# Private – riskante IT-Dienstleister bei Behörden

Harald Zwingelberg

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein



## *Übersicht*

- Rechtslage Auftrags-DV für Behörden im Inland
  - Grundlagen
  - Grenzen
  - Kontrolle
  - Auftrags-DV in EU / EWR
  - Auftrags-DV in Drittstaaten
- Vergaberecht
- PATRIOT ACT, FISA und Co.
- Lösungsideen: Technische u. organisatorische Maßnahmen
- Einzelfälle

# Auftragsdatenverarbeitung gegenwärtige Rechtslage

- Verwendete Abkürzungen
  - AG Auftraggeber / Verantwortliche Stelle
  - AN Auftragsnehmer / Dienstleister
  - Auftrags-DV Auftragsdatenverarbeitung



ULD www.datenschutzzentrum.de

# Auftragsdatenverarbeitung gegenwärtige Rechtslage

- Grundsatz der Rechtmäßigkeit erfordert Gesetz oder Einwilligung zur Datenweitergabe
- Für viele Ansprüche nicht praxisgerecht
  - Webhosting, externe Datensicherung, Clouddienste ...
  - IT-Betreuung von Diensten mit persbez. Daten, ...
  - Druck- und Versanddienste, Aktenvernichtung, ...
- Bei rechtmäßiger Auftrags-DV sind Datenflüsse an AN mit Sitz in EU/EWR keine Übermittlung
  => keine weitere Rechtsgrundlage für Transfer erforderlich

# Auftragsdatenverarbeitung Rechtslage

- Rechtsgrundlagen
  - Umsetzungen von Art. 17 RiLi 95/46/EC
- Umsetzung in nationales Recht unterscheidet nach Auftraggeber
  - Landesbehörden nach LDSG, in S-H: § 17 LDSG-SH
  - Bundesbehörden und private Auftraggeber, § 11 BDSG
  - Sonderregelungen z.B. § 80 SGB X, § 30 AO
- Künftig Art. 26 Datenschutzgrundverordnung für Auftrags-DV und Art. 24 DSGVO für „joint controllers“





# Auftragsdatenverarbeitung deutsche Rechtslage

- Voraussetzungen für Auftrags-DV-Verträge, § 17 LDSG
  - Verantwortung verbleibt beim AG
  - AN verfolgt keine eigenen Zwecke mit den Daten
  - AG stellt durch techn.-org. Maßnahmen sicher, dass Daten nur nach seinen Weisungen verarbeitet werden
  - Besondere Sorgfalt bei der Auswahl des AN
  - Schriftliche Fixierung des Auftrags-DV-Vertrages
  - Sicherstellung der Maßnahmen nach §§ 5-6 LDSG bei AN
  - AN muss betrDSB bestellt haben

# Auftragsdatenverarbeitung deutsche Rechtslage

- Mustertexte und Hinweise für Verträge zur Auftrags-DV
  - Schleswig-Holstein: Derzeit kein Mustertext des ULD
    Vertragsmuster zu § 11 BDSG können herangezogen werden
    Ergänzungen für Schutzziel „Intervenierbarkeit“ nötig

- Mustertexte anderer Aufsichtsbehörden
  - Datenschutz-WIKI beim BfDI
    http://www.bfdi.bund.de/bfdi_wiki/index.php/Mustervereinbarung_Auftragsdatenverarbeitung
  - Orientierungshilfe und Muster Auftrags-DV, LfD Bayern
    Orientierungshilfe: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsdatenverarbeitung.html
    Mustervertrag: https://www.datenschutz-bayern.de/technik/orient/m-vertr.htm





# Rechtliche Grenzen der Auftrags-DV

- Berufsgeheimnisträger: Auftrags-DV rechtfertigt nur Übermittlung nach BDSG, nicht Offenbarung nach StGB

- AO: Steuerdaten dürfen nur bei öffentlich-rechtlichen Auftragnehmern verarbeitet werden

- SGB: Sozialdaten bei öffentlichen Stellen oder in den engeren Grenzen des § 80 Abs. 5 SGB X

- Dilemma: Oftmals könnten AN bessere IT-Sicherheit gewährleisten als die AG selbst, z.B. bei kleinen öffentlichen Stellen, Ärzten, ...

# Auftragsdatenverarbeitung Kontrolle

- Kontrolle durch Aufsichtsbehörde des Auftraggebers
  - Für AG in S-H Kontrolle durch ULD
  - Sofern AN in S-H auch unmittelbar für den AN
- Kontrolle der Verarbeitung beim AN durch AG
  - Sorgfältige Auswahl des AN
  - Dokumentation der techn.-org. Maßnahmen
  - AN fähig und willig zu weisungsgemäßer DV
  - Kontrollmöglichkeit für AG ist vertraglich zuzusichern, § 17 IV LDSG. Folge: mittelbare Kontrolle des ULD für AN in anderen Bundesländern / Ausland





# Auftragsdatenverarbeitung in EU Mitgliedstaaten

- Gleichlauf mit Übermittlung im Inland, § 16 I LDSG
- Spezialvorschrift für Auftrags-DV im Ausland fehlt im LDSG
- ULD: Gleiche Voraussetzungen wie Übermittlung in Drittstaat: Angemessenes Datenschutzniveau oder Einwilligung, ... § 16 II LDSG
- Bei Entscheidung über Angemessenheit des Datenschutzniveaus ist das ULD zu hören

# Auftragsdatenverarbeitung in Drittstaaten

- Dilemma
  - Vergaberecht: Diskriminierung von Bietern stark eingeschränkt
  - Objektive Unmöglichkeit anderweitiger Beschaffung
    - Relevante Betriebssysteme
    - Programmiersprachen und Compiler überwiegend unter Kontrolle von Unternehmen in Drittstaaten entwickelt
    - Komponenten für (Mobilfunk-)Netzinfrastruktur hergestellt in USA oder China
    - Kaum Hardwareherstellung in Europa
    - ...
- Drittstaatenfreie Datenverarbeitung ist de facto unmöglich





# Vergaberecht als kollidierendes Rechtsgebiet

- § 97 II GWB Gleichbehandlung der Bieter
- § 97 IV GWB Vergabe an fachkundige, leistungsfähige sowie gesetztreue und zuverlässige Unternehmen
  - Gesetzesverstöße nur bei einigem Gewicht relevant und wenn im Rahmen beruflicher Tätigkeit
  - Gesetzestreue muss mit Auftrag in Verbindung stehen
  - Intention zu „gesetzestreue“ waren Arbeitsbedingungen
- Weitere Anforderungen nur sofern in Bundes- oder Landesgesetz besonders vorgesehen

# Vergaberecht und „No Spy“-Erklärung

- Inhalte der „No spy“-Klausel im BMI-Erlass vom 30. April 2014
- Bei Vergabeverfahren mit Sicherheitsrelevanz, insbesondere im IT-Bereich soll von Bietern Eigenerklärung gefordert werden
- „Bestätigung des Bieters, keiner Verpflichtung zu unterliegen, im Auftragsfall vertrauliche Informationen Dritten zugänglich machen zu müssen; ausgenommen sind danach gesetzliche Offenlegungspflichten (z.B. gegenüber der Börsenaufsicht, Finanzverwaltung oder Regulierungsbehörden), es sei denn, solche Offenlegungspflichten bestünden gegenüber ausländischen Sicherheitsbehörden.“

Zitiert aus dem Beschluss der 2. Vergabekammer S. 23 http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Vergaberecht/2014/VK2-39-14.pdf?__blob=publicationFile&v=2.

Pflicht zur Offenbarung möglicher rechtlicher Hindernisse auch in Ziff. 6.3 der Stellungnahme der Art. 29 WP genannt:, Siehe Working Paper 195





# Vergaberecht und „No Spy“-Erklärung

- Beschluss 2. Vergabekammer des Bundes vom 24. Juni 2014
  - Abschluss des Teilnahmewettbewerbs mit Entscheidung für Beigeladene mit einer US-Konzernmutter
  - Antragstellerin verweist auf Erlass der Bundesregierung No Spy Erklärung abzugeben und verlangt, erneute Eignungsprüfung der Bieter. Die Bg. könne diese Erklärung jedenfalls nicht abgeben.
  - I. Formell kommt Forderung zu spät. BMI hätte gar nicht wieder in Eignungsprüfung eintreten dürfen
  - II. Pflichten nach Patriot Act waren seit 2001 bekannt und exzessive Datenabrufe seit Juni 2013. Damit hätte sie bereits bei Eignungsprüfung einfließen müssen
  - III. Eignungsanforderungen sind Bieterbezogen. Nur was Bieter zurechenbar ist, darf berücksichtigt werden. Pflichten aus fremden Rechtsordnungen sind nicht zurechenbar

http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Vergaberecht/2014/VK2-39-14.pdf?__blob=publicationFile&v=2

# Vergaberecht und „No Spy“-Erklärung

- Beschluss 2. Vergabekammer des Bundes vom 24. Juni 2014
- Erfahrungen für den Datenschutz:
  - Bieter können nicht für allgemein geltende Rechtsordnung, der sie unterworfen sind haftbar gemacht werden
  - Aspekt der Datenweitergabe hätte aber ggf. als „besondere Anforderung an die Auftragsausführung“ nach § 97 IV 2 GWB Berücksichtigung finden können.
  - „No-Spy“-Klausel muss als explizite Anforderung an die Antragsausführung im Vorfeld aufgestellt werden

http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Vergaberecht/2014/VK2-39-14.pdf?__blob=publicationFile&v=2





# USA: PATRIOT Act, FISA und co.

- Berechtigung für US-Behörden:
  - Sicherheitsbehörden können Unternehmen mit National Security Letters (NSL) zur Herausgabe von Informationen zwingen während Unternehmen gleichzeitig zur Geheimhaltung verpflichtet sind
  - Anzahl NSL mit Bezug zu „US-persons“ von 9200 (2005) auf 16500 (2011) gestiegen
  - FBI kann u.a. von Access Providern Name, Adresse, Dauer des Vertragsverhältnisses und Rechnungen verlangen – aber keine Inhaltsdaten

- *Fossoul, “Does the USA PATRIOT Act Give U.S. Government Access to E.U. Citizens’ Personal Data Stored in the Cloud in Violation of the E.U. Law? “ S. 31 ff, Link: arno.uvt.nl/show.cgi?fid=127396*

# USA: PATRIOT Act, FISA und co.

- Möglichkeiten des Umgangs mit NSL für US-Unternehmen
  - Gerichtliche Prüfung der Verschwiegenheitspflicht beantragen
  - Twitter hat dies erfolgreich durchgeführt mit Verweis auf die eigene Datenschutzerklärung, die Nutzern Transparenz verspricht
  - Übergabe nur der absolut notwendigen Daten statt Gewährung übermäßigen Datenzugriffs

- *Fossoul, "Does the USA PATRIOT Act Give U.S. Government Access to E.U. Citizens' Personal Data Stored in the Cloud in Violation of the E.U. Law? " S. 31 ff, Link: arno.uvt.nl/show.cgi?fid=127396*





# USA: PATRIOT Act, FISA und co.

- Zugriff unabhängig vom Ort der Datenspeicherung gemäß eines „warrant" gegen Microsoft
  - Gegenstand sind E-Mails in einem Verfahren wegen Drogendelikten auf Microsoft Servern in Dublin
  - Nach Begründung der StA ist die geografische Belegenheit der Daten irrelevant für den Electronic Communications Privacy Act, da Microsoft als Unternehmen Adressatin der Pflicht sei
  - Spitzfindige Begründung des Richters: Die Anordnung ist sowohl erlaubter Zwang zur Herausgabe von Dokumenten im Ausland als auch eine dann in den USA erfolgende Durchsuchung der E-Mails

- Zusammenfassung mit Verweisen auf die Entscheidung und die Schriftsätze: http://www.washingtonpost.com/world/national-security/microsoft-fights-us-search-warrant-for-customer-e-mails-held-in-overseas-server/2014/06/10/6b8416ae-f0a7-11e3-914c-1fbd0614e2d4_story.html

# USA: PATRIOT Act, FISA und co.

- Aktuelle Lage
  - USA FREEDOM ACT im Congress am 22. Mai 2014 behandelt bringt kleine Verbesserungen beschränkt auf „US-persons“
  - Vorratsdatenspeicherung wird auf TK-Unternehmen verlagert
  - Keine wesentliche Einschränkungen der Überwachung von Ausländern
  - IT-Industrie in der USA stellt breite Front gegen die Maßnahmen zum Schutz des Europa-Geschäfts





# Die Zukunft mit CETA und TTIP

- Freihandelsabkommen zwischen EU und USA (TTIP) und Kanada (CETA) geplant
- Im CETA Entwurf heißt es u.a.:

- “Further to Article X (Exceptions - General Exceptions), and notwithstanding the paragraph 3, a Party shall take appropriate measures to protect:
  (a) the security and confidentiality of telecommunications services, or
  (b) the privacy of users of public telecommunications transport services, subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.”

- Consolidated CETA Text S. 288. Quelle: *www.tagesschau.de/wirtschaft/**ceta-dokument-101**.pdf*

# Die Zukunft mit CETA und TTIP

- Mögliche negative Folgen für Datenschutz
  - AG müssten ausreichendes Interesse an besonders strengen Vertraulichkeitsbedarf nachweisen, wenn US-Konzerne aus Rechtsgründen nicht mitbieten sollen
  - Verbot der Lokalisierung von Datenverarbeitungs-vorgängen in TTIP / CETA kollidiert mit Pflicht des AG, Kontrolle und Transparenz zu wahren
  - Konflikte sind vor allem bei Zweckbindung und Grenzen für den Zugriff staatlicher Behörden zu erwarten
  - Künftig könnte der Umfang erforderlicher datenschutz-rechtlicher Maßnahmen ggf. durch TTIP und CETA beschränkt werden





# Technisch-organisatorische Maßnahmen

- Es bleibt bei den „klassischen“ Lösungen des Datenschutzrechts
- Regelungen im Auftrags-DV-Vertrag / Vergabeverfahren
  - Offenlegung der Konzernstruktur und Angabe, ob Verschwiegenheitspflicht und Transparenzgebot aus gesetzlichen oder vertraglichen Gründen nicht eingehalten werden können
  - Selbstverpflichtung zur vollen Transparenz gegenüber AG und allen Betroffenen in der Datenschutzerklärung des Unternehmens
  - Unterrichtungspflicht des AN, sobald die Pflichten nicht eingehalten werden können
  - Vertragsstrafe in abschreckender Höhe für Datenweitergabe
  - Außerordentliches Kündigungsrecht des AG bei Verstößen
  - Verpflichtung aller Mitarbeiter der AN auf Vertraulichkeit

# Technisch-organisatorische Maßnahmen

- Maßnahmen
  - Datenhaltung, -verarbeitung und -lagerung nur in den Räumen, auf Geräten und unter Kontrolle des AG
  - Hilfsweise keine unverschlüsselten Kundendaten des AG auf eigener Infrastruktur des AN und Schlüssel nur bei AG
  - Verbot der Weitergabe von projektinternen Informationen innerhalb des Unternehmens der AN
  - Zugriff auf auftragsrelevante Daten durch Konzernunternehmen mit Sitz in Drittstaaten ausschließen oder nur mit Wissen und Wollen des hiesigen Vertragspartners
  - Kein (Fern-)Zugriff der Mitarbeiters des AN auf personenbezogene Daten außer rein AN-bezogene Daten z.B. Stunden für Abrechnung
  - Sensibilisierung und Ausbildung aller Mitarbeiter zum Datenschutz
  - Zugang zu personenbezogenen Daten und sonstigen vertraulichen Informationen des AG bevorzugt für Personen mit Wohnsitz in EU





# Technisch-organisatorische Maßnahmen

- Maßnahmen für geeignete Einzelfälle
  - AN ohne möglichen Zugriff auf Inhalte
    Soweit Verfahren mit verschlüsselten Daten möglich ist, hat Verschlüsselung vor dem Datentransfer zu erfolgen und Keys dürfen ausschließlich beim AG liegen (z.B. für Storage und Backup)
  - Soweit Personenbezug über Nutzerdaten hergestellt wird, sollten Dienste genutzt werden, die anonyme oder datenminimierende Authentifizierung innerhalb des Systems unterstützen (verlg. ABC4Trust Projekt, u.a. sind Angebote der Unternehmen IBM und Microsoft zu erwarten)

Für technische Details und rechtliche Aspekte siehe https://www.abc4trust.eu

# Einzelfragen Sozialdaten

- Sonderregelungen in § 80 Abs. 4, 5 SGB X
- Private müssen sich zusätzlichen Kontroll- und Duldungsrechten gegenüber AG unterwerfen, § 80 II SGB X
- Auftrags-DV durch Private nach Abs. 5 nur zulässig, wenn
  - Andernfalls Störungen im Betriebsablauf des AG auftreten können oder
  - Aufgaben durch AN erheblich kostengünstiger besorgt werden können als durch AG, dabei muss überwiegender Datenbestand beim AG verbleiben
- Kontrolle über AN übt die für AN zuständige Aufsichtsbehörde aus. Mittelbar auch Kontrolle durch die LfD des AG (Auftrag, Maßnahmen, Umsetzung), soweit nicht durch z.B. Staatsvertrag anders geregelt





# Einzelfragen Berufsgeheimnisträger

- Besonderheiten für Berufsgeheimnisträger nach § 203 StGB (Amtsärzte, Amtstierärzte, ...)
- Auftrags-DV legitimiert Datentransfer nur nach Datenschutzrecht, nicht aber Offenbarung nach § 203 StGB
- Offenbarungsbefugnis via Einwilligung, mutmaßlicher Einwilligung oder bereichsspezifischem Gesetz erforderlich

# Einzelfragen Steuerdaten

- Besondere Vertrauensschutz der AO ist Ausgleich zur umfassenden Offenbarungs- und Mitwirkungspflicht
- Nur öffentliche Stellen als Auftragnehmer bei Steuerdaten erlaubt
- Einwilligung erlaubt nach Ansicht diverser LfD nur Offenbarung an Dritte, nicht aber vorsätzliche Nichtachtung der vorgeschriebenen Sicherheitsanforderungen
- § 87a I AO zwingende Ende-zu-Ende Verschlüsselung, außer Vorgang des „Umschlüsselns“ bei De-Mail
- Übermittlung möglich bei Schutz nach PostG oder TKG





# Einzelfragen Versand im hybriden Verfahren

- Hybride Versanddienste erlauben postalische Zustellung von digital eingelieferten Schreiben
- Vorteile: Kostenersparnis, Wegfall von Fehlerquellen wie Kuvertiermaschine, dynamische Inanspruchnahme
- Feststellungen des Lorenz-von-Stein-Instituts, 2011 [1] zum e-Postbrief:
  - Einsatz hybrider Lösung genügt wohl Schriftform
  - Hybride Lösung könnte TKG und PostG unterfallen, aber gesetzliche Klarstellung für Medienbruch nötig

[1] http://www.lvstein.uni-kiel.de/t3/fileadmin/user_upload/MSV_11_FINAL.pdf (Seiten 115 ff, S. 138)

# Einzelfragen
# Versand im hybriden Verfahren

## Gegenwärtige Bewertung des ULD

- Druckvorgang im hybriden Verfahren ist weder Telekommunikation (TKG) noch Postdienst
- Qualitätskontrollen, Papier nachlegen etc. ist Offenbarung im Sinne der AO
- Argument De-MailG: Gesetzgeber sah Bedarf für Fiktion, dass „Umschlüsseln“ keine Offenbarung ist. Damit ist entschlüsseln mit Druck und Möglichkeit der Einsicht eine Offenbarung.

⇒ Hybride Dienste privater Anbieter dürfen derzeit nicht verwendet werden

⇒ Gesetzgeber könnte in E-Gov-Gesetzen modernisieren





# Zusammenfassung

- Gesetzgeberische Initiative zur Auftrags-DV nötig
  - Auftragsdatenverarbeitung ist Chance und Risiko für den Datenschutz
  - Auftraggeber muss Kontrolle und Sicherheit auch beim AN umfassend gewährleisten können – gerade bei Wahl von Anbieter in Drittstaaten

- EU-Gesetzgeber gefordert bei Auftragnehmern Drittstaaten
  - Verhinderung staatlicher Zugriffe
  - Transatlantische Handelsabkommen gefährden Datenschutz und Bürgerrechte


# Fragen?
# Anregungen?

Kontakt:
Harald Zwingelberg
uld2@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1284

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein