IT´S MORNING

Dr. Florian Modlinger

Rechtsanwalt

DATENSCHUTZ UND IT-SICHERHEIT ZWISCHEN RECHT UND TECHNIK

Vertrag zur Auftragsdatenverarbeitung (ADV)

§ 11 Abs. 1 Satz 1 BDSG

„Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.“

DATENSCHUTZ UND IT-SICHERHEIT ZWISCHEN RECHT UND TECHNIK

Inhalt und Form des Auftrags

§ 11 Abs. 2 BDSG

„Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind: …“

DATENSCHUTZ UND IT-SICHERHEIT ZWISCHEN RECHT UND TECHNIK

10-Punkte-Katalog des § 11 Abs. 2 BDSG

- Gegenstand & Dauer des Auftrags
- Umfang, Art & Zweck, Art der Daten, Kreis der Betroffenen
- TOMS (§ 9 BDSG)
- Berichtigung, Löschung und Sperrung von Daten
- Pflichten des AN, insbes. die von ihm vorzunehmenden Kontrollen
- etwaige Berechtigungen zur Begründung von Unterauftragsverhältnissen
- Kontrollrechte des AG sowie Duldungs- & Mitwirkungspflichten des AN
- mitzuteilende Verstöße des AN oder die bei ihm beschäftigten Personen
- Umfang der Weisungsbefugnisse, die sich der AG ggü. dem AN vorbehält
- Rückgabe überlassener Datenträger & Löschung beim AN gespeicherter Daten nach Beendigung des Auftrags

DATENSCHUTZ UND IT-SICHERHEIT ZWISCHEN RECHT UND TECHNIK

Cloud-Computing als Auftragsdatenverarbeitung

Problempunkte:

- **Wie kontrolliert man in der Cloud?**
  - **Vor Ort?**
  - **Indirekt über Zertifikate? Wenn ja, welche?**
- **§ 11 BDSG gilt nur innerhalb der EU bzw. dem EWR**
  - **Und ausserhalb der EU?**
    - **Save Harbour und der EuGH**
    - **Privacy Shield**
    - **Standardvertragsklauseln**

    => Empfehlung: „Regionale“ Anbieter

DATENSCHUTZ UND IT-SICHERHEIT ZWISCHEN RECHT UND TECHNIK

Cloud-Computing als Auftragsdatenverarbeitung

Die Zukunft EU-DSGVO:

"Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

Inhalte:

- **Verarbeitung nur nach Weisung der verantw. Stelle**
- **Verzeichnis der Verarbeitungstätigkeiten**
- **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 30 Absatz 1**

DATENSCHUTZ UND IT-SICHERHEIT ZWISCHEN RECHT UND TECHNIK

Cloud-Computing als Auftragsdatenverarbeitung

Art. 30 DSGVO

Technische und organisatorische Maßnahmen unter Berücksichtigung der Kosten und des Risikos (Eintrittswahrscheinlichkeit und Schwere des Risikos) => Angemessenes Schutzniveau:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

AKTUELLE RECHTLICHE THEMEN

IT-Sicherheitsgesetz

Rechtliche Anknüpfungspunkte:

- Vereinzelte „Initiativen“ zur Regelung / Standardisierung von IT-Sicherheit:
  - Standards und Best Practices: BSI IT-Grundschutz-Kataloge (12. EL)
  - ISO 27001, 27002 / ISO/IEC 38500 / CobiT / ITIL usw.
- Aktuell: IT-Sicherheitsgesetz des Bundes

AKTUELLE RECHTLICHE THEMEN

IT-Sicherheitsgesetz

Zielsetzungen des Gesetzesentwurfs

- IT-Sicherheit von Unternehmen in Deutschland verbessern:

  = Verbesserung des Schutzes der Verfügbarkeit, Integrität und Vertraulichkeit datenverarbeitender Systeme in Anpassung an gestiegene / veränderte Bedrohungslage.

- “verbessertes Bild zur IT-Sicherheitslage” in Deutschland gewinnen
- Verstärkter Schutz der Bürgerinnen und Bürger in sicherem Netz

AKTUELLE RECHTLICHE THEMEN

IT-Sicherheitsgesetz

Überblick zu neuen Regelungen im BSIG

- Definition „kritische Infrastrukturen“ mit VO-Ermächtigung (§§ 2, 10).
- IT-Sicherheitsanforderungen an KRITIS-Betreiber (§ 8a).
- Meldepflicht für Sicherheitsvorfälle (§ 8b)

AKTUELLE RECHTLICHE THEMEN

IT-Sicherheitsgesetz

Betreiber kritischer Infrastrukturen werden verpflichtet,

- ✓ einen Mindeststandard an IT-Sicherheit einzuhalten und
- ✓ dem BSI IT-Sicherheitsvorfälle zu melden.

- Mindeststandard = angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zum Schutz der kritischen Infrastrukturen

  → Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen

- Umsetzungsfrist: 2 Jahre nach Erlass der RVO, danach im Abstand von 2 Jahren nachzuweisen (für Banken Sonderregeln)

COMPLIANCERELEVANTE VORSCHRIFTEN

Gesetzliche Vorschrift	Normadressat	Sanktioniertes Fehlverhalten	Sanktion
Art. 79 DSGVO	Mitarbeiter und Unternehmen	Verletzung der Vorgaben der DSGVO	20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs
§ 823 BGB	Jeder Mitarbeiter eines Unternehmens	Verletzung von Rechts-gütern (z.B. Leben, Gesundheit, Eigentum) anderer Personen	Schadenersatz (§ 249 BGB), ggf. Schmerzens-geld, evtl. Kündigung

COMPLIANCERELEVANTE VORSCHRIFTEN

Gesetzliche Vorschrift	Normadressat	Sanktioniertes Fehlverhalten	Sanktion
§§ 280, 311 Abs. 2, 241 Abs. 2 BGB	Jeder Mitarbeiter eines Unternehmens	Verletzung von Pflichten des Arbeitsvertrags	Kündigung, ggf. Schadenersatz
§ 30 OWiG	Person in leitender Stellung in einem Unternehmen (z.B. Geschäftsführer, Prokurist)	Begehung einer Straftat oder einer Ordnungswidrigkeit durch den Normadressaten und dadurch verursachte Pflichtverletzung oder Bereicherung des vertretenen Unternehmens	Geldbuße bis zu 10 Mio. Euro (vom vertretenen Unternehmen zu zahlen) sowie Gewinnabschöpfung nach § 17 Abs. 4 OWiG, Kündigung

SUN TZU, DIE KUNST DES KRIEGES

Die Kunst des Krieges lehrt uns, nicht darauf zu hoffen, daß der Feind nicht kommt, sondern darauf zu bauen, daß wir bereit sind, ihn zu empfangen.

Sie lehrt uns nicht auf die Möglichkeit zu hoffen, daß er nicht angreift, sondern auf die Tatsache, daß wir unsere Stellung uneinnehmbar gemacht haben.

BESTEN DANK FÜR DIE AUFMERKSAMKEIT