Deutsche Stiftung für Recht und Informatik

# Vertragsgestaltung und Kontrolle bei Auftragsdatenverarbeitung

**Matthias Bergt**
Rechtsanwälte v. Boetticher Hasse Lohmann

Herbstakademie 2013

# Begriff der Auftragsdatenverarbeitung, § 11 BDSG

- Auslagerung von Verarbeitungsvorgängen personenbezogener Daten
- Auslagerung von Wartung, wenn Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (§ 11 Abs. 5)
- Weit:
  - klassische IT-Outsourcing-Projekte
  - SaaS Unternehmensbuchhaltung
  - Entsorgung von Schriftstücken durch fremdes Reinigungspersonal
  - PC-Reparatur
  - E-Mail-Account

# Grenzen der Auftragsdatenverarbeitung

- Meinungsstreit um Funktionsübertragung im IT-Bereich nicht relevant
- Keine Erheblichkeitsschwelle
  - Also auch kurzfristige Cloud-Nutzung

# Rechtsfolgen der Auftragsdatenverarbeitung

- Gesetzliche Fiktion: Datenweitergabe an Auftragnehmer zur Verarbeitung in EU/EWR ist keine Übermittlung
- Auftraggeber bleibt für Einhaltung des Datenschutzrechts verantwortlich (§ 11 Abs. 1)
  - Auskunft (§ 34)
  - Löschung (§ 35)
  - Schadensersatz (§ 7)
- Auftragnehmer haftet bei weisungswidriger Verwendung der Daten
- Haftet Auftragnehmer auch bei formunwirksamem Auftragsdatenverarbeitungsvertrag?

# Anforderungen an den Auftragnehmer

- Sorgfältige Auswahl „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen“ (§ 11 Abs. 2 Satz 1)
- Schutzstandard regelmäßig Vertragsbestandteil

# Anforderungen an die Vertragsgestaltung

- § 11 Abs. 2 Satz 2 Mindest-Inhalte (nicht abschließend)
  - § 11 Abs. 2 Satz 2: „im Einzelnen festzulegen“
- Schriftform (§ 126 BGB) jedenfalls wegen § 43 Abs. 1 Nr. 2b
- Problematisch:
  - Technisch-organisatorische Maßnahmen (Datensicherheit)
  - Kontrolle (§ 11 Abs. 2 Satz 4)

# Technisch-organisatorische Maßnahmen

- Festlegung „im Einzelnen“ = konkrete Sicherheitsmaßnahmen, deren Vorhandensein überprüft werden kann
- Notwendiges Schutzniveau beim Auftragnehmer = notwendiges Schutzniveau beim Auftraggeber
  - Abwägung, § 9 Satz 2
  - Abhängig auch davon, ob klassische Auftragsdatenverarbeitung oder Wartung (§ 11 Abs. 5)

# Wichtige Regelungsinhalte hinsichtlich TOM

- Datenlöschung
  - Auch aus dem Backup
- Rückgabe/Vernichtung Datenträger
- Sicherheit der Datenübertragung und –speicherung
- Hilfreich: Verschlüsselung
  - Verschlüsselte Datenträger
    - Ermöglicht Nutzung von Gewährleistung/Garantie
    - Ermöglicht Löschung durch Löschen des Schlüssels
  - Verschlüsselte Datenübertragung
    - Auch im Backend
    - Auch bei Weiterleitung als E-Mail

# Festlegung technisch-organisatorischer Maßnahmen

- Sicherheitskonzepte, Zertifizierungen und Aufstellungen technisch-organisatorischer Maßnahmen zum Vertragsbestandteil machen
- Umfassende Liste möglicher technisch-organisatorischer Maßnahmen zum Ankreuzen
  - Prüfen, ob ausreichend; ggf. Einführung ergänzender Maßnahmen vereinbaren
- Regelung über Anpassung an künftige Entwicklungen
  - Regelung über Kostentragung

# Sonstiger Regelungsbedarf

- Ausschluss Zurückbehaltungsrecht an Daten und Datenträgern
- Kontrollen
  - Duldungs- und Mitwirkungspflichten des Auftragnehmers
    - Auskunftserteilung
    - Vorlage von Unterlagen
  - Kontrollrechte ausreichend intensiv, ggf. ergänzend zu Zertifizierungen
  - Betrieblicher Datenschutzbeauftragter, Betriebsrat
- Bei Erstkontrolle nach Vertragsschluss: Rücktrittsrecht bzw. aufschiebend bedingte Auftragserteilung für den Fall von Beanstandungen

# Sonstiger Regelungsbedarf II

- Subauftragnehmer
  - Verbieten?
  - Schriftliche Zustimmung?
  - Vorab-Information mit Widerspruchsrecht?
  - Schutzniveau beim Subauftragnehmer, Kontrollrechte, kein Zurückbehaltungsrecht des Subauftragnehmers
  - Beachte § 11 Abs. 5 (Wartung)
- Unterstützung bei Verfahrensverzeichnis und Data Security Breach Notification
  - Über Anforderungen des § 42a hinaus
- Definition wichtiger Gründe i.S.v. § 314 BGB
  - Auswirkungen bei Rahmenverträgen?
- Vertragsstrafen, Beweislastumkehr analog § 7 BDSG

# Vertragstechnik

- Modularer Aufbau
- In Anlagen auslagern:
  - Gegenstand und Dauer des Auftrags
  - Umfang, Art und Zweck der Verarbeitung; Art der Daten und Betroffene
    - Verfahrensverzeichnis verwenden?
  - Namentlich benannte erlaubte Subunternehmer
  - Technisch-organisatorische Maßnahmen

# Vorgehen bei Massenverträgen

- Initiative vom Anbieter
  - Kostenersparnis durch Standard-Vertrag
- Angebot für normal vertrauliche Daten, ggf. besonderes Schutzniveau als Premium-Produkt
- Ersatz der Kontrolle des Auftraggebers durch Zertifizierungen durch unabhängige Dritte

# Kontrolle des Auftragnehmers

- Vor Beginn der Verarbeitung und sodann regelmäßig (§ 11 Abs. 2 Satz 4)
- Dokumentation (§ 11 Abs. 2 Satz 5)
- Erstkontrolle von besonderer Bedeutung
  - Ordnungswidrigkeit (§ 43 Abs. 1 Nr. 2b)

# Kontrolle durch Dritte

- Vor-Ort-Kontrolle nicht zwingend vorgeschrieben
- Gesetzesbegründung:
  - Auftraggeber kann Sachverständigen beauftragen
  - U.U. Auskunft des Auftragnehmers ausreichend
- Aber auch Zertifizierung im Auftrag des Auftragnehmers zulässig

# Kontrolle ausschließlich durch Zertifizierung?

- Bisher Aufsichtsbehörden: Zumindest Recht auf persönliche Kontrolle unabdingbar
- Aber kein Grund für absolute Einschränkung der Prüfung durch Dritte, wenn umfassende Zertifizierung
- Abhängig vom Schutzbedarf usw. allerdings ergänzendes Prüfungsrecht, ggf. auf Verdachtsfall beschränkt

# Anforderungen an Zertifizierungen

- Keine Entbindung von Auftraggeber-Kontrollpflichten
- Keine Absenkung des Kontrollniveaus
  - Zertifizierer sachkundig und unabhängig?
    - Zertifizierung durch BSI (z.B.)
  - Alle technisch-organisatorischen Maßnahmen bestätigt?
  - Ggf. ergänzende Kontrollen
- Abstimmung von Vertrag und Zertifizierung
  - Gleicher Aufbau Checkliste – Vertrag – Bericht des Zertifizierers
- Verträge und Zertifizierung nicht zu einseitig auf Anbieterinteressen ausgerichtet
  - Der Auftraggeber muss seinen gesetzlichen Pflichten nachkommen können!

# Dokumentation der Kontrolle

- Dokumentationspflicht (§ 11 Abs. 2 Satz 5)
  - Nicht bußgeldbewehrt, aber wichtig als Nachweis der bußgeldbewehrten Erstkontrolle
- Bei Zertifizierung durch vertrauenswürdige Dritte knapper als bei Eigenkontrolle
  - Prüfung auf Einhaltung aller vereinbarten technisch-organisatorischen Maßnahmen muss erkennbar sein

# Gesetzgeberischer Handlungsbedarf

- Aufwand für gesetzeskonforme Auftragsdatenverarbeitung lässt sich bereits de lege lata erheblich verringern
  - Problematisch bleiben Schriftformerfordernis und Kontrolle
- De lege ferenda: keine Schriftform erforderlich
  - Entwurf Datenschutz-Grundverordnung: Dokumentation genügt
- De lege ferenda: Anforderungsprofile an technisch-organisatorische Maßnahmen für Standard-Anwendungsfälle
  - Für Rechtssicherheit: Gesetzliche Definition als ausreichend
- Zertifizierungen anhand der Standard-Anforderungsprofile

# Vielen Dank für Ihre Aufmerksamkeit

**Matthias Bergt**
Rechtsanwälte v. Boetticher Hasse Lohmann
Oranienstr. 164
10969 Berlin
Telefon 030/61 68 94 03
E-Mail mbergt@boetticher.com