**81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 16./17. März 2011**

# Datenschutzrechtliche Herausforderungen annehmen!

Zum Abschluss der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat der diesjährige Konferenzvorsitzende, der Bayerische Landesbeauftragte für den Datenschutz Dr. Thomas Petri, gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, und dem Landesbeauftragten für den Datenschutz Baden-Württemberg, Jörg Klingbeil, die Konferenzergebnisse vorgestellt. Baden-Württemberg war Ausrichter der Konferenz 2010.

Vor wenigen Tagen veröffentlichte die Gemeinsame Kontrollinstanz von Europol ihren Kontrollbericht zur Umsetzung des SWIFT-Abkommens. Nach diesem Abkommen dürfen europäische Bankdaten nur auf begründetes Ersuchen hin an die US-Sicherheitsbehörden übermittelt werden. Für die Beurteilung der Rechtmäßigkeit des Ersuchens ist die Europäische Polizeibehörde Europol zuständig. Ausweislich des Kontrollberichts waren die bei Europol eingegangenen schriftlichen US-Anträge jedoch nicht spezifisch genug begründet, um eine Entscheidung über die Genehmigung oder Ablehnung zu ermöglichen. Vielmehr waren die Anträge der USA viel zu abstrakt gehalten, um die korrekte Bewertung der Notwendigkeit der beantragten Datenübermittlungen zu ermöglichen. Dessen ungeachtet genehmigte Europol jeden eingegangenen Antrag. Nach Auffassung der Konferenz stellt diese Vorgehensweise eine gravierende Missachtung der datenschutzrechtlichen Vorgaben des SWIFT-Abkommens dar.[1]

Die EU-Kommission hat einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt. Zentraler Gegenstand des Entwurfs ist die systematische Erfassung und Verarbeitung der Daten aller Fluggäste, die die EU-Außengrenzen überschreiten. So sollen Flugpassagierdaten künftig anlassfrei automatisiert ausgewertet und analysiert werden, ohne dass die Notwendigkeit hierfür erwiesen ist. Das Vorhaben der EU-Kommission läuft letztlich auf eine verdachtslose Vorratsspeicherung und Rasterung von Flugpassagierdaten hinaus. Die Konferenz fordert auch in Ansehung der verfassungsrechtlichen Vorgaben die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.[2]

Um verschlüsselte Internetkommunikationsvorgänge – wie insbesondere Internettelefonie – überwachen und aufzeichnen zu können, greifen die Strafverfolgungsbehörden zur sogenannten Quellen-Telekommunikationsüber-wachung. Dabei wird beispielsweise auf dem Endgerät der betroffenen Person eine Software aufgebracht, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Strafverfolgungsbehörde weiterleitet. Die Konferenz macht darauf aufmerksam, dass diese Ermittlungsmethode in der Vorgehensweise einer Online-Durchsuchung gleicht und auch den Zugriff auf gespeicherte Inhalte ermöglicht. Eine Quellen-Telekommu-nikationsüberwachung kann daher nur auf der Grundlage konkreter, normenklarer gesetzlicher Regelungen erfolgen, die sicherstellen, dass sich die Überwachung auf die Daten des laufenden Telekommunikationsvorgangs beschränkt. Die gegenwärtigen Vorschriften der Strafprozessordnung reichen hierfür nicht aus. Die Konferenz fordert den Gesetzgeber auf, die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.[3]

Der Deutsche Bundestag berät derzeit verschiedene Gesetzentwürfe zur Regelung des Beschäftigtendatenschutzes. Die Konferenz begrüßt die gemeinsame Zielsetzung, den Datenschutz in Beschäftigungsverhältnissen auf eine rechtssichere Grundlage zu stellen. Um dieses Ziel vollumfänglich zu erreichen, müssen aber unter anderem folgende Anforderungen beachtet werden: Das Recht eines Beschäftigten, sich an die zuständige Datenschutzaufsichtsbehörde zu wenden, darf in keiner Hinsicht eingeschränkt werden. Hinsichtlich der Durchführung von Screenings sind klare materielle Kriterien – wie die Prüfung der Verhältnismäßigkeit – erforderlich. Zur Klärung der Rechtslage sollten auch Bestimmungen etwa zum Whistleblowing, zur Personalaktenführung, zum Konzerndatenschutz und zu Folgen etwaiger Datenschutzverstöße aufgenommen werden.[4]

Für Abrechnungs-, Behandlungs- und Dokumentationszwecke übermitteln niedergelassene Ärztinnen und Ärzte vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Um auf die Beachtung der ärztlichen Schweigepflicht hinzuwirken, hat die Konferenz Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze formuliert.[5]

Angenommen hat die Konferenz auch eine Orientierungshilfe zur datenschutzkonformen Gestaltung und Nutzung von Krankenhausinformationssystemen. Im Hinblick auf den Einsatz der Informationstechnik in Krankenhäusern hat sich der dringende Bedarf gezeigt, zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen. Im Rahmen der Entwicklung und Ausarbeitung der Orientierungshilfe wurden neben Herstellern von Krankenhausinformationssystemen auch Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen. Das vorliegende Dokument wird den Datenschutzbehörden als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit dienen.[6]

1 Seite 355 in diesem Heft

2 Seite 355 in diesem Heft

3 Seite 355 in diesem Heft

4 Seite 356 in diesem Heft

5 Seite 356 in diesem Heft

6 Seite 357 in diesem Heft