudonyme erlauben die Identifizierung Versicherter über einen sehr langen Zeitraum hinweg und sind aus der Perspektive des Datenschutzes daher besonders risikobehaftet.
- Mit den erhobenen Daten wie Geburtsjahr, Postleitzahl, Geschlecht, Betriebsnummer der Krankenkasse sowie Kosten- und Leistungsdaten aus ambulanter und stationärer Versorgung, Versorgung mit Arzneimitteln, Heil- und Hilfsmitteln und vielen weiteren Daten kann auf die Identität der Versicherten geschlossen werden.
- Die Bereitstellung einer Datenbasis an die Forschung ist grundsätzlich begrüßenswert. Jedoch regelt die Verordnung keineswegs Beschränkungen, die für die Nutzung dieser Daten gelten müssen. Der Zugriff auf die Datenbestände ohne jegliche Beschränkung und Kontrolle stellt daher

eine enorme Bedrohung für alle persönlichen und personenbezogenen Gesundheitsdaten dar.

Wir begrüßen grundsätzlich die Einbeziehung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in (BfDI) die Definition der Anforderungen an die Pseudonymisierungsverfahren; die Einbeziehung greift jedoch zu kurz, weil die Ausstattung mit konkreten Kompetenzen unterbleibt. Beiden Behörden verbleibt im vorliegenden Entwurf lediglich die Funktion eines Feigenblatts. Nicht nur die Bildung von Pseudonymen ist von Interesse, es muss vielmehr eine aktive Vorsorge gegen den Missbrauch der erhobenen und später verarbeiteten Daten erkennbar, nachvollziehbar und durch unabhängige Gremien und Institutionen prüfbar werden.

Zusammenfassend muss gesehen werden, dass mit dieser durch den Spitzenverband betriebenen Datensammlung ein attraktiver, schlecht abgesicherter Angriffspunkt installiert wird – auch für Kriminelle: Bereits ein einziger Sicherheitsvorfall kann ausreichen, um persönliche Daten aller Versicherten in der Bundesrepublik unberechtigt offen zu legen. Über den wenig nützlichen Satz „Jeglicher Datenzugriff von unberechtigten Stellen ist auszuschließen“ hinaus, werden (fast) keine Datenschutzmaßnahmen vorgeschlagen. Es werden insgesamt keinerlei Sicherheitsvorgaben oder Sorgfaltspflichten der Krankenkassen und des Spitzenverbands formuliert, mit denen Datenschutz und Sicherheit der Daten gewährleistet werden könnten. Der Entwurf beinhaltet keinerlei Vorgaben, um sowohl den unberechtigten Zugriff als auch das Speichern verfälschter Daten zu verhindern oder auch nur angemessen zu erschweren.

Das BMG hat eine Frist von 9 (!) Kalendertagen für Stellungnahmen gesetzt; diese Frist erscheint unangemessen kurz, zumal bereits Entwürfe im Mai 2019 kursierten.

Der Entwurf muss zurückgezogen werden und es muss eine sorgfältige öffentliche Analyse der Risiken unter Einbeziehung von BfDI, BSI und der Fachöffentlichkeit erstellt werden. Neue und weitere Entwürfe müssen mit einer fachlich angemessenen Kommentarfrist (z. B. 6 Wochen) veröffentlicht werden.

GESELLSCHAFT
FÜR INFORMATIK

Über den Präsidiumsarbeitskreis Datenschutz und IT-Sicherheit der GI

Sicherheits- und Datenschutzaspekte werden stark zunehmend von Gesellschaft, Unternehmen und auch der Politik adressiert. In der GI befassen sich eine Vielzahl von Fachbereichen (u.a. Sicherheit – Schutz und Zuverlässigkeit) mit diesen Themen, so dass das Präsidium den alle Fachbereiche übergreifenden Arbeitskreis Datenschutz und IT-Sicherheit mit der Bearbeitung beauftragt hat. Weitere Informationen finden Sie unter pak-datenschutz.gi.de

Über die Gesellschaft für Informatik (GI)

Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Die Mitglieder binden sich an die Ethischen Leitlinien für Informatikerinnen und Informatiker der GI. Weitere Informationen finden Sie unter www.gi.de.