

# Neues vom Datenschutz

8. Juli 2010

Sirin Torun, SerNet GmbH

## SerNet GmbH

- gegründet 1997
- Büros in Göttingen, Berlin, Nürnberg, Sunnyvale
- Informationssicherheit und Datenschutz
- spezialisiert auf Open Source Software
- Samba: Storage-Lösungen and Private Clouds
- Netzwerksicherheit für Industrie und öffentl. Hand
- Zertifizierungen und Audits
- IT-Grundschatz und ISO 27001
- „Old Economy“, kein Risiko-Kapital, keine Bank-Kredite  
über 700 Bestandskunden in DE, EU, US

## Dienstleistungen der SerNet

- Beratung zu Informationssicherheit, IT-Grundschutz, ISO 2700x, Risikomanagement, Datenschutz
- Schulungen zu IT-Grundschutz und verinice.
- Anpassung von verinice auf Kundenwunsch
- Auditierungen und Zertifizierungen
- Bereitstellung: Externe Datenschutzbeauftragte  
Coaching: Interne Datenschutzbeauftragte
- technische Analysen, Penetration-Tests
- Implementierung von Firewall- und VPN-Infrastrukturen

## Gliederung

- **Datenschutz, was ist das?**
- **Kurzübersicht über die Änderungen Novelle 1 -3**
- **Highlights der Novelle:**
  - Auftragsdatenverarbeitung
  - Kundendatenschutz
  - Informationspflichten
- **Bußgelder und Haftungsrisiken**
- **Was ist zu tun ?**

## Datenschutz

- Informationelles Selbstbestimmungsrecht, Art. 2 Abs. 1 GG i.v.m. Art. 1 Abs. 1 GG
- BDSG regelt den Umgang mit personenbezogenen (pb) Daten
- § 3 I BDSG:
  - *„Personenbezogene Daten sind Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.“*

# Änderungen im Überblick

## **BDSG-Novellen 1-3**

- Kündigungsschutz für internen Datenschutzbeauftragten
- Auftragsdatenverarbeitung, § 11 BDSG
- Kundendatenschutz, § 28 ff BDSG
- Auskunftsteien und Scoring, §§ 28 a, b
- Arbeitnehmerdatenschutz, § 32 BDSG
- Auskunftsrechte, § 34 BDSG
- Meldepflicht bei Datenschutzverstößen
- Aufsichtsbehörden
- Neue Bußgeldvorschriften

# Auftragsdatenverarbeitung

## Auftragsdatenverarbeitung im BDSG

- ADV (+), wenn pb Daten im Auftrag durch externe Stelle erhoben, verarbeitet oder genutzt werden
- AG bleibt Herr der Daten
- AN  $\neq$  Dritter (Privilegierungseffekt)

## Auftragsdatenverarbeitung

### Änderungen im Rahmen der Reform

- § 11 II BDSG
  - Sorgfältige Auswahl des Auftragnehmers
  - Schriftlicher Vertrag
- 10-Punkte Katalog
  - Gegenstand und Dauer des Auftrages
  - Technische und organisatorischen Maßnahmen
  - Unterauftragsverhältnisse
  - Kontrollrechte des AG
  - Mitteilungspflichten bei Verstößen

# Auftragsdatenverarbeitung

## Änderungen im Rahmen der Reform

- Kontroll- und Dokumentationspflichten des AG, § 11 II S.4, 5

*(2) .....Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.*

## Auftragsdatenverarbeitung

### Änderungen im Rahmen der Reform

- Kontrollpflicht
  - Erstkontrolle (Bereits vor Beginn der Datenverarbeitung)
  - Laufende Kontrollen (Prüfintervalle)
  - Persönliche Kontrolle (nicht zwingend)
  - Vor-Ort-Kontrolle (nicht zwingend)
  - Selbstauskunft des AN
  - Sachverständigen Testat

## Auftragsdatenverarbeitung

### Änderungen im Rahmen der Reform

- Dokumentationspflicht
  - Angaben zu den Beteiligten
  - Angaben zu der Kontrolle
  - Art und Umfang der Kontrolle
  - Feststellungen
  - Weitere Maßnahmen

# Auftragsdatenverarbeitung

## Änderungen im Rahmen der Reform

- Rechtsfolge bei Verstößen
  - Bußgeldbewehrte Ordnungswidrigkeit, § 43 I Nr. 2b BDSG
    - *Verstoß gegen § 11 II S.2 BDSG*
    - *Verstoß gegen § 11 II S.4 BDSG*
  - Geldbuße bis zu 50.000 Euro; zusätzlich sog. Gewinnabschöpfung möglich.
  - Problem:
    - Wegfall der Privilegierung?
    - Wie sind Altverträge zu behandeln?

## Auftragsdatenverarbeitung

### Maßnahmen für die Praxis

- Auswahl der AN anhand der TOM (Checkliste erstellen)
- 10-Punkte Katalog als verbindliche Checkliste bei Vertragsgestaltung beachten
- Umstellung bestehender Vertragsmuster
- Altverträge anpassen
- Detailregelungen zu Prüfintervallen und Auditrechten
- Implementierung eines Kontroll- und Dokumentationsverfahrens

## Kundendatenschutz

### Änderungen im Rahmen der Reform

- Grundregel : Opt-In-Prinzip
- Ausnahmen: Verwendung ohne Einwilligung nach § 28 III BDSG
- Erhalt des Listendatenprivilegs, § 28 III S.2 BDSG
  - Berufs- , Branchen- und Geschäftsbezeichnung
  - Name, Titel, akademischer Grad, Anschrift, Geburtsjahr
  - Zugehörigkeit zu einer Personengruppe
- Widerspruchsrecht, § 28 IV BDSG
  - Bei Begründung des Schuldverhältnisses
  - Bei jeder werblichen Ansprache
  - Keine strengere Form als Schuldverhältnis

## Kundendatenschutz

### Änderungen im Rahmen der Reform

- Bewerbung eigener Angebote, § 28 III S.2 Nr.1 BDSG
  - Bestandskunden
  - Rechtsgeschäftsähnliches Schuldverhältnis
  - Hinzuspeicherung weiterer Daten erlaubt

## Kundendatenschutz

### Änderungen im Rahmen der Reform

- Öffentliches Verzeichnisse, § 28 III S.2 Nr.1 BDSG
  - Eigene Angebote
  - Daten erhoben aus allgemein zugänglichen
    - Adress-,
    - Rufnummern-,
    - Branchen- oder
    - Vergleichbaren Verzeichnissen
  - Hinzuspeicherung weiterer Daten erlaubt

# Kundendatenschutz

## Änderungen im Rahmen der Reform

- B2B-Werbung, § 28 III S.2 Nr.2 BDSG
  - Nur unter beruflicher Anschrift
  - Name und Ansprechpartner dürfen verwendet werden
  - Keine Hinzuspeicherung weiterer Daten zum Ansprechpartner
  - Hinzuspeicherung weiterer Daten zum Unternehmen erlaubt, sofern es keine personenbezogene Daten sind
- Spendenwerbung, § 28 III S.2 Nr.3 BDSG
  - Gemeinnützige Organisationen
  - Parteien
  - Spendenwerbung
  - Keine Hinzuspeicherung weiterer Daten

# Kundendatenschutz

## Änderungen im Rahmen der Reform

- Werbung für fremde Angebote, § 28 III S.2 Nr.5 BDSG
  - Verantwortliche Stelle muss in jeder Werbeaussendung eindeutig erkennbar sein

*„Wir empfehlen Ihnen die Produkte im beiliegenden Prospekt der Firma Muster“*

*Absender: Firma X*

# Kundendatenschutz

## Änderungen im Rahmen der Reform

- Datenübermittlung an Dritte für Werbezwecke, § 28 III S.2 Nr.4 BDSG
  - Listendaten
  - Ersterhebende Stelle muss in der Werbung eindeutig benannt sein.
  - Dokumentation der Datenliefer- und -empfangskette für 2 Jahre, § 34 I a BDSG
  - Mit den Listendaten dürfen keine weiteren Daten übermittelt werden.
  - Keine Erleichterung für Datenaustausch innerhalb Konzernen

## Kundendatenschutz

### Änderungen im Rahmen der Reform

- **Einwilligung, § 28 III a, b BDSG**
  - Einwilligung in Schriftform, § 4 a BDSG
  - Schriftliche Bestätigung mündlicher Einwilligungen
  - Elektronische Einwilligung
  - Protokollierung elektronischer Einwilligung
  - Jederzeitige Zugriffsmöglichkeit des Betroffenen
  - Drucktechnische deutliche Gestaltung
  - Kopplungsverbot marktbeherrschender Unternehmen

# Kundendatenschutz

## Änderungen im Rahmen der Reform

- Sanktionen nach dem BDSG
  - bis zu 50.000 EUR. Für formale Verstöße
    - *Verstoß gegen die Unterrichtungspflichten, Dokumentationspflichten, § 43 I Nr. 3*
  - bis zu 300.000 EUR für materielle Verstöße
    - Übermittlung oder Nutzung nach erteiltem Widerspruch, § 43 II Nr. 5b BDSG
  - Erhöhung des Bußgeldrahmens um Verletzergewinne

## Kundendatenschutz

### Maßnahmen für die Praxis

- Beachtung der Übergangsfrist 31.08.2012
- Trennung von Alt- und Neudatenbeständen
- Keine Mischung von eigenen und fremden Daten
- Separate Einholung der Opt-Ins für die verschiedenen Ansprachkanäle (E-Mail, Telefon)
- Dokumentation in der Datenbank für welchen Kanal Einwilligungserklärung vorliegt
- Anpassung der AGBs, Vertrags- und Angebotsvordrucke
- Hinweis auf Widerrufsrecht ist bei jeder werblichen Ansprache zu wiederholen
- Ausreichende Haftungs- und Freistellungsregelungen

# Informationspflichten

## Änderungen im Rahmen der Reform

- Informationspflicht bei Datenpannen, § 42 a BDSG
  - Unrechtmäßige Übermittlung oder Kenntnisnahme pb Daten
    - Bank- oder Kreditkartendaten
    - Daten , die Berufsgeheimnis unterliegen
    - Daten über strafbare Handlungen oder Ordnungswidrigkeiten
    - Diensteanbieter: Bestands-, Verkehrs- oder Nutzungsdaten
    - Sonstige, besonders sensible Daten , § 3 IX BDSG
  - Verpflichtung zur Benachrichtigung
    - Aufsichtsbehörde und Betroffene
    - Bei Vielzahl von Betroffenen Anzeige in Tageszeitungen
- Geldbuße bis zu 300.000 EUR, § 43 II Nr.7 BDSG

## Informationspflicht

### Maßnahmen für die Praxis

- Organisatorische Maßnahmen
  - Spezielle Datenkategorien im Unternehmen
  - Festlegung der Verantwortlichkeiten
  - Meldeweg für Datenpannen
  - Dokumentation der Informationspflicht
  - Verfahrensanweisung für Mitarbeiter
- Technische Maßnahmen
  - Monitoring des Datenverkehrs mit Warnung bei Anomalien
  - Warnsystem für unerlaubte Zugriffe auf Dateisysteme
  - Regelmäßige Kontrolle der Konfiguration des Webserver und anderer zentraler Server

## **Bußgelder, § 43 BDSG**

### **Geldbuße bis 50.000 EUR, § 43 I BDSG u.a. für :**

- Keine Kontrolle bei Auftragsdaten
- Verstoß gegen Anordnung der Aufsichtsbehörde
- Verstoß gegen Auskunftsverpflichtung
- Kein Datenschutzbeauftragter

### **Geldbuße bis 300.000 EUR, § 43 II BDSG u.a. für:**

- Unbefugte Datenverarbeitung
- Zusammenführung von Daten
- Zweckentfremdung von Daten
- Missachtung des Kopplungsverbotes

## Was ist zu tun?

- Verarbeiten Sie Ihre Daten gesetzeskonform
- Datengeheimnis
- Datenschutzbeauftragter
- Überprüfung der Verträge
- Überwachen und dokumentieren Sie Ihre Auftragsverhältnisse
- Kundendatenbanken strukturieren und bereinigen
- Dokumentation
- Notfallplan für Datenpannen
- Arbeitnehmerdatenschutz beachten

## Kontakt

### SerNet – Service Network GmbH

Bahnhofsallee 1b  
37081 Göttingen

Tel: +49 -551-370000-0

Fax: +49 -551-370000-9

Schützenstr.18

10117 Berlin

Tel: +49 -30-5779779-0

Fax: +49 -30-5779779-9

[datenschutz@sernet.de](mailto:datenschutz@sernet.de)

<http://www.SerNet.DE>