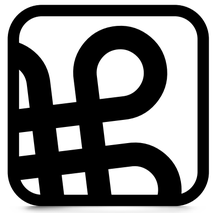


Macoun

Datenschutz und Apps

Thomas Biedorf
Konzerndatenschutz DB Mobility Logistics AG

Der langweiligste Vortrag auf der Macoun ever!
Aber: Er kann Leben retten!

Ablauf

- Worüber reden wir hier eigentlich?
- Datenschutz in Deutschland
- Welche personenbezogene Daten gibt es?
- Verantwortl. Stelle: Wer muss den Kopf hinhalten? Was muss sie tun?
- Technische und organisatorische Maßnahmen
- Vorgaben der Aufsichtsbehörden zu Apps/Web
- Bußgeldvorschriften

Worum geht es?

- Datenschutz schützt Menschen, keine IT (das wäre IT-Sicherheit)
- Das Recht auf „informationelle Selbstbestimmung“ ist ein Grundrecht
- Es ist das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen

Worum geht es?

- 2008 – Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
- Spezielle Ausprägung des allgemeinen Persönlichkeitsrechts
- Vom BVerfG als Grundrecht formuliert
- Erschwert u.a. den Einsatz des „Staatstrojaners“

Worum geht es?

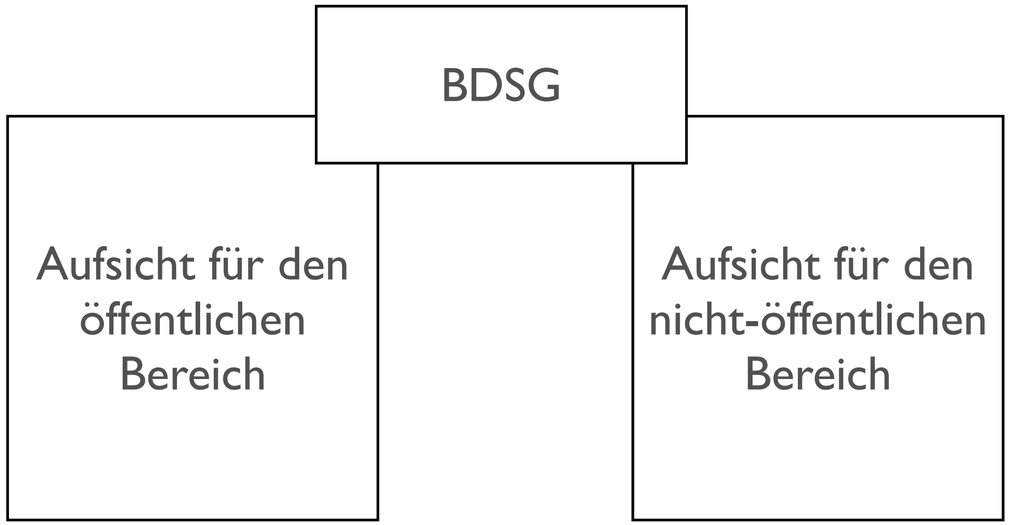
- Die maßgeblichen Gesetze hierzu sind das BDSG und das TMG
- Das BDSG genießt Subsidiarität
- Das BDSG ist ein Gesetz mit Erlaubnisvorbehalt

Datenschutz in Deutschland

- Getragen von zwei Säulen

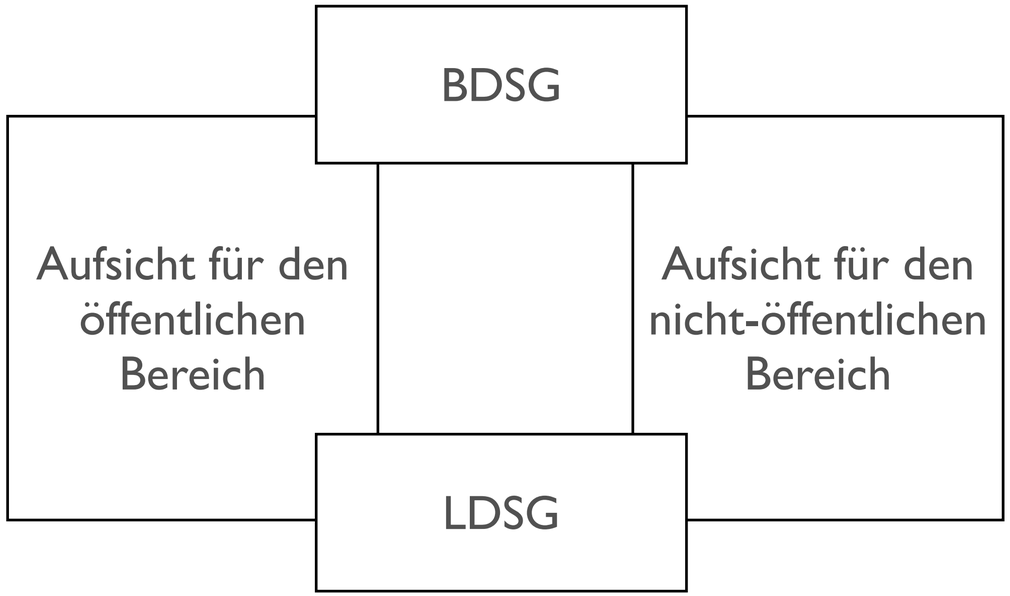
Datenschutz in Deutschland

- Oberstes Gesetz: BDSG



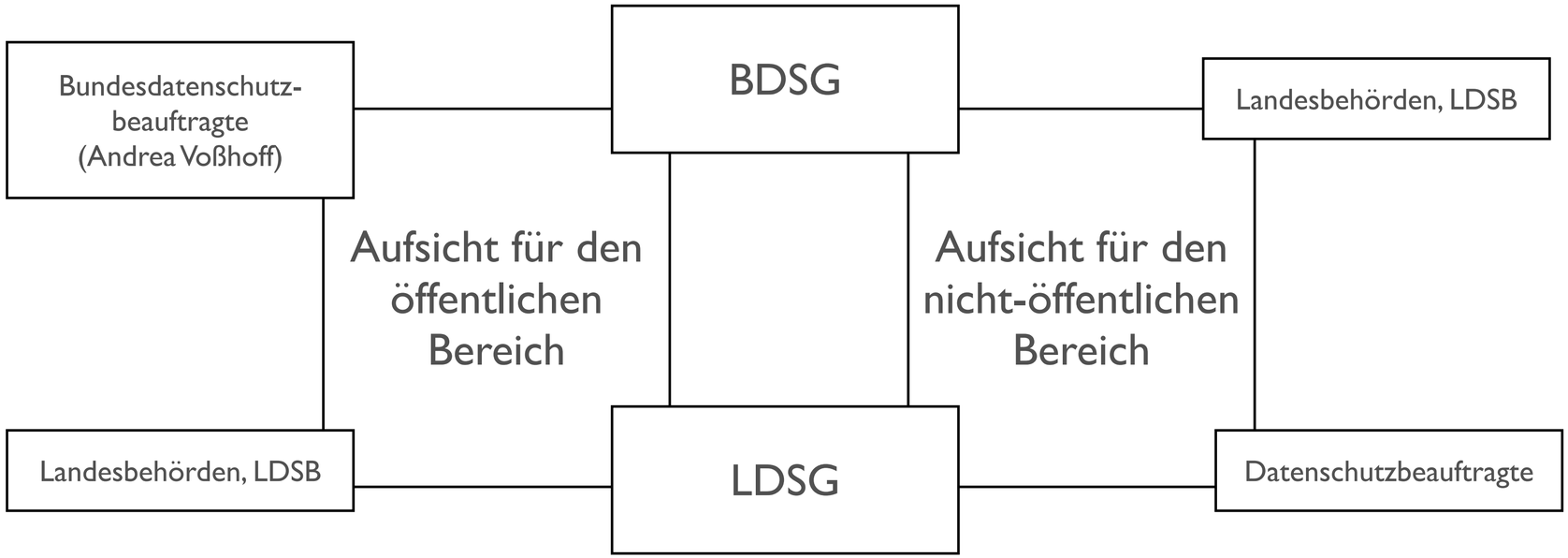
Datenschutz in Deutschland

- Landesdatenschutzgesetze



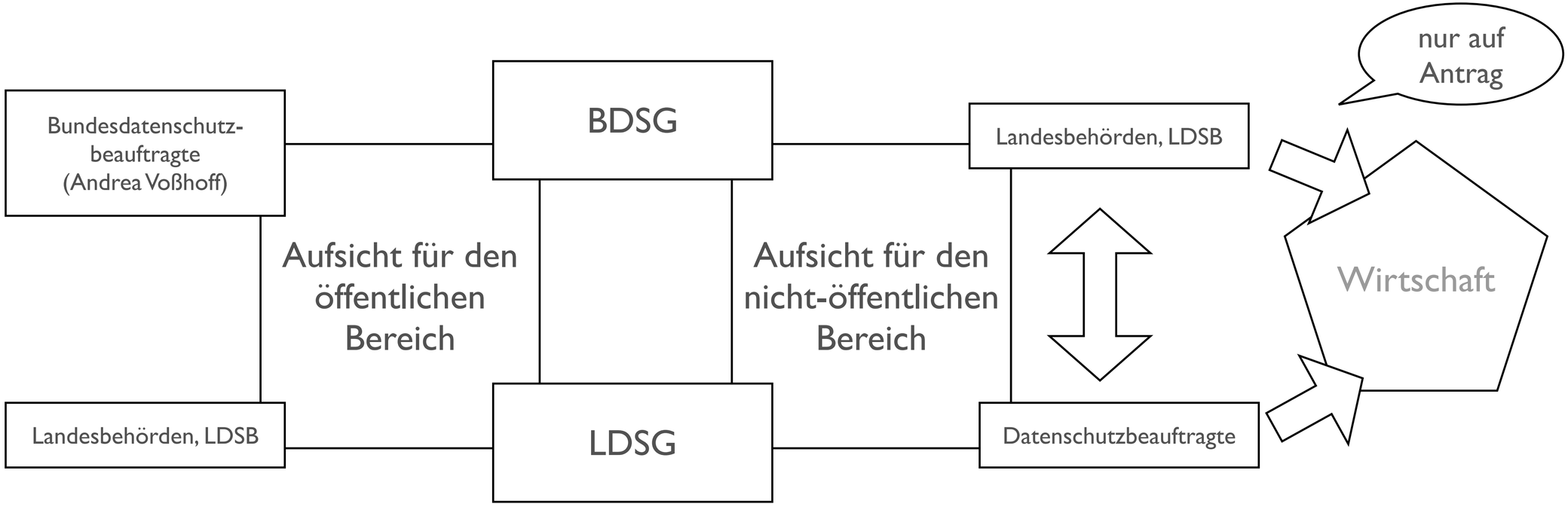
Datenschutz in Deutschland

- Bundes- und Landesbehörden



Datenschutz in Deutschland

- Wirtschaft: Freiwillige Selbstkontrolle durch DSBs



Welche Daten gibt es?

- Personenbezogene Daten sind Angaben zu persönlichen oder sachlichen Verhältnissen eines Betroffenen:
  - Name und Adressangaben (auch E-Mail und Telefon)
  - Bankverbindung, Kreditkartennummern
  - (...)

Welche Daten gibt es?

- Besondere personenbezogene Daten sind
  - Angaben über die rassische und ethnische Herkunft
  - politische Meinungen
  - religiöse oder philosophische Überzeugungen
  - Gewerkschaftszugehörigkeit
  - Gesundheit (HealthKit!) oder Sexualleben

Welche Daten gibt es?

- Besondere personenbezogene Daten
  - ... genießen allerhöchsten Schutz

Welche Daten gibt es?

- Im Beschäftigtenverhältnis gilt u.a. auch das Betriebsverfassungsgesetz
- Leistungskontrolle und Überwachung ist verboten

Daten sammeln, aber richtig!

- Erhebung nur beim Betroffenen
- Freiwilligkeit des Betroffenen vorausgesetzt
- Eine Rechtsvorschrift muss es erlauben

Verantwortliche Stelle

- Ist im BDSG verankert
- Ist immer der Auftraggeber
- Bei Eurer eigenen App seid Ihr die verantwortliche Stelle
- Die verantwortliche Stelle haftet für alle Verstöße

Verantwortliche Stelle

- Unterliegt der Meldepflicht (Verfahrensverzeichnis)
  - Name, Adresse, ggfs. Geschäftsführer der verantwortl. Stelle
  - Zweckbestimmung und Personengruppen
  - Empfänger der Daten und Regelfristen für Löschung
  - Drittstaatenübermittlung ja/nein
  - detaillierte Beschreibung des Verfahrens, techn. und organ. Maßnahmen

Verantwortliche Stelle

- Verfahrensverzeichnis
  - muss auf Antrag jedermann vorgelegt werden (außer letztem Punkt)
  - muss auf Antrag Behörden vorgelegt werden (inkl. letztem Punkt)

Technische und organisatorische Maßnahmen

- Sind einzuhalten!
- Die Anlage zum §9 BDSG regelt das
- 8 Punkte

Technische und organisatorische Maßnahmen

- Zutrittskontrolle

Technische und organisatorische Maßnahmen

- Zugangskontrolle

Technische und organisatorische Maßnahmen

- Zugriffskontrolle

Technische und organisatorische Maßnahmen

- Weitergabekontrolle

Technische und organisatorische Maßnahmen

- Eingabekontrolle

Technische und organisatorische Maßnahmen

- Auftragskontrolle

Technische und organisatorische Maßnahmen

- Verfügbarkeitskontrolle

Technische und organisatorische Maßnahmen

- Zweckbindung

Vorgaben der Aufsichtsbehörden zu Apps

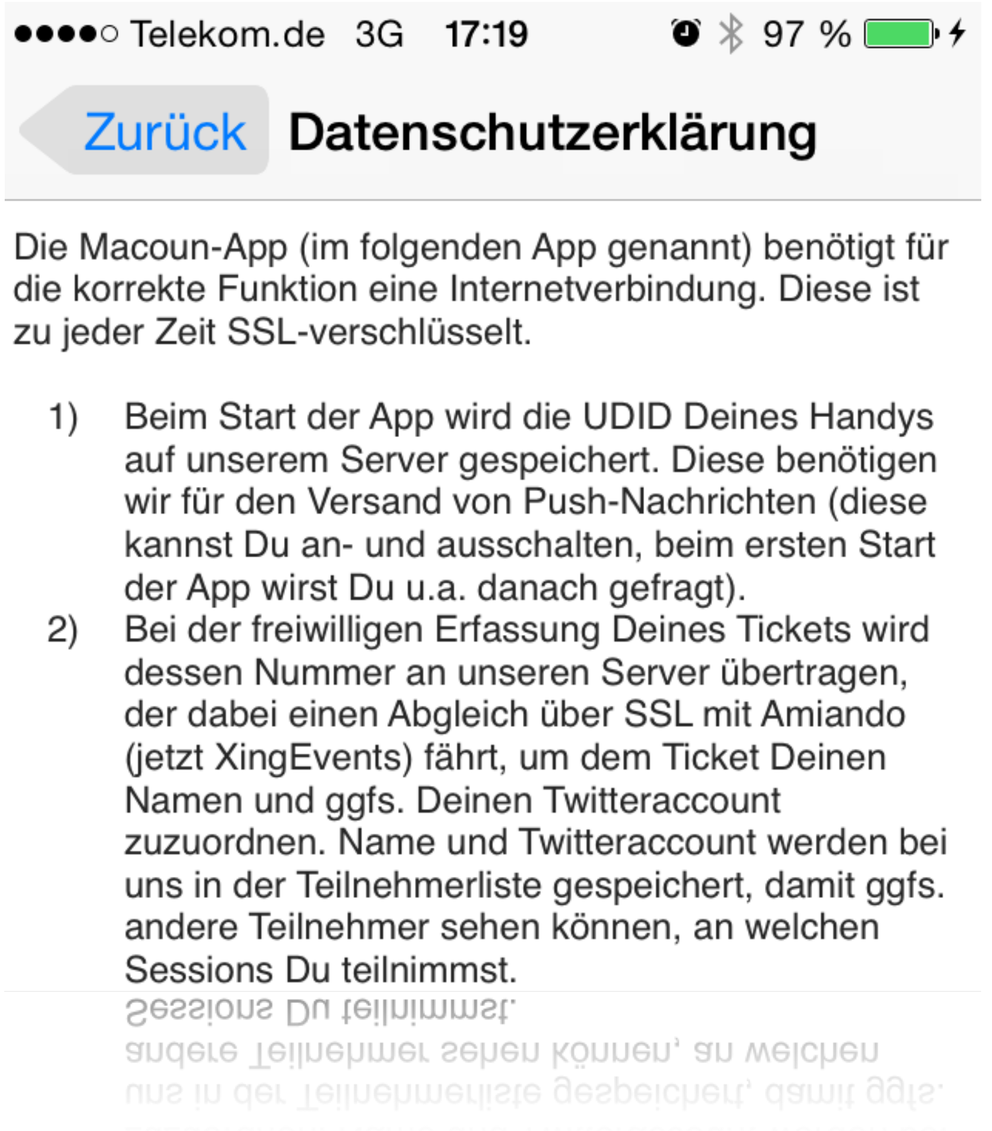
- Es gilt ein Personenbezug bei
  - Speichern der IP-Adresse
  - Geräte- und Kartenkennungen (IMEI, UDID etc.)
  - Name des Telefons
  - Standortdaten
  - Audio- (Stimmenaufzeichnung) und Filmaufnahmen
  - Biometrische Daten und Nutzungsdaten

Vorgaben der Aufsichtsbehörden zu Apps

- Datenschutzerklärung:
  - Der App-Anbieter hat den Nutzer „zu Beginn des Nutzungsvorgangs (…) in allgemein verständlicher Form zu unterrichten“, d.h. eigentlich schon im Appstore
  - Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein (UI?), Kontaktmöglichkeit muss gegeben sein
  - Lesbarkeit! Erklärung der App muss auf App angepasst sein, Webseitenerklärung langt nicht

Vorgaben der Aufsichtsbehörden zu Apps

- Datenschutzerklärung:
  - Es muss über Sinn und Zweck der Erhebung detailliert aufgeklärt werden
  - Stichwort: Transparenz



Vorgaben der Aufsichtsbehörden zu Apps

- IT-Sicherheit spielt zentrale Rolle, dabei das Einhalten der techn. und organisator. Maßnahmen

Vorgaben der Aufsichtsbehörden zu Apps

- Ausreichend sichere Passwörter
- ggfs. Zwei-Faktor-Authentifizierung (auf dem Handy?)
- Zugangsdaten möglichst nicht auf dem Gerät speichern
- Bei Speicherung (auch im Backend) geeignete kryptographische Verfahren verwenden
- Keine Gerätekennungen als Authentifizierungsmerkmal verwenden
- Passworteingabe maskieren

Vorgaben der Aufsichtsbehörden zu Apps

- Verschlüsselung mit SSL/TLS
- Nach Stand der Technik (normaler Schutzbedarf) mind.:
  - TLS1.2 mit RSA 2048-Bit und AES 128-Bit
- Perfect Forward Secrecy verwenden
- Backend-Server muss sauber konfiguriert sein

Vorgaben der Aufsichtsbehörden zu Apps

- Besonders schützenswerte Daten (Gesundheitsdaten, HealthKit!)
  - AES-256 Bit, RSA-16384 Bit (umsetzbar)
  - Löschung auf Flash-Speicher
  - 2-Faktor-Authentifizierung
  - SSL-Pinning
  - Auto Log-Out

Vorgaben der Aufsichtsbehörden zu Apps

- Datensparsamkeit : „Verwaschen“ der Koordinaten
  - App erfasst genaue Standortdaten
  - Nullung von Dezimalstellen führt zu Informationsverlust
  - Standortgenaue Daten häufig nicht notwendig
  - Lokale Logik kann standortgenaue Dienste mit verwaschenen Daten ermöglichen

Bußgeldvorschriften

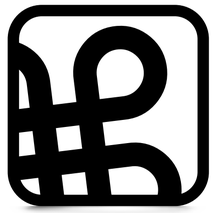
- Die Aufsichtsbehörde in Bayern hat eigenes forensisches Prüflabor
- Andere Behörden können das mitbenutzen
- Verstöße gegen Vorgaben werden mit Bußgeld geahndet
- Z. Zt. Prüfung fast aller Apps bayerischer Anbieter am Laufen

Bußgeldvorschriften

- Ordnungswidrigkeiten: bis zu EUR 50.000
- Strafbewehrte Verstöße: Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe
- Verfolgung aber nur auf Antrag

Fragen?

Vielen Dank!



Macoun