

**08.07.10**

## **Antrag**

**des Freistaates Bayern**

---

### **Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes**

**- Antrag der Länder Hamburg und Saarland -**

Punkt 28 der 873. Sitzung des Bundesrates am 9. Juli 2010

Der Bundesrat möge folgende EntschlieÙung fassen:

1. Der Bundesrat erinnert an die Nummern 31 und 32 seines Beschlusses vom 13.02.2009 [BR-Drs. 4/09 (Beschluss)], mit dem er die Bundesregierung gebeten hat, einen Diskussionsentwurf für ein grundsätzlich überarbeitetes Datenschutzrecht vorzulegen, der die allgemeinen Regelungen im Bundesdatenschutzgesetz mit den bereichsspezifischen Vorschriften zusammenführt und systematisiert sowie das Datenschutzrecht angesichts neuer Formen und Techniken der Verarbeitung personenbezogener Daten risikoadäquat fortentwickelt.
2. Als ersten Schritt hierzu hält der Bundesrat die Schaffung einer rechtssicheren Regelung für die geschäftsmäßige Datenerhebung und -verarbeitung im Zusammenhang mit der georeferenzierten großräumigen Erfassung von Daten zum Zwecke des Bereithaltens fotografischer oder filmischer Panoramaaufnahmen im Internet zum Abruf für jedermann oder zur Übermittlung an jedermann für erforderlich. Auf den vorliegenden Gesetzesantrag wird verwiesen.

3. Der Bundesrat hält es sodann für erforderlich, in Wahrnehmung staatlicher Schutzpflichten für die informationelle Selbstbestimmung unter den Bedingungen der modernen Informationsgesellschaft folgende Regelungen zu schaffen:
  - 3.1. Völkerrechtliche Vereinbarungen zur datenschutzrechtlichen Verantwortlichkeit, die auch für nichtöffentliche Stellen, die ihren Sitz außerhalb der EU haben, verbindlich sind und deren Einhaltung von den deutschen Datenschutzaufsichtsbehörden wirksam überprüft werden können;
  - 3.2. Regelungen zur Verbesserung der Transparenz bei der Datenverarbeitung durch erweiterte Informations- und Auskunftspflichten der verantwortlichen Stellen;
  - 3.3. Regelungen für Verfahren, die nicht gezielt auf den Umgang mit personenbezogenen Daten gerichtet sind (z.B. RFID-Anwendungen, Fahrzeugdatenspeicher), um dem Risiko entgegenzuwirken, dass diese Daten ggf. von Dritten mit natürlichen Personen in Verbindung gebracht werden; dabei sind vor allem Vorschriften zur Wahrung der Persönlichkeitsrechte der Betroffenen wie z.B. klare Informationspflichten sowie Auskunfts- und Löschungsansprüche zu schaffen;
  - 3.4. Regelungen, die der Bildung von Persönlichkeitsprofilen (z.B. Konsumentenprofile, Bewegungsprofile, Nutzerprofile im Internet) möglichst enge Grenzen setzen;
  - 3.5. Regelungen für die Bewertung von Personen in Internetportalen;
  - 3.6. Regelungen für soziale Netzwerke zum Schutz des Persönlichkeitsrechts der Nutzer (z.B. Verpflichtung der verantwortlichen Stelle zu datenschutzfreundlichen Voreinstellungen, zu besonderem Schutz für minderjährige Nutzer, Löschungsanspruch bei Ausscheiden aus dem Netzwerk);

- 3.7. Regelungen, die der Erhebung, Speicherung, Auswertung und Bereitstellung von Informationen zur visuellen oder örtlichen Identifizierung von Personen im öffentlichen Raum oder einer Bestimmung ihres Aufenthaltsortes klare Grenzen setzen;
- 3.8. Regelungen zum Schutz personenbezogener Daten im Zusammenhang mit der planmäßigen Erfassung und Kartografierung von Funknetzdaten sowie der planmäßigen Aufzeichnung von Daten aus Mobiltelefonen und vergleichbaren Sendeanlagen;
- 3.9. Regelungen zum Umgang mit allgemein zugänglichen Daten im Internet, wie z.B. die Schaffung einer Verfallsklausel für in diesem Medium veröffentlichte Daten entsprechend § 35 Abs. 2 Satz 2 Nr. 4 des Bundesdatenschutzgesetzes;
- 3.10. Präzisierung der Anforderungen an die Wirksamkeit von Einwilligungen, z.B. durch das Verbot, auf die Einwilligung zurückzugreifen, wenn dadurch in Erlaubnistatbeständen enthaltene Schutzvorschriften für die Betroffenen umgangen werden;
- 3.11. Stärkung der innerbetrieblichen und behördlichen Instrumente der Vorabkontrolle bei Datenverarbeitungsverfahren, indem z.B. weitere Regelbeispiele ergänzt und eine schriftliche Dokumentation der Vorabkontrolle vorgeschrieben wird;
- 3.12. Verpflichtung der verantwortlichen Stellen, für ihre Datenverarbeitung personenbezogener Daten ein Datenschutzkonzept zu entwickeln und der Aufsichtsbehörde auf Verlangen vorzulegen;
- 3.13. Verbesserte Eigenkontrolle der verantwortlichen Stellen, indem beispielweise Mindestanforderungen an die Fachkunde des Beauftragten für den Datenschutz festgelegt und geeignete Nachweise vorgeschrieben werden und vorgesehen wird, dass der Beauftragte für den Datenschutz bei allen

datenschutzrechtlichen Vorgängen zwingend und rechtzeitig zu beteiligen ist.

4. Der Bundesrat bittet die Bundesregierung, umgehend einen intensiven Dialog mit den Ländern über die aufgezeigten Regelungserfordernisse zu eröffnen, um daraus baldmöglichst konkrete Vorschläge für die notwendigen Verbesserungen des Datenschutzrechts zu entwickeln.

Begründung:

Den Anforderungen, die in der modernen Informationsgesellschaft an den Persönlichkeitsschutz zu stellen sind, wird das Bundesdatenschutzgesetz trotz seiner zuletzt zum 11. Juni 2010 in Kraft getretenen Anpassungen nur unzureichend gerecht. Seine Aufgabe, verbindliche Regelungen zur Datenerhebung und -verarbeitung durch öffentliche Stellen des Bundes sowie durch nicht-öffentliche Stellen durch Eingriffsschranken des informationellen Selbstbestimmungsrechts sowie staatliche Schutzpflichten gegenüber seiner Gefährdung durch Private festzulegen, muss vielfach durch die Aufsichtsbehörden und Gerichte ersetzt werden. Deren Auslegung vermag das Spannungsverhältnis zwischen den aus der Anfangszeit der automatisierten Datenverarbeitung stammenden Grundsätzen und Einzelregelungen des Bundesdatenschutzrechts und den technologischen Möglichkeiten und Risiken der weltweiten Internetnutzung nicht immer befriedigend zu lösen.

Zur Gewährleistung eines hohen Datenschutzniveaus müssen deshalb zunächst aktuelle Problemstellungen wie die Rahmenbedingungen großräumiger georeferenzierter Panoramaaufnahmen deutscher Städte und Gemeinden durch den Gesetzgeber aufgegriffen werden. In einem zweiten Schritt muss die laufende bundespolitische Debatte über Aufgaben und Ziele der Internetpolitik des Bundes um konkrete Anliegen aus der Vollzugserfahrung der Datenschutzaufsichtsbehörden der Länder ergänzt werden.

Angesichts der aktuellen Debatte um neue Anwendungen bzw. Informationsangebote für die stationäre und mobile Internetnutzung und grundlegender Veränderungen des Kommunikationsverhaltens sind auf Grundlage der bewährten Datenschutzprinzipien der Erforderlichkeit, der Zweckbindung, der Transparenz und der Vorabkontrolle mindestens die unter Nr. 3 des Antrags genannten Leitthemen durch besonderen gesetzlichen Modernisierungsbedarf gekennzeichnet:

Vorrangig ist zunächst die Verantwortlichkeit globaler Diensteanbieter gegenüber den deutschen Datenschutzaufsichtsbehörden im Rahmen des Völkerrechts rechtssicher zu regeln.

Für verschiedene, in der Datenschutzpraxis bedeutsame Fallgestaltungen privater und gewerblicher Datenverarbeitung, wie z.B. Fahrzeugdatenspeicher, Bewertungsportale im Internet, soziale Netzwerke, Identifizierungsverfahren oder die Erfassung von WLAN-Daten, sind wirksame Schutzrechte zur

Abwehr von Gefährdungen der informationellen Selbstbestimmung zu entwickeln. Dazu zählt auch eine Regelung über die obligatorische Löschung von im Internet bereitgestellten personenbezogenen Daten. Angesichts der zunehmenden Möglichkeiten der Verknüpfung personenbezogener Daten sollte die Modernisierung des Datenschutzrechts zudem die Risiken der geschäftsmäßigen Bildung von Nutzerprofilen und der Akkumulierung und Aggregation von Nutzerdaten gerade unter den Bedingungen zunehmender Kommunikation über das Internet in allen Lebensbereichen aufgreifen. Besonderes Augenmerk erfordert außerdem der Schutz des Einzelnen vor einer zielgerichteten visuellen oder örtlichen Identifizierung durch neue Technologien. Die von mehreren Unternehmen angekündigten Gesichtserkennungsdienste widersprechen, unabhängig von der konkreten Ausgestaltung, dem Recht der informationellen Selbstbestimmung, da dies die jederzeitige Identifizierbarkeit im öffentlichen Raum sowie die Bestimmung des Aufenthaltsorts durch Dritte grundsätzlich ausschließt. Bei der planmäßigen Erfassung und Kartografierung von WLAN-Netzen besteht die Gefahr, dass diese Daten mit personenbezogenen oder personenbeziehbaren Daten der WLAN-Nutzer verknüpft werden. Es ist daher erforderlich, klare Regelungen für die geschäftsmäßige planmäßige Erfassung und Kartografierung von Funknetzdaten zu schaffen, die einerseits einen wirksamen Schutz der Bürgerinnen und Bürger vor der ungewollten Nutzung ihrer persönlichen Daten bieten, andererseits aber auch nicht die Verwendung moderner Technologien unbeabsichtigt erschweren oder verhindern. Da sich bereits weitere technische Möglichkeiten zur Erfassung von WLAN-Daten durch die Auswertung der Signale von sog. Smartphones abzeichnen, sollte die Regelung auch eine entsprechende Erfassung von Daten aus Mobiltelefonen und vergleichbaren Sendeanlagen mit einbeziehen.

Im materiellen Datenschutzrecht sollten die Anforderungen an die freie und informierte Einwilligung als zentrale Grundlage vieler Datenverarbeitungsverfahren im Internet, z.B. in sozialen Netzwerken, insbesondere durch genauere Regelungen ihrer Ausübung präzisiert werden. Zentrale Bedeutung hat dabei auch die Verbesserung der Informationsrechte des Betroffenen, die auf Grundlage der bewährten Systematik des Auskunftsanspruchs als Holschuld der Betroffenen z.B. durch Anforderungen an die Erkennbarkeit von Datenschutzhinweisen und den Abruf von Nutzerdaten fortentwickelt werden könnten. Die Einwilligung sollte als Rechtsgrundlage nur zugelassen werden, wenn Handlungsalternativen bestehen, sie durch aktives Tun erklärt wird, ihre Geltungsdauer begrenzt ist und ein strengeres Kopplungsverbot im Bereich der Werbung geschaffen wird.

Neben der Stärkung der innerbetrieblichen und behördlichen Instrumente der Vorabkontrolle (z.B. durch Erweiterung der meldepflichtigen Verfahrensarten) sollte die präventive Kontrolle von Datenverarbeitungsverfahren durch die Verpflichtung zur frühzeitigen Auseinandersetzung mit datenschutzrelevanten Fragestellungen neuer Anwendungen ergänzt werden.

Ziel der Modernisierung des Bundesdatenschutzgesetzes sollte es sein, das hohe Datenschutzniveau Deutschlands auch unter den Bedingungen der modernen Informationsgesellschaft zu bewahren und zukunftsfähig fortzuentwickeln.