Bürger gläserne

Heute ist der 4. Europäische Datenschutztag, der seit 2007 auf Initiative des Europarates ausgerichtet wird und mit dem das Bewusstsein der Bürger für den Datenschutz gestärkt werden soll. Die Redaktion von anwalt.de will dazu einen Beitrag leisten und zeigt, in welchen Lebensbereichen inzwischen Daten gesammelt und somit auch missbraucht werden können. Denn sind die Daten erst einmal übermittelt und erfasst, ist die Weitergabe an sich unumkehrbar, weil man sie nicht wieder hundertprozentig wieder zurückholen kann. Die Frage lautet: Zu welcher Personengruppe zählen Sie?

Datensicherheit: In Netzwerk oder Internet sollen mit Verschlüsselungstechniken Daten vor dem Zugriff Unbefugter gesichert werden

Der gläserne Patient?

Anlässlich des Gedenktages findet heute in Berlin eine Veranstaltung zum Thema „Gesundheitsdaten im Netz: Zu Risiken und Nebenwirkungen für das Persönlichkeitsrecht der Patienten" statt, die sich mit der Problematik der Speicherung und des Austausches von Patientendaten befasst. Im Gesundheitswesen kommen zum Beispiel für Abrechnungen vernetzte Systeme zum Einsatz, über die sensible Gesundheitsdaten gespeichert und ausgetauscht werden. Die Experten aus Medizin, Wissenschaft, Datenschutz und Verwaltung werden sich mit den datenschutzrechtlichen Risiken von Elektronischer Gesundheitskarte, Online-Gesundheitsakten, Telematikinfrastruktur, elektronischen Fallakten, Telemedizin und auch Ärzteportalen befassen.

Im Gegensatz zu der derzeitigen Krankenkarte, die lediglich mit einem Speicherchip ausgestattet ist, soll die neue elektronische Gesundheitskarte mit einem Mikroprozessorchip versehen sein, der nicht nur die Speicherung von Daten auf dem Chip selbst, sondern in einem speziellen Netzwerk ermöglicht, damit der Datensatz per Internet jederzeit abgerufen und geändert werden kann, sog. Telematikinfrastruktur. Denn es reicht der Speicherplatz nicht aus, um freiwillige weitere Informationen (Patientenakte, Patientenfach etc.) auf dem Chip selbst zu hinterlegen. Diese Daten sollen über die Telematikinfrastruktur auf einem Server gespeichert werden.

Der technische Aufwand ist also enorm, da nicht nur spezielle Schutzsysteme, sondern auch Terminals und Ladestationen an verschiedenen Orten zur Verfügung gestellt werden müssen, damit der Karteninhaber und von ihm berechtigte Personen Zugriff auf seinen Datensatz erhalten. Vermutlich auch wegen des immensen technischen Aufwands wurde die Einführung der elektronischen Gesundheitskarte seit 2006 immer wieder verschoben. Die Kartenfunktionen Patientenakte und elektronisches Rezept werden laut Angaben des Gesundheitsministers derzeit nicht weiter verfolgt, weil für eine Umsetzung erst die datenschutzrechtlichen Anforderungen gewährleistet sein müssen. Dementsprechend erhöhen sich auch die Kosten. Die geschätzten Investitionskosten in Höhe von ca. 1,4 Milliarden Euro könnten nach Angaben des Pressesprechers der Firma Gematik im günstigsten Fall auf 2,8 Milliarden Euro, im schlechtesten Fall sogar auf bis zu 14,1 Milliarden Euro steigen („Monitor", DasErste, Sendung vom 02.07.2009). Damit dürfte die nächste Beitragssteigerung für Krankenversicherte im wahrsten Sinne des Wortes vorprogrammiert sein.

Weil es sich bei den erfassten Gesundheitsdaten um sensible Daten gemäß § 3 Bundesdatenschutzgesetz (BDSG) handelt, müssen hohe Sicherheitsanforderungen bei Telematikinfrastrukturen gewährleistet werden. Laut Gesetz ist deshalb jede weitere Nutzung dieser Daten ausgeschlossen und strafbar. Allerdings bietet jede Datenspeicherung auch das Risiko des Datenmissbrauchs durch Kriminelle. Eine Sicherheitslücke kann in jedem System auftauchen. Darüber hinaus bieten kommerzielle Anbieter inzwischen auch Internet-Gesundheitsakten an, für die kein vergleichbarer gesetzlicher Schutz gilt.

Der gläserne Fluggast?

Die Diskussion um die sog. Körperscanner flacht derzeit gerade wieder etwas ab. Auf europäischer Ebene steht aktuell eher wieder einmal die Weitergabe von Fluggastdaten zur Debatte. Bereits seit einigen Jahren sind Fluggesellschaften verpflichtet, Fluggastdaten von USA-Reisenden, für die keine Visumspflicht besteht, an die US-Behörden zu übermitteln. Seit Anfang 2009 erfolgt dies über die elektronische Reisegenehmigung ESTA (electronic system for travel authorisation), bei der die Daten 72 Stunden vor Reiseantritt online übermittelt und mit dem sie besser ausgewertet werden können. Zudem sollen die Daten mit ESTA nicht mehr nur zwölf, sondern bis zu fünfundsiebzig Jahre lang gespeichert werden.

Die Weitergabe von Fluggastdaten hat inzwischen auch bei anderen Staaten Begehrlichkeiten geweckt, etwa bei Kanada und Australien. Und auch in der EU strebt Großbritannien mit dem sog. eBorder eine Übermittlung von Fluggastdaten wie Telefon- und Kreditkartennummern zur Terrorbekämpfung per Rasterfahndung an. Derzeit ist eine solche generelle Weitergabe von Daten nach dem Bundesdatenschutzgesetz nicht erlaubt und die Vereinbarkeit mit dem EU-Recht nicht geklärt. Die Weitergabe von Name, Adresse und Passnummer stellt sich zunächst wenig spektakulär dar. Doch es werden auch Daten zu Krankheiten, Behinderungen und Straftaten abgefragt. Zusätzlich kommen hier die Ausweisdokumente ins Spiel. Bislang dürfen die Ausweisdaten ohne eine Gefahrensituation nicht bei innereuropäischen Flügen übermittelt werden und eine entsprechende Umsetzung würde also über die entsprechende Europäische Richtlinie 2004/82/EG, die für Fluggastdaten gilt, weit hinausgehen. Inzwischen regt sich auch im EU-Parlament Widerstand gegen die EU-weite Weitergabe von Fluggastdaten, das seit dem Lissabon-Vertrag aufgrund seines Mitspracherechts die Möglichkeit hat, sämtliche Gesetzesvorhaben im Bereich Justiz und Innere Sicherheit zu blockieren.

Hinweis: Nachdem mit dem ePass erstmals biometrische Daten (biometrisches Passfoto, Fingerabdrücke etc.) der Bürger erfasst wurden, wird nun auch der elektronische Personalausweis (ePA) eingeführt. Fingerabdrücke können aber beim ePA im Gegensatz zum ePass freiwillig auf dem Chip gespeichert werden. Der ePA soll die Identifizierung über das Internet ermöglichen und bei Behörden und im Geschäftsverkehr zum Einsatz kommen. Wer sich nicht mit dem neuen ePA anfreunden kann, hat noch bis 1. November Zeit, sich einen herkömmlichen Personalausweis ausstellen zu lassen.

Der gläserne Arbeitnehmer?

Seit Anfang des Jahres werden mit dem ELENA-Verfahren wichtige Daten von Arbeitnehmern monatlich vom Arbeitgeber elektronisch an die Zentrale Speicherstelle (ZSS) übermittelt. ELENA, der sog. Elektronische Entgeltnachweis, wurde von der letzten Bundesregierung am 25.06.2008 beschlossen und ist in den §§ 95ff. des Vierten Sozialgesetzbuches (SGB IV) geregelt. Übermittelt werden hauptsächlich Daten, die bislang von den Behörden auf Antragungsbögen und Formularen erfragt werden. Derzeit sind Daten von fünf Bescheinigungen aus den Bereichen Arbeitslosengeld I, Bundeserziehungsgeld und Wohngeld umgesetzt. Das gilt in erster Linie für die Sozialleistungsträger, aber auch in gerichtlichen Verfahren, etwa wenn es um Unterhalt oder Prozesskostenhilfe geht. ELENA wird planmäßig bis 2015 auf weitere Bereiche ausgedehnt, etwa auf Krankengeld, Kurzarbeitergeld, Arbeitslosengeld und Rentenzahlungen. Allerdings sind auch neue Informationen enthalten, beispielsweise die Teilnahme an Streiks, Abmahnungen und Kündigungsgründe.

Die Übermittlung und Speicherung der Daten erfolgt automatisch, ohne dass der Arbeitnehmer dem zustimmen muss. Die Teilnahme an ELENA ist also nicht freiwillig. Erst wenn eine Behörde auf die Daten zugreifen will, muss der Betroffene seine Zustimmung zum Abruf der Daten über eine elektronische Signatur (Registerkarte) erteilen. Er kann die Zustimmung dann zwar verweigern. Allerdings kann dann die Behörde ohne Zugriff auf die Daten nicht entscheiden, ob ihm die Leistung zusteht. Mit anderen Worten: Wer zukünftig Sozialleistungen beantragen will, wird der Behörde den Zugriff auf diese Daten genehmigen müssen. Achtung: Gemäß § 103 Abs. 1 S. 3 SGB IV kann aber das Einverständnis jederzeit widerrufen und zeitlich begrenzt werden. Derzeit werden die Daten übermittelt und für den Bedarfsfall bis zu fünf Jahre gespeichert. Die Sicherheit soll durch verschiedene Verschlüsselungen und Signaturen gewährleistet sein (sog. Doppel-Schlüssel-System). Bis spätestens 1. Januar 2012 soll den Behörden und Sozialträgern

der Abruf aller gespeicherter Daten ermöglicht werden. Laut Ministerium kann die Behörde in ihrer Datenbank nur die Informationen einsehen, die sie für ihren Bearbeitungsbereich benötigt.

Nachdem sich seit dem Start von ELENA in der Öffentlichkeit Protest gegen die Erhebung und zentrale Speicherung von sensiblen Arbeitnehmerdaten regte und Datenschützer und Arbeitnehmervertreter Kritik geäußert haben, sollen beispielsweise Daten zum Arbeitskampf (Streik, Aussperrung) nicht mehr wie ursprünglich geplant erfasst werden. Allerdings bleiben die Bedenken der Datenschutzbeauftragten von Bund und Ländern bislang bestehen, was die Erforderlichkeit von ELENA angeht. Denn hier werden wichtige Einkommens- und Verdienstdaten vorsorglich von ca. 35 bis 40 Millionen Bundesbürgern zentral gespeichert, obwohl überhaupt nicht feststeht, ob diese Daten je tatsächlich von den Betroffenen benötigt werden und ob sie je Sozialleistungen mit ELENA beantragen werden. Problematisch ist weiterhin, ob bei einem im ELENA-Formular enthaltenen Freitextfeld, das vom Arbeitgeber frei ausgefüllt werden kann, die datenschutzrechtlichen Vorgaben erfüllt sind. Aus diesen Gründen ist zu erwarten, dass schließlich wieder einmal das Bundesverfassungsgericht darüber befinden muss, ob ein solches Gesetz überhaupt mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar ist.

Datenschutz contra Sicherheit und Kosten?

Steht der Datenschutz zur Disposition, findet eine breite Diskussion in der Öffentlichkeit häufig erst statt, wenn das Gesetz bereits erlassen und die Reform in Kraft getreten ist. So war es beispielsweise beim ELENA-Verfahren. Schießt der Gesetzgeber manchmal über das Ziel hinaus, ist eine Entscheidung aus Karlsruhe gefragt. Das Bundesverfassungsgericht hat sich in der Vergangenheit häufig auf die Seite der Bürger gestellt und den Gesetzgeber zu Änderungen des Gesetzes verurteilt, etwa mit seinem Urteil zur Online-Durchsuchung *(BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07; 1 BvR 595/07, hierzu auch dieser anwalt.de-Rechtstipp)*. Doch bis das Bundesverfassungsgericht über einen solchen Streit entschieden hat, sind die Daten oft längst erfasst und gespeichert. Ist Eile geboten, bleibt den Verfassungsrichtern nur die Möglichkeit, die Nutzung (Abruf) der ohnehin bereits gespeicherten Daten in einer einstweiligen Anordnung zu untersagen, wie dies etwa bei der Vorratsdatenspeicherung geschehen ist *(BVerfG, Beschluss v. 28.10.2008, Az.: 1 BvR 256/08, hierzu auch dieser anwalt.de-Rechtstipp)*. Die Entscheidung zum Hauptsacheverfahren steht derweil noch aus. Auch gegen das BKA-Gesetz, das unter anderem die Wohnraumüberwachung per Video ermöglichen soll, ist inzwischen eine Verfassungsbeschwerde eingereicht worden, über deren Ausgang wir Sie gerne informieren werden.

Der gläserne Autofahrer (evtl. Pkw-Maut, Navi), der gläserne Kontoinhaber (SWIFT), der gläserne Ausländer (Ausländerzentralregister), der gläserne Handy-Nutzer (GPS) oder andere gläserne Bürger - bei jedem Eingriff in das Grundrecht der informationellen Selbstbestimmung müssen stets Datenart, Speicherdauer, Auswertungsmöglichkeiten und auch die Missbrauchsgefahr gegenüber Sicherheitsinteressen und Kostenfaktoren vom Gesetzgeber berücksichtigt und stets im Einklang mit dem Grundgesetz gewichtet werden. Nur wenn hier die Zweckmäßigkeit und Verhältnismäßigkeit gewahrt ist, sind solche Grundrechtseingriffe gerechtfertigt.

Denn eines steht fest, sind die getroffenen Sicherheitsvorkehrungen und Verschlüsselungssysteme auch noch so ausgefeilt: Mit jeder Weitergabe und Speicherung von Daten wird gleichzeitig auch deren Missbrauch möglich. Dabei spielt es für das Opfer von Datenmissbrauch vermutlich wenig eine Rolle, ob der Missbrauch durch fahrlässiges Handeln oder aus kriminellen Motiven erfolgte. Seine Daten sind Unbefugten zugänglich. Und zwar unwiederbringlich. Denn ist einmal ein unbefugter Datenzugriff möglich, sind diese Informationen nie mehr zu hundert Prozent sicher. Erschwerend kommt hinzu, dass bei der Sammlung solcher riesigen Datenmengen noch nicht endgültig absehbar ist, für welche Zwecke der Datenbestand in Zukunft noch genutzt werden soll. So wurde zum Beispiel bereits 2006 eine Zweckänderung der Lkw-Maut und die Nutzung der Mautdaten zur Strafverfolgung vom damaligen Innenminister angestrebt.