Cloud Computing und Datenschutz

Forum V - Juristisches Kolloquium

Dr. Ulrich Baumgartner, LL.M. (King's College London), CIPP/E
Nürnberg
14. Februar 2019

KNUDDELS-LEAK

Datenschützer verhängen erstmalig Bußgeld nach DSGVO

Nach einem schweren Datenleck ist der Chatanbieter Knuddels noch einmal glimpflich davongekommen. Das Bußgeld nach der DSGVO fiel niedrig aus, weil das Unternehmen gut mit dem Datenschutzbeauftragten kooperierte.

22. November 2018, 10:36 Uhr, Friedhelm Greis

(Bild: Kristina Schäfer/LfDI BW)

Keine gesetzliche Regelung

- DS-GVO soll zu „Modernisierung“ des Datenschutzrechts führen
- Cloud Computing nicht erwähnt
- Auch keine sonstige spezialgesetzliche datenschutzrechtliche Regelung

Cloud Computing nicht spezifisch gesetzlich geregelt!

Orientierungshilfen der Datenschutzbehörden

- „Orientierungshilfe Cloud Computing“ der dt. Aufsichtsbehörden vom Oktober 2014
- Faktisch Bindungswirkung für Cloud-Anwender und Cloud-Anbieter in Deutschland
- Noch keine Stellungnahme explizit zum Cloud Computing nach neuer Rechtslage durch die DSK oder EDSA

Praxiserfahrungen

- Große Cloud-Anbieter haben standardisierte Verträge
- Neben dem kommerziellen Hauptvertrag wird üblicherweise ein „Datenschutzvertrag“ abgeschlossen
- Da Cloud-Services hoch standardisiert sind, haben Anbieter oft wenig Spielraum
- Weiterhin Unsicherheit hinsichtlich Datentransfers in die USA

Verhandlungen in der Praxis oft langwierig und intensiv

Datenschutzrechtliche Einordnung

- Üblicherweise eine sog. „Auftrags(daten)verarbeitung“ nach Art. 28 DS-GVO
- Setzt eine Tätigkeit des Cloud-Anbieters „im Auftrag“ des Cloud-Anwenders voraus
- „Verantwortlicher“: Cloud-Anwender/Kunde
- „Verarbeiter“: Cloud-Anbieter

Spiegelt die tatsächlichen Verhältnisse oft nicht wieder

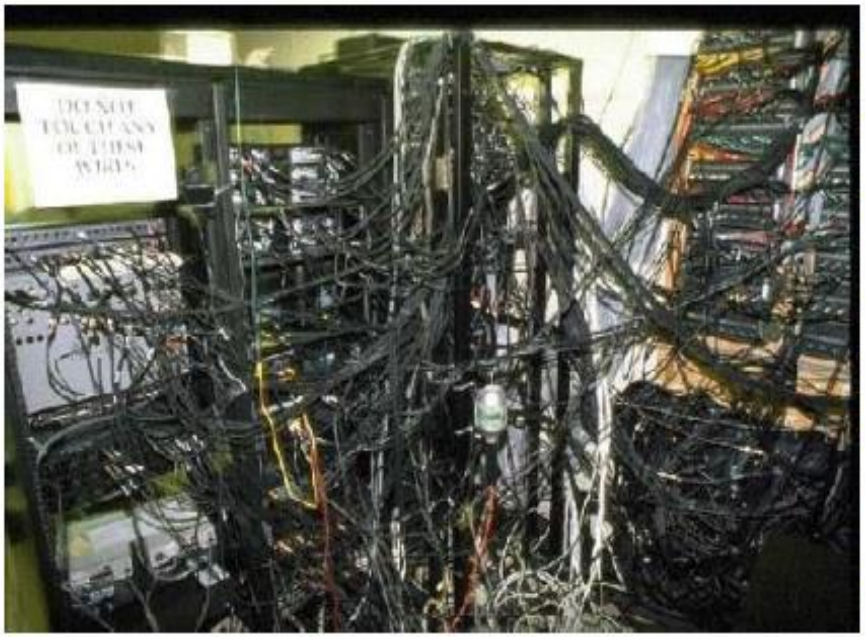
Auftragsverarbeitung

- Art. 28 Abs. 1 DS-GVO:

> „*Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet*.“

Dokumentierte Prüfung und Auswahlentscheidung erforderlich!

Betreffen die TOMs „nur“ die IT-Systeme?



TOMs nicht erfüllt?

TOMs erfüllt?

-> So „einfach“ ist es nicht!

Auftragsverarbeitung - Auswahlentscheidung

- Deutsche Datenschutzbehörden fordern eine umfassende Risikoanalyse durch den Anwender
- Aufsichtsbehörden erwarten ein Konzept für das „*Onboarding*“ von Auftragsverarbeitern (Auszug aus BayLDA Fragebogen):

28. Beschreiben Sie bitte kurz (ca. 1 Seite), wie Sie sicherstellen, dass Auftragsverarbeiter nach Art. 28 DS-GVO auf Basis eines geeigneten Risikomodells und darauf aufbauenden wirksamen technischen und organisatorischen Maßnahmen (entsprechend Art. 25 Abs. 1 DS-GVO) ausgewählt werden?

29. Beschreiben Sie bitte kurz (ca. 1 Seite), wie Sie sicherstellen, dass (bei Auftragsverarbeitungen) die Rechtsgrundlage der sog. zweiten Stufe bei Datentransfers in Drittstatten korrekt ausgestaltet wird.

Auftragsverarbeitung – Vertragliche Regelung

- Art. 28 Abs. 3 DS-GVO legt fest, welche Inhalte zwingend in einer Vereinbarung zur Auftragsverarbeitung enthalten sein müssen
- Weitestgehend wie unter BDSG-alt, aber
  - Anwendungsbereich wird weiter
  - Sanktionsmöglichkeiten und Direktansprüche gegen den Auftragsverarbeiter möglich
  - Zusätzliche Pflichten für den Auftragsverarbeiter (DSB, Verzeichnis von Verarbeitungstätigkeiten, etc.)

Auftragsverarbeitung – Vertragliche Regelung

- Insbesondere folgende Punkte sind zu regeln:
  - Gegenstand und Dauer der Verarbeitung
  - Art und der Zweck der Verarbeitung
  - Art der personenbezogenen Daten
  - Kategorien betroffener Personen
  - Pflichten und Rechte des Verantwortlichen
  - Technische und organisatorische Sicherheitsmaßnahmen
  - Prozess zur Berichtigung, Löschung und Sperrung der Daten
  - Kontroll-/Auditrechte
  - Berechtigung zur Unterbeauftragung („Ob“ und „Wie“)
  - Sonstige Unterstützungsleistungen

Auftragsverarbeitung – Vertragliche Regelung

- In der Praxis sind Vertragsverhandlungen (auf beiden Seiten) meist schwierig
- Grund: Cloud-Dienste meist hoch standardisiert und „Massengeschäft“
- Fast immer grenzüberschreitende Datenübermittlungen, zumindest für Supportzwecke

In der Praxis oft Kompromisslösungen erforderlich!

Auftragsverarbeitung – Praxisprobleme

- Kontrollrechte des Cloud-Anwenders
  - Kontrollen durch Verantwortlichen oder durch Auditor
  - Neben „Überprüfungen“ müssen auch „Inspektionen“ möglich sein
- Vor-Ort-Kontrollrechte weiter erforderlich
  - Unwahrscheinlich, dass Aufsichtsbehörden künftig Ausschluss tolerieren
  - Für Anbieter nur schwer zu akzeptieren und umzusetzen
  - Direkte Kontrollrechte auch ggü. Unterauftragnehmern erforderlich
- Künftig: DS-GVO-Zertifizierungen relevant

Auftragsverarbeitung – Praxisprobleme

- Unterbeauftragung durch Cloud-Anbieter
  - Große Anbieter arbeiten mit langen Ketten von Unterauftragnehmern
- Einschaltung weiterer Auftragsverarbeiter erfordert aber vorherige Zustimmung des Cloud-Anwenders
- Allgemeine Genehmigung ist ausreichend
- Aber: Wie umgehen mit Ablehnung einzelner Unterauftragnehmer die Cloud-Anwender?

Cloud-Anwender bleibt für alle Unterauftragnehmer voll verantwortlich!

Auftragsverarbeitung – Praxisprobleme

- Cloud-Anwender zur Erfüllung von Betroffenenrechten verpflichtet
  - Z.B. Auskunft, Berichtigung, Löschung, Datenportabilität
- Aber: Cloud-Anwender hat (wenn überhaupt) nur sehr eingeschränkten administrativen oder operativen Zugriff auf die Cloud-Infrastruktur
- Also vertragliche Pflicht des Cloud-Anbieters, den Cloud-Anwender
  - zu unterstützen sowie
  - über entsprechende Anfragen zu informieren.

In der Praxis oft umstritten

Auftragsverarbeitung – Praxisprobleme

- Weitgehende Suspensions- und Kündigungsrechte der Cloud-Anbieter
  - Anbieter behalten sich i.d.R. sehr weitgehende Recht vor, die Dienste einzustellen oder zu kündigen
  - Z.B. bei Zahlungsverzug, Sicherheitsvorfällen, Gesetzesänderungen, etc.
- Relevant für unternehmenskritische Anwendungen
- Cloud-Anwender hat hohes Interesse, diese Rechte zu beschränken

Klassischer Interessenkonflikt, der nur schwer aufzulösen ist

Gemeinsame Verantwortlichkeit

- DS-GVO führt in Deutschland gemeinsame Verantwortlichkeit ein
- Eröffnet neue Gestaltungsmöglichkeiten
- Cloud-Anwender und Cloud-Anbieter als gemeinsam Verantwortliche
  - Entspricht oftmals wohl eher der Realität
- Folge für die Praxis:
  - Interessante Option
  - Genaue vertragliche Regelung der Verantwortlichkeiten erforderlich
  - Höhere Verantwortlichkeit für Cloud-Anbieter

Grenzüberschreitende Datenverarbeitung

- Datenverarbeitung in der Cloud nicht ortsgebunden
- I.d.R. wird Cloud-Anwender nicht wissen, an welchem „Ort“ aktuell die Verarbeitung seiner Daten erfolgt
  - Follow-the-Sun-Prinzip
- Vertragliche Vereinbarung über Standorte der Rechenzentren erforderlich
- Zugriffsrechte (z.B. für Support) stehen einer physischen Datenübermittlung gleich
  - In der Praxis erfolgt bei U.S.-Anbietern Support (auch) von außerhalb des EWR

Grenzüberschreitende Datenverarbeitung

- „Ausgleich“ des i.d.R. nicht-adäquaten Datenschutz-Niveaus außerhalb des EWR erfordert weitere Maßnahmen
  - Üblich sind
    - EU/US Privacy Shield (ehemals „Safe Harbor“)
    - EU Standardvertragsklauseln
- Letztere erfordern weitere Verträge, u.U. auch mit Unterauftragnehmern des Cloud-Anbieters

Dadurch steigt Komplexität oft enorm

Grenzüberschreitende Datenverarbeitung

- Sonderfall: „Sensible Daten“
  - Konnten bisher nicht in Clouds außerhalb des EWR verarbeitet werden

- DS-GVO ermöglicht nun grds. die weltweite Verarbeitung „sensibler Daten“
  - Einzelheiten aber noch unklar
  - Noch keine belastbaren Stellungnahmen der Aufsichtsbehörden

Grenzüberschreitende Datenverarbeitung

- Sonderfall: Zugriffe von Regierungsstellen/Geheimdiensten
  - Diskutiert nach Snowden/NSA
  - Hauptgrund für EuGH, Safe Harbor für ungültig zu erklären
- In der Praxis weiter relevant
- US CLOUD Act ermöglicht weitgehenden Zugriff auf Daten, die in Europa gespeichert sind
  - U.S.-Cloud-Anbieter unterfallen diesem Gesetz
  - Entscheidend: Hat Anbieter in den USA „*possession, custody or control over the data being sought*“?

Datenschutzverletzungen

- Cloud-Anwender muss nach DS-GVO u.U. zuständige Aufsichtsbehörde und die betroffenen Personen über „Datenpannen“ informieren
- Wenn die „Datenpanne“ beim Cloud-Anbieter geschieht, ist Cloud-Anwender daher auf Information und Kooperation angewiesen
- Also vertragliche Pflicht des Cloud-Anbieters, den Cloud-Anwender
  - unverzüglich zu informieren und
  - bei Meldungen zu kooperieren

Datenschutzverletzungen

- Achtung - neue „Bedrohung“!
  - Cloud-Anbieter hat Verzeichnis nach Art. 30 Abs. 2 DS-GVO zu führen
  - Darin enthalten sind Namen aller Kunden
  - Aufsichtsbehörden haben angekündigt, bei Datenpannen bei Cloud-Anbietern künftig deren Verzeichnisse zu prüfen und mit Meldungen nach Art. 33 Abs. 1 DS-GVO abzugleichen

Fragen

Dr. Ulrich Baumgartner, LL.M. (King's College London)
Rechtsanwalt | Partner | CIPP/E

T +49 89 5434 8000
T +49 170 2202185
ulrich.baumgartner@osborneclarke.com