Wiesbaden, den 19. März 2015

Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Vor dem Hintergrund der Terroranschläge von Paris weisen die Datenschutzbeauftragten des Bundes und der Länder anlässlich ihrer 89. Konferenz darauf hin, dass der Datenschutz kein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates ist. Eingriffe in das Grundrecht auf informationelle Selbstbestimmung müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus tatsächlich zielführend und erforderlich sind. Ließe man jeden Eingriff in dieses Grundrecht zu, hätten die Terroristen eines ihrer Ziele erreicht.

Weitere Entschließungen der Konferenz:

Datenschutzgrundverordnung darf keine Mogelpackung werden

Die Verabschiedung der Datenschutzgrundverordnung geht auf die Zielgerade. Welche Rolle die Bundesregierung in den Verhandlungen spielt, bleibt für die Mitglieder der Datenschutzkonferenz undurchsichtig. Sie warnen eindringlich vor einer Aushöhlung des Datenschutzes. Von wesentlichen Datenschutzgrundsätzen wird durch die jetzt vorgeschlagene Fassung des Kapitels 2 der Datenschutzgrundverordnung abgewichen.
Dies betrifft insbesondere:

- Den Grundsatz der Datensparsamkeit
- Das Zweckbindungsgebot und
- Das Einwilligungsgebot

Zudem wird das Privileg, personenbezogene Daten zu Forschungszwecken zu verarbeiten, über das Recht auf informationelle Selbstbestimmung gestellt.

Damit wird nicht die angestrebte Verbesserung, sondern eine Verschlechterung des Datenschutzniveaus erreicht.

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telefon (06 11) 14 08-0 · Telefax (06 11) 14 08-9 00 oder -9 01
E-Mail poststelle@datenschutz.hessen.de · Internet http://www.datenschutz.hessen.de

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Der Nachweis, dass amerikanische Sicherheitsbehörden nicht auf personenbezogene Daten zugreifen, die deutsche Unternehmen an US-Unternehmen übermitteln, kann nach den Enthüllungen von Edward Snowden kaum erbracht werden.

Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht unmittelbar anwendbar ist, dürfen damit nach Auffassung der Konferenz nur erfolgen, wenn folgendes sichergestellt ist:

- Einhaltung der Zweckbindung
- Beschränkung staatlicher Zugriffsmöglichkeiten auf ein angemessenes und grundrechtskonformes Maß
- Sicherstellung der Betroffenenrechte (Auskunft, Berichtigung, Löschung)
- Sicherstellung des Rechtsschutzes bei Verstößen

Verschlüsselung ohne Einschränkungen ermöglichen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Schaffung einer Infrastruktur, die eine verschlüsselte Kommunikation von Bürgern, Verwaltungen, Unternehmen mit- und untereinander ermöglichen. Durch Schaffung einer solchen Infrastruktur kann die Sicherung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet werden. Es ist nach Auffassung der Datenschutzbeauftragten des Bundes und Länder Aufgabe der Politik, dies aktiv zu unterstützen. Eine Einschränkung kryptographischer Verfahren durch staatliche Regulierungen lehnt die Konferenz ab.

Sicherheit informationstechnischer Systeme nicht ohne Datenschutz

Informationssicherheit und Datenschutz haben Gemeinsamkeiten, jedoch geht die Stärkung der Informationssicherheit vielfach mit Eingriffen in das Recht auf informationelle Selbstbestimmung einher. Dies kann nur aufgrund normenklarer Regelungen zulässig sein, aus denen sich ergibt, welche personenbezogenen Daten für welchen Zweck erhoben, verarbeitet und gespeichert werden. Das vorgelegte IT-Sicherheitsgesetz erfüllt diese Anforderungen nach Auffassung der Datenschutzkonferenz nicht. Die Konferenz kritisiert zudem, dass nach dem derzeitigen Gesetzgebungsstand die Informationssicherheit allein den Behörden aus dem Direktionsbereich des Bundesinnenministeriums überlassen ist. Damit sei bei der Abwägung zwischen Sicherstellung der Informationssicherheit und klassischer Gefahrenabwehr und Strafverfolgung ein Interessenskonflikt vorprogrammiert.

Mindestlohngesetz und Datenschutz

Ein Unternehmen haftet dafür, ob ein beauftragtes Subunternehmen an seine Beschäftigten den Mindestlohn zahlt. Bei der Überprüfung, ob beauftragte Subunternehmen ihrer Zahlungsverpflichtung nachkommen, werden vielfach Mitarbeiterdaten in einem Umfang erhoben, der datenschutzrechtlich nicht gerechtfertigt ist. Die Konferenz appelliert an den Gesetzgeber, bei der in Aussicht gestellten Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten.

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Der vorgelegte eHealth-Gesetzentwurf sollte die Chance nutzen, die IT-Nutzung im Gesundheitsbereich datenschutzgerecht auszugestalten. Das ist bisher nicht der Fall. Insbesondere sollte sichergestellt werden, dass die gesetzlich zugestandenen Patientenrechte (Auskunft/Löschung von Daten) von Versicherten auch wahrgenommen werden können.

Auch muss nach Auffassung der Konferenz der Gesetzgeber klare Rahmenbedingungen schaffen, inwieweit Berufsgeheimnisträger externe Dienstleister beauftragen dürfen und wie gegebenenfalls die Daten bei diesen Dienstleistern zu schützen sind.

Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

Der Einsatz von Systemen zur Datenanalyse („Big Data“) zu Vorhersagen über künftige Straftaten ist nicht ohne Risiken. Er kann zu einer Verschiebung der Eingriffsschwelle von polizeilichen Handlungen im Vorfeld von Gefahren und Straftaten führen. Dies gilt erst Recht, wenn allgemein zugängliche Daten aus dem Internet mit Daten aus polizeilichen Informationssystemen verknüpft werden und die Auswertungskriterien nicht bekannt sind.

Die derzeit zum Teil in den Ländern eingesetzten Verfahren rufen diese Risiken zwar nicht hervor, doch können geringfügige Änderungen zu einer anderen Bewertung führen.