

Wertewandel des Datenschutzes

Internationaler Datenschutz als globale Herausforderung

Dr. Kerstin A. Zscherpe
Rechtsanwältin, Licenciée en Droit



Tutoring, 27. September 2008

Internationaler Datenschutz – was ist das?

Idealvorstellung:

Weltweit einheitliche Regeln zum Schutz personenbezogener
Daten vor unzulässiger Erhebung und Verwendung sowie
Missbrauch (einschließlich Identitätsdiebstahl)



Realität:

„Zerklüftete“ Rechtslandschaft, keine einheitlichen Regeln
(betrifft nicht nur Datenschutz sondern auch Datensicherheit,
trotz z.B. Regelungen von BASEL II oder SOX)

Gibt es Regeln zum internationalen Datenschutz?

- Keine umfassenden völkerrechtlichen Verträge zum Datenschutz (insbesondere WTO)
- Auch keine einheitliche Regelung in (Nord-)Amerika
- Weltweit stark unterschiedliches Konzept vom Datenschutz
 - Europa: Persönlichkeitsschutz (⇒ Menschenrechte)
 - USA: geringer Schutz, v.a. „no privacy in the workplace“
 - Dubai, Katar, Singapur u.a. kennen gar kein Datenschutzrecht!
- Andererseits: ähnliche Regelungen in Teilbereichen vorhanden, z.B. Schutz vor Spam, Gesundheitsdatenschutz
- „Einheitlicher“ Europäischer Datenschutz (EU/EWR, Schweiz)
 - Richtlinie 1995/46/EC
 - Richtlinie 2002/58/EC (v.a. E-Mail-Marketing)

3

Wertewandel im internationalen Datenschutz

- Europa als „Vorreiter“ beim Datenschutz (ab 1995)
- Einfluss des europäischen Konzepts auf andere Länder
 - Länder der europäischen Wirtschaftsraumes
 - „White List“, z.B. Schweiz, Argentinien, Kanada
 - Weitere, z.B. Australien, asiatische Länder
- USA
 - Lange zögerlich, wegen befürchteter Wettbewerbsverluste
 - Entwicklung beschleunigt wg. Spam und Gesundheitsdatenschutz
 - „Safe Harbor“ als Reaktion auf EU-Regelungen
 - Aber: wieder Einschränkungen und Zunahme der Überwachungen (auch von Ausländern) unter dem Aspekten der „Terrorbekämpfung“
- Problem auch: gespaltene öffentliche Wahrnehmung

4

Konsequenzen der „zerklüfteten“ Rechtslandschaft

- Zu beachtende Vorgaben relativ unübersichtlich
 - Hoher Aufwand zur Feststellung des geltenden Rechtsrahmens
 - Verbleibende Restunsicherheit bzgl. Interpretation der Vorgaben
- Global agierende Unternehmen haben Probleme bei der Implementierung einheitlicher Datenschutz-Verfahren
 - ⇒ Datenschutz-„Dilemma“
 - Bemühen um Einhalten der Vorgaben („weißes Schaf“) ODER
 - (Weitgehendes) Ignorieren der Vorgaben („schwarzes Schaf“)?
- Übeltäter machen sich unterschiedliches Schutzniveau in den verschiedenen Ländern zu Nutze („Forum-Shopping“)
 - Internetplattformen / Spam / Phishing
 - Adresshändler
 - Und weitere...

5

Derzeitige Herausforderungen für Unternehmen (1/2)

- Internationale Datentransfers
 - Zentralisierung von Datenverarbeitungsvorgängen
 - Outsourcing (Nearshore/Offshore)
 - Rückübertragungen von Daten (Insourcing)
 - Auftragsdatenverarbeitung
- Arbeitnehmerdatenschutz
 - Background Checks
 - Aufbewahrung von Bewerberdaten
 - Überwachung („Monitoring“)
 - Whistleblowing

6

Derzeitige Herausforderungen für Unternehmen (2/2)

- Marketing / CRM
 - Datenbeschaffung und Adresshändler
 - Spamverbot und Zulässigkeit von E-Mail-Werbung
- Daten-Archivierung und E-Discovery
 - Gesetzliche Vorgaben (Handels-/Bilanzrecht, Steuerrecht)
 - E-Discovery (bald auch in Europa?)
- Internet-Datenschutz
 - „Ausrichtung“ auf den Markt
 - Cookies / Data Mining

7

Lösungsansätze der Unternehmen

- Einheitliche Lösung („One-Solution-Fits-All“)
 - Orientiert an einem mittleren bis hohen Standard
 - „Übertriebener“ Datenschutz für Länder mit niedrigem Standard
 - Lücken in Ländern mit höherem Standard
- Basislösung mit länderspezifischen Spezialregelungen
 - Minimum-Lösung, orientiert an niedrigem oder mittlerem Standard
 - Erheblicher Aufwand zur Adressierung der länderspezifischen Regelungen
- „Best Practices“
 - Wirtschaftlich orientierte Kompromisslösung (mittlerer Standard)
 - Identifikation internationaler Gebräuche und Regeln („Practices“)
 - Compliance-Lücken werden in Kauf genommen

8

Die (traurige) Datenschutz-Realität

- Einschränkung des Datenschutzes durch staatliche Stellen
 - Vorratsdatenspeicherung (EU und Thailand)
 - Austausch von Daten von Straftätern (EU und EU-USA)
- Einschränkung des Datenschutzes durch Unternehmen
 - Datenpannen, z.B. MasterCard, Monster, HSBC, engl. Behörden
 - Beobachten von Mitarbeitern, z.B. Telekom, Lidl etc.
- Lebhafter Datenhandel
 - Direktmarketing / Mailing-Aktionen
 - Sehr einfacher Dateneinkauf (Testreihe der Verbraucherschützer)
- Internet
 - Datenkrake Google
 - Soziale Netzwerke nicht sicher

9

Praktische Konsequenzen der Unternehmen

- Weniger „weiße Schafe“, mehr „schwarze Schafe“
 - Bemühen um Einhalten der gesetzlichen Vorgaben rückläufig
 - Stattdessen: Risikoabschätzung und -minimierung
- Wenn Compliance, dann nur „Best Practices“
 - Orientiert sich am Herkunftsland (häufig USA)
 - Lücken beim Einhalten der gesetzlichen Vorgaben
- Paradox: Markt von IT-Sicherheitsprodukten und entsprechenden Dienstleistungen im stetigen Wachstum

10

Fazit: Die globale Herausforderung

- Es besteht Handlungsbedarf
 - Einheitliche Regelungen zur Sicherstellung eines Mindestniveaus
 - Einheitliche Sanktionen und Rechtsweggarantie bei Verstößen
- Geeigneter internationaler „Gesetzgeber“?
 - Völkerrechtlicher Vertrag über UNO, WTO, andere Organisation?
- Vorteile
 - Rechtssicherheit für Betroffenen und Unternehmen
 - Abbau von Handelshemmnissen
 - Kein „Forum-Shopping“ mehr möglich
- Nachteile
 - Realisierbarkeit?
 - Unterschiedliche Umsetzung in den einzelnen Ländern
 - Eingeschränkter Wettbewerb

11

Danke für Ihre Aufmerksamkeit.

Wenn noch Fragen sind:

isarlaw@email.de

oder

0172/8340963

