

# Das Geschäft mit den Verordnungsdaten

Ende des Jahres 2011 wurden dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) umfangreiche Unterlagen zur Verarbeitung von medizinischen Verordnungsdaten aus Apothekenrechenzentren zugespielt. Daraus ging hervor, dass Pharmaunternehmen personenbeziehbare Daten erhielten, mit denen sie detailliert das Ordnungsverhalten von Ärzten analysieren konnten. Mit diesen Daten kann die Ärzteschaft gezielt umworben und der Erfolg von Vermarktungsveranstaltungen effektiver gemessen werden<sup>1</sup>.

Eine Überprüfung der besagten Datenverarbeitung ist bis heute nicht abgeschlossen. Aktiv sind dabei mehrere Datenschutzbehörden und Staatsanwaltschaften. Über viele Jahre wurden personenbezogene Daten nicht nur von Ärzten, sondern auch von Versicherten unbeanstandet an die Pharmaindustrie weitergegeben. Beteiligt war ein Geflecht von Firmen, die von Apothekenrechenzentren, Krankenkassen und Pharmaindustrie beauftragt wurden. Das Motiv ist letztlich der Wert der Verordnungsdaten für die Pharmaindustrie. Das Geschäftsmodell der Pharmaindustrie und der beteiligten IT-Firmen beruht auf einem falschen Verständnis von Anonymisierung. § 300 Abs. 2 S. 2 Sozialgesetzbuch (SGB) V regelt für Apothekenrechenzentren: „Anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden.“

Anonymisieren ist das Verändern von personenbezogenen Daten, so „dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können“ (§ 67 Abs. 8 SGB X). Unstreitig ist, dass auch Ärztinnen und Ärzte gemäß dieser Norm „natürliche Personen“ sind.

Zunächst wurde von den Unternehmen vorgetragen, sie hätten keine Absicht einer Reidentifizierung verfolgt. Auf die subjektive Absicht bzw. Intention bei der Datenverarbeitung kommt es jedoch nicht an. Relevant sind die objektiven Bedingungen.

Dann wurde vorgetragen, eine Reidentifizierung wäre nur möglich, wenn sich die Datenempfänger von Dritten unzulässig Zusatzwissen beschaffen; dies sei ein „unverhältnismäßiger Aufwand“. Praktisch erfolgt die „Anonymisierung“ unter Nutzung eines asymmetrischen Verfahrens durch die Verschlüsselung von identifizierenden Daten mit Hilfe eines öffentlichen Schlüssels, der unternehmensübergreifend verwendet wird, den Empfängern aber geheim gehalten werden soll. Der private Schlüssel wurde bzw. wird verworfen. Tatsächlich blieb der öffentliche Schlüssel

aber nicht geheim, sondern wurde an den Dienstleister der Pharmaindustrie weitergegeben. Dies bedeutet: Liegt das für die De-anonymisierung nötige Zusatzwissen bei einer anderen als der die Personendaten verarbeitenden Stelle (oder deren Auftragnehmer), so kann nicht mehr von Anonymität gesprochen werden.

Im konkreten Fall ist eine De-anonymisierung einfach möglich: Die zu verschlüsselnden Daten – etwa eines Arztes – werden mit dem öffentlichen Schlüssel verschlüsselt. Das Ergebnis wird mit den angeblich anonymisierten Datensätzen verglichen. Im Trefferfall hat man den Datensatz des namentlich bekannten Arztes gefunden.

Weiter wurde vorgetragen, das Ordnungsverhalten eines Arztes werde nicht übermittelt; die Daten würden zu einer Gruppe von Ärzten zusammengeführt, d. h. aggregiert, damit mit der Kenntnis des Ordnungsverhaltens eines Arztes hierüber eine De-anonymisierung verhindert werden könne. Dies genügt den Anonymisierungsanforderungen dann nicht, wenn ein bestimmtes Merkmal, z. B. ein ärztliches Ordnungsverhalten, auf alle aggregierten Ärzte zutrifft. Dieses Ordnungsverhalten ist als „Zusatzwissen“ – jedenfalls potenziell – für die Dienstleister der Pharmaindustrie verfügbar.

In die Diskussion gebracht wurde schließlich der Einsatz eines „Trustcenters“. Tatsächlich können derartige Trustcenter – z. B. bei Forschungsprojekten, wenn die gesetzlichen Regelungen eine Abwägung zulassen und keine vollständige Anonymisierung fordern – zur Wahrung der Betroffeneninteressen eingesetzt werden. Dies geht aber nicht, wenn – wie hier – vom Gesetz eine wirksame Anonymisierung gefordert wird. Schon die Datenweitergabe an das Trustcenter ist eine – unzulässige – Datenübermittlung.

Folgendes Vorgehen ist denkbar: Identifikationsmerkmale werden angemessen verschlüsselt; der Schlüssel darf nur der verarbeitenden Stelle verfügbar sein und sollte nur eine kurze Laufzeit haben. Der Informationsgehalt von im Klartext gelieferten Daten ist soweit zu reduzieren, dass eine Zuordnung über extern verfügbares Zusatzwissen nicht mehr möglich ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat verabredet, Kriterien für eine gesetzeskonforme hinreichende Anonymisierung zu erarbeiten. Die Pharmaindustrie bleibt aufgefordert, ihre illegale Datenbeschaffung einzustellen.

*Thilo Weichert*

*Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)*

<sup>1</sup> Der Spiegel 2012, Heft 7, Seite 121