Sind die gesetzlichen Schutzregelungen im Telekommunikationsgesetz und im Bundesdatenschutzgesetz für die Nutzenden ausreichend?

Thilo Weichert, Leiter des ULD

Bamberger Verbraucherrechtstage 2013

„Mobile Commerce“

Arbeitsgruppe 1 „Mobiler Datenschutz“

Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz

Bamberg 12.11.2013

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Facetten des „Mobilen Datenschutzes“

- Mobile Shopping
- Mobile Payment
- Kfz-Elektronik
- Öffentlicher Personenverkehr
- Mobile Marketing
- Location Based Services
- Mobilgeräte im Arbeitsbereich (Bring Your Own Device)
- Nutzung von Sozialen Netzwerken, Suchmaschinen, Clouds, Online-Spiele, Foren

Player – kumulativ oder alternativ

- Hersteller von Geräten, Betriebssystemen, Browsern
- Netzbetreiber
- Portalanbieter (z. B. Facebook, Google, Apple)
- App-Stores, App-Marketplaces, App-Anbieter
- Shop-Betreiber (Customer Relations Management)
- Payment-Anbieter (u. a. Banken, Kreditkartenunternehmen)

> Einzelne Rechtsbeziehungen, arbeitsteiliges Vorgehen, Individual- und Gruppenkommunikation

Netz-Infrastrukturen

- Global System for Mobile Communication (GSM)
- Universal Mobile Telecommunications System (UMTS)
- Long Term Evolution (LTE)
- Wireless Local Area Networks (WLAN)

Besonderheiten des Mobile Computing

- Erfassung von Standortdaten
- Funkkommunikation statt Austausch per Kabel
- Personale Verbindung von Mobilgerät mit Person
- Synchronisationsbedarf, Cloud-Nutzung

Datenkategorien u. Rechtsgrundlagen

- Inhaltsdaten > BDSG/EU-DSRl, künftig EU-DSGVO
- Nutzungs- und Verkehrsdaten > TMG, TKG/EU-TK-DSRl
- Stamm- und Bestandsdaten > TMG, TKG/EU-TK-DSRl

> Eingriffsgrundlagen orientieren sich grds. an Sensibilität

> Eigenständige Sensibilität von TK-Metadaten (Service, Partner, Ort, Zeit): Profiling, Tracking, Scoring, Personalizing

> Grundnorm: TMG (nicht TKG – Schwerpunkt bei Signalübertragung)

> Anwendung des Telekommunikationsgeheimnisses (Art. 10 GG, Art. 7 EUGRCh)

> Grundrecht auf Datenschutz (Art. 2 I iVm 1 I GG, Art. 8 EuGRCh)

Konflikte

- Personenbezug ?
- Datenschutzrechtliche Verantwortlichkeit ?
- Anwendbares Recht ?
- Verarbeitung von Standortdaten und –profilen ?
- Transparenz für die Betroffenen ?
- Anforderungen an Einwilligungen ?
- Realisierung der Betroffenenrechte ?

Personenbezug

Personenbeziehbarkeit besteht u.a. über folgende Identifikatoren:

dynamische IP-Adresse,
Cookie,
Geräte-ID (UDID), Identifier for Advertising (IDFA),
Kfz-Kennzeichen, Fahrzeugidentifizierungsnummer,
Browser-Fingerprint u. Ä.

Problem: pseudonyme Profile

Lösung: Regulierung des Profiling (vgl. Art. 20 EU-DSGVO)

Datenschutzrechtliche Verantwortlichkeit

- Arbeitsteilung vieler Stellen (Nutzer, Webseite, App-Anbieter, Portal, Netzbetreiber) auf (oft) unentgeltlich vertraglicher Basis
- § 3 Abs. 7 BDSG: wer „für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“
- Art. 2 lit d EU-DSRl: wer „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“
- Ebenso Art. 4 Abs. 5 EU-DSGVO
- VG Schleswig: Verfügungsgewalt nötig
- ULD SH: bewusste Zweckveranlassung genügt

Anwendbares Recht

Rechtsgrundlagen: § 1 Abs. 5 BDSG / Art. 4 EU-DSRl

- Grundsatz Territorialprinzip
- Ausnahme Niederlassung in der EU

OVG Schleswig: Bestimmt über Datenverarbeitung

ULD: Marketing und Akquise genügen

- Planungen EU-DSGVO

Art. 3 II a: Angebot von Waren und Dienstleistungen in EU

Art. 51 I: Territorialitätsprinzip

Art. 73: jede Aufsichtsbehörde = Beschwerdeadressat

Art. 54a: Vorrang „Lead Authority“ bei Hauptniederlassung

Art. 57 ff.: Kohärenzverf., bei Konflikt Europ. Privacy Board

Standortdaten

- Methoden: GPS, WLAN, Ortung Mobilfunk, NFC ...
- § 98 TKG/Art. 9 EU-TK-DSRl: wenn „zur Bereitstellung von Diensten mit Zusatznutzen erforderlich“, sonst Einwilligung

  Anzeigepflicht u. Information Mitbenutzende

  Unterdrückungsmöglichkeit im Einzelfall
- Direkt anwendbar für TK-Anbieter (vgl. § 15 III TMG, § 28 III BDSG)
- DS-Behörden: analoge Anwendung des § 98 TKG, aber: Was ist „erforderlich?“
- Problem: großes Vollzugsdefizit (u. a. App-Anbieter)

Transparenz für die Betroffenen

- Informationspflichten (§§ 13 I, 5, 6, 13 V, 15 III TMG, §§ 4e f., 28 IV, 33, 6a BDSG):

Art, Umfang, Zweck, Impressum, kommerzielles Angebot, Weitervermittlung, Profilbildung, Verfahrensverzeichnis, Werbung, Weiterübermittlung, autom. Einzelentscheidung

- Was fehlt: betrieblicher DSB, Betroffenenrechte
- Informationen bei Einwilligung (§ 4a BDSG, § 13 III TMG):

Stelle, Datenart, Zweck, Widerrufbarkeit

- Probleme:

Beschränkter Platz für Anzeige und Bedienung

Info per Privacy Policy / Nutzungsbedingungen (§§ 305 ff. BGB)

Gestaltung von Informationen u. Optionen

- Zwecks Transparenz und Wahlfreiheit (Layered Policy Design):
- Kurzhinweis, evtl. mit Icons
- Zusammengefasster Datenschutzhinweis
- Vollständiger Hinweis
- Evtl. Erläuterungen, Hintergründe und Quellen
- Situative Konfrontation
- Vgl. WP 100 Art. 29-Datenschutzgruppe vom 25.11.2004:
- http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_de.pdf

- Jederzeitige Abrufbarkeit und Änderbarkeit des Profils

Einwilligung

- Rechtsgrundlagen: § 4a BDSG, 13 II TMG, künftig Art. 7 EU-DSGVO
- Bestimmt/qualifiziert, explizit, freiwillig (Koppelungsverbot, Problem: Abhängigkeitsverhältnis), hervorgehoben, widerrufbar, protokolliert, elektronisch abrufbar
- Privacy by Default (Datensparsamkeit) besteht bisher nicht explizit, künftig § 23 EU-DSGVO
- Technisch voreingestellte Einwilligungen (Browser), dafür Standardisierung nötig (W3C), Erkennbarkeit d. Einstellung
- Zeitliche Befristung (wünschenswert)

Realisierung der Betroffenenrechte

Gelten auch für pseudonyme Datensätze

- Auskunftsanspruch (§ 34 BDSG; § 13 VII TMG)

Nicht nur Profildaten, auch Meta- und Verkehrsdaten

- Anspruch auf Datenkorrektur (§ 35 BDSG, § 13 IV 2. TMG)

> Reallöschung nach Abbruch der Verbindung/der Geschäftsbeziehung, evtl. Löschroutinen

Ausblick

- Mobile Computing ist Teil des Web-Computing (Verantwortlichkeit, anwendbares Recht)
- Zusammenführung der Telekommunikations-/-medien-regeln
- Aufgabe: Durchsetzung der Einwilligung bei Standortdaten, Abbau von Vollzugsdefiziten
- Regelungsbedarf: Privacy by Default, Standardisierung, Zertifizierung
- Bedarf an Technikgestaltung (wearable Devices, z. B. Brillen, Uhren; Fernsteuerung, z. B. Drohnen; Biometrie, NFC-Bezahlsysteme, ID-Management)

Mobile Computing- Sind die gesetzlichen Schutzregelungen im Telekommunikationsgesetz und im Bundesdatenschutzgesetz für die Nutzenden ausreichend?

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de