Datenschutz aus Sicht von Administratoren (Fortsetzung)

Warum darf ich pers. Daten speichern, Informationsklassifizierungen dieser Daten und Neuerungen seit September 2009

Hanno 'Rince' Wagner <sigint@rince.de>

Wer bin ich?

- Hanno 'Rince' Wagner, arbeite in Stuttgart
- Seit 3 Jahren Betrieblicher Datenschutzbeauftragter für einen Konzern mit Tochtergesellschaften
- Bin mit dem Thema seit >10 Jahren vertraut (CCC, Fitug et al.)
- Sensibilisiere Mitarbeiter (nicht nur in der IT) für Datenschutz

Inhalt des Vortrages

- Warum Datenschutz aus Sicht von Systemadministratoren?
- Informationsklassifizierung
- Technisch-Organisatorische Maßnahmen
- Novellierung des Bundesdatenschutzgesetzes

Warum Datenschutz aus Sicht Systemadministratoren?

Warum mein Vortrag gerade für Administratoren?

- Wir haben viel mit Rohdaten zu tun – den Anwendern ist oft nicht bewusst was für Daten sich ansammeln.
- Projekte kommen früher oder später zu uns, um Daten einzupflegen – durch unseren “Rundblick” wissen wir um den Kontext der Daten
- Wir müssen mitdenken – auch im Zweifelsfall unbequeme Fragen stellen; gerade wenn die Daten für mehrere Firmen sind oder diese durchlaufen (Auftragsdatenverarbeitung)

Warum mein Vortrag gerade für Administratoren? (2)

- Auch andere Menschen sind faul – sie vergessen oft dass sie als **Daten-Verantwortlicher** sich um den Datenschutz Gedanken machen müssen
- Wir sind diejenigen die auch an Löschen und Sichern / Archivieren von Daten denken (müssen) – um Platz zu sparen, aber auch um neugierige Fragen und Ideen gleich wieder wegfallen lassen zu können (Zweckbindung)

Quintessenz

Wir sollten wissen was wir dürfen

(und was wir tun müssen!)

Informationsklassifizierung

Erlaubnisvorbehalt

Das Speichern von personenbezogenen Daten ist rechtlich verboten, es gibt von dieser Regel nur Ausnahmen:

- **Gesetzliche Vorgaben** (Sozialgesetzbuch et al.)
- **Vertragsverhältnis** (Mitarbeiter, Verkauf und Versand von Waren)
- **Öffentliche Quellen** (Telefonbuch)
- **Abwägung** (Mein Interesse als Datensammler vs. Schutzinteresse des Betroffenen)
- **Einwilligung** (freiwillig, keine Nachteile durch nicht-Einwilligung erlaubt, kann jederzeit zurückgezogen werden, muss deutlich hervorgehoben werden)

Informationsklassifizierung

Um zu beurteilen wie wichtig Daten sind – nicht nur aus Sicht des Datenbesitzers sondern auch aus der des Betroffenen – muß man die Daten bewerten.

Dafür habe ich versucht zwei Definitionen für die Daten zu benutzen:

- Einerseits die gesetzliche Definition (BDSG)
- Andererseits den Wert der Daten im Kontext der sonstigen Daten im Verbindung mit der Begründung zur Sammlung

Arten von personenbezogenen Daten (gesetzlich)

Das ist einfach, da hier das BDSG die Definitionen vorgibt

- **Einfache Daten**: Name, Vorname, Geburtstag,Familienstand, aber auch Bankdaten
- **Persönlichkeitsdaten**: Einkommensverhältnis, Familienverhältnis, Lebensstil, Einkaufsverhalten
- **Sensible Daten**: Herkunft (Rasse), politische Meinung, Religion, medizinische Daten

Informationsklassifizierung im Kontext

- Hat der Gesetzgeber noch nicht erkannt, wohl aber das BverfG
- Daten müssen im Kontext angesehen werden; erst dann wird der “Wert” der Daten erkannt
- Hier der Ansatz einer Klassifizierung

Informationsklassifizierung 1

- **Unkritische Daten:** Die Speicherung der Daten ist unkritisch, weil es hierfür eine zwingende Grundlage gibt (gesetzliche Grundlage oder Vertragsverhältnis)
- **Für ordnungsgemäßen Betrieb notwendige Daten (betriebliche Daten):** Die Speicherung der Daten ist nicht aus gesetzlichen, sondern aus *betrieblichen* Gründen notwendig. Sie sind zwar personenbezogen aber „nur“ für betriebliche Zwecke nutzbar (Administrations-Logins auf Produktivsystemen für Revision).

Informationsklassifizierung 2

- **Abwägung:** Bei der Speicherung dieser Daten muss der Verantwortliche abwägen, ob das Datenschutzinteresse des Betroffenen oder das Interesse des Datensammlers der Speicherung der Daten überwiegt, es gibt kein Gesetz oder Verordnung (IP-Adressen der Firmenrechner im Proxy-Server, Archivierung von Mails)
- **Kritische Daten:** Die Speicherung dieser Art von Daten ist aus gesetzlicher Sicht nicht so ohne weiteres möglich, oft ist eine Einwilligung notwendig. Dort muss eine sehr gute Begründung vorhanden sein aufgrund derer eine Speicherung erfolgen soll (Gesprächsaufzeichnungen, Einzelverbindungsnachweise...)

Was können wir tun?

Wir wissen also jetzt um den “Wert” der Daten an sich. Wir wissen auch (vom vorigen Vortrag) dass Daten nur gesammelt werden dürfen für einen vorher bestimmten Zweck. Dieser muß vorher schriftlich festgehalten werden (Verfahrensliste). Weitere Nutzung der Daten ist nicht erlaubt.

Generell gilt der Satz:

Datensparsamkeit ist wichtiger denn je

- Möglichst wenig Daten sammeln
- Begründung für das Sammeln der Daten
- Prüfung ob Daten pseudonym oder anonym erhoben oder verarbeitet werden können
- Löschen von Daten die nicht gebraucht werden

Technisch/Organisatorische Maßnahmen

- §9 BDSG sieht Technisch-Organisatorische Maßnahmen zum Schutz der personenbezogenen Daten vor.
- Im Anhang zum BDSG gibt es einen Maßnahmenkatalog der als Mindestschutz anzusehen ist

Die Mindestanforderungen

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Chinese-Wall-System

Wofür diese Maßnahmen?

- Diese Maßnahmen sind Grundvoraussetzungen
- Erst wenn diese definiert und umgesetzt sind dürfen personenbezogene Daten erhoben oder verarbeitet werden
- Sie gelten als Richtschnur für die Verfahren die mit personenbezogenen Daten zu tun haben (Verfahrenslisten)

Und was dürfen Administratoren?

- Administratoren dürfen (natürlich) in die Daten reinschauen sofern der Zugriff für ihre Arbeit notwendig ist
- Administratoren dürfen aber nicht für Fachbereiche Abfragen oder Statistiken erstellen
- Die Zweckbindung der Daten gilt weiterhin
- Oracle zum Beispiel bietet speziellen Administratorenzugriff an.

Die Novellierung des Bundesdatenschutzgesetzes

Neuigkeiten durch die letzten Novellierungen

In der letzten Legislaturperiode wurden einige Änderungen bzw. Erweiterungen des Bundesdatenschutzgesetzes beschlossen, die seit 1.9.2009 nach und nach umgesetzt werden müssen.

Ich habe hier nur einige – nicht alle – Neuerungen hier aufgeführt. Würde ich alles hier aufführen würde es den Rahmen sprengen; auch meines juristischen Wisses.

Neue Definition für Beschäftigte

Beschäftigte werden im BDSG extra definiert da es für sie eine spezielle Regelung zur Erhebung von Daten gibt – für ELENA.

Neuer Status für Datenschutzbeauftragte

Der betriebliche Datenschutzbeauftragte ist in seiner Aufgabe nicht nur weisungsfrei sondern geniesst ähnliche Privilegien wie ein Betriebsrat – er hat einen Kündigungsschutz und die Aufgabe kann ihm auch nicht einfach entzogen werden

Pseudonymisierung wurde forciert

- Möglichkeit / Nutzen von Pseudonymisierung und Anonymisierung wurde verstärkt (… ist zu ano/pseudonymisieren).
- Damit wird gesetzlich mehr Druck gemacht, Daten so schnell wie möglich von der sensiblen Merkmalen zu befreien.

Rechte der Betroffenen werden verstärkt

Der Betroffene hat das Recht die erhebende Stelle nach den gespeicherten Daten zu fragen und sie muß antworten – er darf nach der Art der Daten und dem Empfänger der Daten fragen; auch wenn diese Daten nicht gespeichert sind (Übergangsregelung) muß diese Auskunft erteilt werden.

Auftragsdatenverarbeitung und Verträge

- Bei Auftragsdatenverarbeitung muß bereits vor dem Erheben oder Verarbeiten der Daten im Auftrag vertraglich festgehalten werden, welche Daten genau zu welchem Zwecke verarbeitet werden dürfen; dies muss (im Gegensatz zu vorher) genau festgelegt werden; besonders die Dauer des Auftrags und die TOMs welche gelten.
- Der Datenschutzbeauftragte des Auftraggebers hat die Pflicht den Auftragnehmer und dessen Maßnahmen regelmäßig zu überprüfen

Daten für Marketingzwecke

- Daten für Werbe/Marketingzwecke werden im Gesetz näher definiert; es gibt einen Unterschied zwischen Marketingszweck und Forschungs-zweck
- Herkunft der Daten muss angegeben werden / verifizierbar sein
- Der Betroffene musste vorher schon darüber informiert werden wer diese Daten über ihn speichert (§4) – nun muss die Stelle auch die Herkunft nennen

Daten für Marketingzwecke 2

- Rechte des Betroffenen: Nicht nur Herkunft, sondern auch Zweck und Empfänger der Daten kennen
- Bei Übermittlung der Daten an Dritte muss die Stelle 2 Jahre lang die Herkunft der Daten und den Empfänger speichern um Auskunft geben zu können.
- Bei Zusammenfassung von Daten muss die erhebende Stelle klar erkennbar sein (zum Beispiel auf Werbe-Postkarten)

Scoring

Scoring selbst arbeitet auch mit personenbezogenen Daten; diese werden allerdings mit Hilfe von Algorithmen mit Schätzwerten“angereichert” die einen Mittelwert über verschiedene personen-übergreifende Daten bilden sollen.

Auch die Wahrscheinlichkeitswerte die für den Betroffenen zutreffen (der letzten 6 Monate) müssen gespeichert und auf Anforderung herausgegeben werden. Geschätzte Daten sind als solche zu kennzeichnen

Scoring 2

- Dem Betroffenen müssen die Bedeutung der Wahrscheinlichkeitswerte erklärt werden
- Die genutzten Datenarten für die Berechnung müssen angegeben werden
- Löschung von Daten nach Vertragsende
- Oder spätestens nach 3 Jahren

Bei Datenschutzproblemen

- Bei Datenschutzproblemen muss die Aufsichtsbehörde sofort informiert werden.
- Die Betroffenen(!) sollen informiert werden, sobald geeignete Schutzmaßnahmen getroffen wurden (sehr schön bei Einbruch in Webseiten)

Ordnungswidrigkeiten

Datenschutzprobleme sind weiterhin „nur“ eine Ordnungswidrigkeit, allerdings wird es schärfer gehandhabt als bisher.

Ordungswidrig ist bereits:

Ordnungswidrigkeiten 2

- eine nicht-mögliche Überprüfung einer Datenübermitlung
- bei einer Auftragsdatenverarbeitung der nicht vollständig formulierte Auftrag
- Wenn einem Auskunftsverlangen nicht richtig entsprochen wird
- Wenn bei einer Einwilligungserklärung der Abschluß eines Vertrags davon abhängig gemacht wird
- Eine Mitteilung an die Datenschutzbehörde oder die Betroffenen nicht rechtzeitig gemacht wird.

Bußgelder

Die Bußgeldmöglichkeiten wurden zur bisherigen Regelung verdoppelt;

- bis zu 50.000€ bei „einfachen“ Ordnungswidrigkeiten bzw.
- Bis zu 300.000€ bei schwereren Ordnungswidrigkeiten möglich

Bußgelder 2

- Einfach: “Unsauberkeiten” wie kein korrekter Auftrag, keine Revisionsmöglichkeit im Nachhinein (noch kein Schaden, aber Schaden möglich)
- Schwer: zum Beispiel keine oder unvollständige Mitteilung (Schaden bereits passiert da Daten unbefugt verarbeitet wurden)

Fragen?

- Wenn es Fragen gibt, bitte stellen!

- Ansonsten stehe ich gerne zur Verfügung unter <sigint@rince.de>

Viel Spass auf der SigInt 2010!!

Vielen Dank für die Aufmerksamkeit

- Dieser Vortrag wird unter der Creative Commons License veröffentlicht: