Entschließung

der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. März 2013

Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.

- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen bzw. absehbar kommen sollen. Hierzu hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser Entschließung).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Abs. 3 BKRG festgelegt werden.

Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen

Anlage zur Entschließung der 85. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder

Mindestens folgende Anforderungen sind an die zukünftige Gestaltung und den Einsatz des Algorithmus zur Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen zu stellen:

- Die kryptografischen Komponenten sind unter Berücksichtigung der Empfehlungen des BSI gemäß dem derzeitigen Stand der Technik zu wählen. Ihre Sicherheitseigenschaften sollen auf unabhängigen kryptografischen Annahmen beruhen. Beide Komponenten müssen sich durch geheim zu haltende Schlüssel parametrisieren lassen.

- Zur Wahrung der Verknüpfbarkeit des derzeitigen Datenbestandes mit zukünftigen Meldungen kann eine Überverschlüsselung der ersten Stufe der derzeitigen Kontrollnummern (dem Ergebnis der Anwendung einer Hashfunktion auf Bestandteile der Identitätsdaten) erfolgen.

- Eine flexible Ausgestaltung des Verfahrens soll vorausschauend berücksichtigen, dass auch in Zukunft mit der Notwendigkeit des Austauschs von kryptografischen Methoden zu rechnen ist.

- Die Sicherheit des verwendeten Schlüsselmaterials wie auch seiner Nutzung ist bei allen Beteiligten durch Maßnahmen der Systemsicherheit, den Einsatz von dem Stand der Technik entsprechenden Kryptomodulen und die Protokollierung von Einsatz und Administration auf einheitlichem Schutzniveau zu gewährleisten.

- Für jedes Register und jedes Abgleichverfahren sind zumindest in der zweiten Stufe der Kontrollnummernbildung spezifische Schlüssel einzusetzen.

- Bei einem Abgleich von Registerdaten ist zu gewährleisten, dass keine Zwischenwerte gebildet werden, aus denen Rückschlüsse auf Identitätsdaten möglich sind.