

19. Entschließungen der Internationalen Konferenz der Datenschutzbeauftragten (Auswahl)

19.1 Transfer von Daten von Flugpassagieren

(Entschließung der 25. Internationalen Konferenz der Datenschutzbeauftragten vom 12. September 2003)

Die 25. Internationale Konferenz der Datenschutzbeauftragten beschließt folgendes:

Die Konferenz stellt fest, dass

Im Zuge des legitimen Kampfes gegen den Terrorismus und das organisierte Verbrechen werden in einigen Ländern Maßnahmen in Betracht gezogen, die die Grundrechte und Freiheiten, insbesondere das Recht auf den Schutz der Privatsphäre, gefährden könnten.

Das Risiko besteht, Demokratie und Freiheit zu gefährden, unter der Vorgabe diese Werte zu verteidigen.

Gesetzliche Anforderungen an Fluggesellschaften oder andere Transportanbieter den Zugriff an Gesamtdaten von Passagieren, die in Reservationssystemen gespeichert werden, zu gewährleisten oder diese zu übertragen, mit den internationalen Datenschutzgrundsätzen oder den Verpflichtungen der Transportanbieter, die sich auf den nationalen Datenschutzgesetzen stützen, im Konflikt stehen könnten.

Die Konferenz bekräftigt infolge dessen, dass

In der Bekämpfung des internationalen Terrorismus und des organisierten Verbrechens die Staaten unter vollständiger Achtung der Grundprinzipien des Datenschutzes reagieren sollten, denn diese Werte stellen einen integralen Bestandteil der Werte dar, die sie verteidigen.

Regelmäßige internationale Transfers von Personendaten, soweit nötig, nur innerhalb eines bestimmten Datenschutzrahmens erfolgen dürfen, z. B. auf Basis eines internationalen Abkommens, welches den datenschutzrechtlichen Anforderungen wie einem klar definierten Zweck, der verhältnismäßigen Datenerhebung, einer zeitlichen Begrenzung der Datenspeicherung, der Benachrichtigung der betroffenen Personen, der Gewährleistungen der Rechte der betroffenen Person, sowie einer unabhängigen Aufsicht gerecht wird.

19.2 Radio-Frequency Identification

(Entschließung der Internationalen Konferenz der Datenschutzbeauftragten vom 20. November 2003)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für die Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle von Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie könnten aber auch mit personenbezogenen Informationen, wie Kreditkarten-Daten, verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpft sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zur Erreichung dieses Zweckes erforderlich ist und

soweit RFID-Etiketten im Besitz von Personen sind, sollte diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.