Wir schaffen Klarheit.

DORDA
BRUGGER
JORDIS

# US Patriot Act, FISA & Co

## Zugriff durch US Behörden auf Daten

9. Österreichischer IT-Rechtstag

7.5.2015

Axel Anderl

# Überblick

- Grundlagen
  - US Rechtsgrundlagen für (gerichtliche) Zugriffe
  - EU-Datenschutzrecht
- Faktische Durchsetzung
  - Anordnungen/Herausgabe versus EU Datenschutzrecht
  - Szenarien aus der Praxis
  - Durchgriff Geheimdienste?
- Rechtsfolgen
  - Konsequenzen einer (unzulässigen) Herausgabe
  - Haftung wegen Sorgfaltsverstoß?
  - Haftung bei Eingriffen von Geheimdiensten?
- Aktuelle Fälle
  - Fälle "*Microsoft*", "*Gmail*" und "*Wikipedia* "
- Konsequenzen für die Vertragsgestaltung

# Grundlagen

## US Rechtsgrundlagen für (gerichtliche) Zugriffe

- FISA
  - **F**oreign **I**ntelligence **S**urveillance **A**ct 1978
  - regelt Auslandsaufklärung und Spionageabwehr
  - FISC ausschließlich für FISA-Fälle geschaffenes Gericht
    - für Anordnung von Überwachungen
    - kann Überwachungsmaßnahmen bei Gefahr nachträglich genehmigen
    - nicht öffentliche Sitzungen
- US Patriot Act
  - **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **A**ct 2001
  - direkte Reaktion auf die Terroranschläge vom 11.9.2001
  - ändert und ergänzt FISA

# Grundlagen

## US Datenzugriff mit richterlicher Genehmigung

- Ursprung Terrorismusbekämpfung
  - Herausgabe Geschäftsunterlagen und Daten aller Art von beliebiger Stelle
  - Gerichtliche Genehmigung durch das FISC auf Antrag von US Sicherheitsbehörden (zB FBI)
  - Verbindung zu Terrorismus oder Spionage (auch Untersuchung) erforderlich (§ 1861 FISA).
  - "Gag-order": Anordnungsempfänger wird idR zur Verschwiegenheit verpflichtet
  - Herausgeber ist von SchaE Ansprüchen (in den USA) befreit
- Einzige inhaltliche Ausnahme
  - Religions-, Meinungs-, Presse- und Versammlungsfreiheit von US Staatsbürgern

# Grundlagen

## US Datenzugriff ohne richterliche Genehmigung

- "Targeting":

  US Geheimdienste können
  - ohne richterliche Genehmigung oder Information der Betroffenen,
  - die gesamte elektronische Kommunikation von, zu und über eine Zielperson
  - bis zu einem Jahr lang abfangen und analysieren (§ 1881a FISA)
  - sofern "*vernünftigerweise anzunehmen*" ist, dass sich die Zielperson im Ausland befindet
  - Zufallsfunde gg US Bürger sind verwertbar

- Extensive Auslegung
  - Zugriff auf Daten aller Art von Personen, die rechtlich oder tatsächlich Zugang zu den begehrten Daten erlangen können
  - Anordnungen auch auf europäische Server, wenn faktische Zugriffsmöglichkeit

# Grundlagen

## US Datenzugriff ohne richterliche Genehmigung

- National Security Letter
  - direkter Datenzugriff durch das FBI
  - Informationen, die für Untersuchung zu Zwecken nat Sicherheit benötigt
  - Telekommunikationsanbieter, Banken und Finanzunternehmen können verpflichtet werden, Daten über ihre Kunden herauszugeben
  - auf Name, Adresse, Dauer der Nutzung und Abrechnungsdaten beschränkt
  - idR mit Geheimhaltungsanordnung ("Gag-order") verbunden
  - Kunde und Öffentlichkeit werden daher vom Datenzugriff nicht informiert

# Grundlagen

## Datenschutzrecht in EU weitgehend vereinheitlicht

- RL 95/46/EG (Datenschutz-RL) beschränkt die Übertragung von personenbezogenen Daten an Staaten ohne vergleichbares Datenschutzniveau
- Staaten ohne angemessenem Datenschutz sind Drittstaaten außerhalb des EWR, die nicht explizit in der DSAV genannt sind
  - zB Indien, Singapur, Russland, USA, Kanada
  - Ausnahmen: Safe Harbor in USA, PIPEDA in Kanada
  - US Behörden idR nicht Safe Harbor zertifiziert
- Übermittlungen/Überlassungen an Empfänger in unsicheren Drittstaaten erfordert Genehmigung der DSB (§§ 12, 13 DSG)
  - lange Verfahrensdauer bei der Datenschutzbehörde
  - weitere, detaillierte Rückfragen können Verfahren zusätzlich verzögern
  - ad hoc Genehmigung nicht erzielbar

# Grundlagen

## Datenschutzrecht in EU weitgehend vereinheitlicht

- Herausgabeanspruch einer Behörde erfordert Übermittlung (C2C)
  - Behörde verarbeitet Daten zu eigenen Zwecken
- Übermittlung bedarf einer gesonderten Rechtfertigung (§§ 8, 9)
  - gesetzliche Grundlage – geltende Rechtslage in Österreich
  - überwiegende berechtigte Interessen des Auftraggebers/Dritten
  - Zustimmung des Betroffenen
  - lebenswichtige Interessen des Betroffenen
- FISA, Patriot Act, etc sind keine gesetzliche Grundlage iSd DSG
- Zugriffe der US Behörden erfordert daher andere Rechtfertigung
  - überwiegende Interessen werden eng ausgelegt
  - in der Praxis überwiegen die Geheimhaltungsinteressen der Betroffenen

# Faktische Durchsetzung

## Anordnungen/Herausgabe versus EU Datenschutzrecht

- Befolgung eines Herausgabeanspruchs
  - zwingend nur für US Unternehmen
  - keine gesetzliche Verpflichtung für EU Auftraggeber
  - Problem in der Praxis: EU Auftraggeber mit US Tochter oder US Dienstleister
- Befolgung ist Verstoß gegen EU Datenschutzrecht
  - keine gesetzliche Grundlage
  - Übermittlung idR nicht durch überwiegende berechtigte Interessen gedeckt
  - gültige Zustimmung aller Betroffenen praxisfern (Bestimmtheitserfordernis!)
  - keine lebenswichtigen Interessen betroffen
  - **Übermittlung daher <u>unzulässig</u>**
- Herausgabe von Daten an US Behörden durch EU Auftraggeber daher klarer Datenschutzverstoß und damit rechtswirdrig

# Faktische Durchsetzung

## Szenarien aus der Praxis – US Anbieter

- US Anbieter von IT-Infrastruktur und –Services
  - EU Auftraggeber setzt US Dienstleister ein
  - Dienstleister meist Safe Harbor zertifiziert – heilt aber keinesfalls Weitergabe an US Behörden
  - direkter Datenzugriff für Behörden möglich, sofern Zugang zu Daten (rechtlich oder tatsächlich) besteht
  - Zugriff/Herausgabe durch US-Sanktionen gegenüber US Anbieter durchsetzbar
  - umfasst auch in Europa gelegene Infrastruktur des US Anbieter
- US Muttergesellschaft mit europäischer Tochter
  - Anordnung gegenüber Muttergesellschaft
  - Tochter darf Weisung wegen EU-Datenschutzrecht nicht befolgen
  - Muttergesellschaft drohen ggfs Sanktionen
  - Problem in der Praxis: wirtschaftlicher Druck auf Tochterunternehmen

# Faktische Durchsetzung

## Szenarien aus der Praxis – (Konzern-)Verflechtung in die USA

- Europäische Muttergesellschaft mit US Tochter
  - kein Weisungsrecht der Behörde gegenüber EU-Muttergesellschaft
  - US-Tochter unterliegt aber unmittelbar der Herausgabeanordnung
  - indirekter Druck auf EU-Muttergesellschaft über Tochter bei Verweigerung der Herausgabe ihrer Daten?
- Keine Niederlassung, aber Geschäfte in den USA
  - Anwendbarkeit der US-Regelungen schon bei "*kontinuierlichen und systematischen Geschäften*" in den USA
- Keinerlei gesellschaftsrechtliche Verflechtung in die USA
  - kein unmittelbares Datenzugriffsrisiko
  - faktisches Problem: geheimdienstlicher Datenzugriff auch auf außerhalb der USA gespeicherte Daten

# Faktische Durchsetzung

## Überwachung durch Geheimdienste

- Zugriffe (durch Geheimdienste) auch in EU praktisch unumgänglich
  - UKUSA Vereinbarung (Five Eyes): NSA (USA), GCHQ (UK), DSD (Australien), CSEC (Kanada), GCSB (Neuseeland)
- Zugriffe sind jederzeit und ohne Gerichtsbeschluss sowohl in den USA als auch innerhalb der EU faktisch möglich
- keinerlei Transparenz über tatsächliche Datenzugriffe
  - große mediale Bekanntheit erst seit Wikileaks und Snowden
- Geheimdienstaktivitäten kein kalkulierbares Risiko
  - Gefahr besteht faktisch zu jeder Zeit, unabhängig vom Ort der Datenverarbeitung

# Rechtsfolgen

## US Konsequenzen bei Nicht-Herausgabe

- Nichtbefolgung von Anordnungen bzw Urteilen gilt nach US-Recht als Missachtung des Gerichts
- Strafe bzw Bußgeld nach richterlichem Ermessen
- durchsetzbar nur gegenüber dem US-Recht Unterworfene
  - Datenzugriffsanordnung /-urteil gegenüber europäischen Staatsbürgern und Unternehmen nicht durchsetzbar/vollstreckbar
  - praktisches Risiko eines US-Datenzugriffs daher von der Verflechtung des Konzerns in den USA abhängig
  - faktisches Risiko bei US Mutterkonzern am höchsten
  - persönliche Anknüpfungspunkte (zB Einreise) beachten

# Rechtsfolgen

## EU Konsequenzen einer unzulässigen Herausgabe

- datenschutzrechtliche Unzulässigkeit der Übermittlung
  - Verstoß gegen DSG = Rechtsbruch nach UWG
  - Klagen von Mitbewerbern auf Basis des UWG (Unterlassung, Herausgabe Gewinn, Schadenersatz, Urteilsveröffentlichung)
- selbst bei Zulässigkeit: Fehlen der notwendigen Genehmigung
  - Verwaltungsstrafen in Österreich bis EUR 25.000 pro Anlassfall
- Ggfs Konventionalstrafen aus Vertrag
- Zivilklagen von Betroffenen
  - Schadenersatzansprüche, Unterlassung, Urteilsveröffentlichung
- negative PR Folgen
  - Skandalberichte in Medien

# Rechtsfolgen

## Haftung wegen Sorgfaltsverstoß?

- GF Haftung?
  - Weitergabe durch Unternehmen – klarer Verstoß
  - Öffnungsklausel in Verträgen – Weitergabe durch US Dienstleister an US Behörden erlaubt/zugestimmt ?
  - sehenden Auges einer unzulässigen Datenweitergabe zugestimmt?
- Ablehnung zu SWIFT Abkommen
  - 2010: Ablehnung EU Parlament wegen Datenübermittlung in USA (20100209IPR68674)
  - 2013: Aussetzung des Abkommens wegen NSA Vorfällen
- Gegenargumente
  - Unmöglichkeit des Anbietens von leistbaren IT Dienstleistungen
  - Vielfach Dienste nur in/über USA bzw US Anbieter möglich

# Rechtsfolgen

## Haftung bei Eingriffen von Geheimdiensten?

- GF Haftung?
  - keine vorhersehbaren Eingriffe
  - Zugriffe ebenso bei Wahl von EU Dienstleistern oder eigener Leistungserbringung möglich
  - kein vorwerfbares Verhalten
- Gegenargumente
  - Zugriffe bei einigen US Anbietern öffentlich bekannt
  - Verpflichtung zur sorgsamen Auswahl von Dienstleistern nach DSG
- Fazit - GF Haftung
  - Risiko bei direkter Weitergabe durch Unternehmen hoch
  - Risiko bei Weitergabe an US Behörden durch Dienstleister eingeschränkt
  - Risiko bei Eingriffen von Geheimdiensten kaum vorstellbar

# Aktuelle Fälle

## Fall "*Microsoft*"

- 2011 bestätigt MS Herausgabepflicht von Gesellschaften mit Sitz in USA von Daten auch aus RZ außerhalb USA an US-Behörden
- zwei US-Gerichte verurteilten MS zur Herausgabe von in Irland gespeicherten Daten
  - 1. Urteil vom 25.4.2014, GZ 13 Mag. 2814
  - 2. Urteil von Richterin Loretta Preska (New York) "*It is a question of control, not a question of the location of that information*"
  - MS stärkt Abgrenzung zur Massenüberwachung und bekämpft Urteile
- Luxemburger Datenschutzbehörde:
  - Übermittlung in die USA stellt keine Verletzung des EU-Datenschutzrechts dar
  - Begründung: MS sei Safe-Harbor-zertifiziert
  - Massenzugriffe stehen jedoch nicht im Einklang mit DatenschutzRL
  - Entscheidung übersieht, dass US-Behörden nicht Safe-Harbor-zertifiziert sind!

# Aktuelle Fälle

## Fall "*Gmail*"

- Google hat US-Behörden (FBI) Zugriff auf drei Gmail-Konten von Wikileaks-Mitarbeitern gewährt, ohne Betroffene darüber zu informieren
  - secret search warrant eines US Richters verbunden mit einer Non-Disclosure Order
  - basierend auf dem Electronic Communications Privacy Act
- Durchsuchungsbefehl war mit "Gag-Order" versehen, die Ende 2014 teilweise aufgehoben wurde

# Aktuelle Fälle

## Fall "*Wikipedia*"

- 2015 klagen Wikimedia Stiftung, Amnesty International und Menschenrechtsorganisationen ua NSA und US-Justizministerium wegen rechtswidriger verdeckter Massenüberwachung
  - Case: 15-cv-00662-RDB, 10.3.2015
- Vorwurf
  - Überschreitung der FISA-Überwachungsbefugnisse, weil auch elektronische Kommunikation von US-Bürgern massenhaft überwacht
  - Verletzung 4th Amendment: Schutz Privatsphäre von Amerikanern
  - Verletzung 1st Amendment: Schutz Meinungsfreiheit von Amerikanern
- Ähnliche Klage scheiterte im Februar 2013, weil (noch) "*zu sehr auf Spekulation basierend*"

# Aktuelle Entwicklungen

## Gesetzgebung und Judikatur

- USA: Zwei aktuelle Entwürfe, die Zugriff der US-Behörden auf ausländische Daten beschränken sollen
  - Beschränkung des Zugriffs auf Daten von US-Bürgern
  - kein Zugriff, wenn der Adressat gegen nationales Recht verstoßen würde
- GB: Gerichtsurteil, wonach elektronische Massenüberwachung durch britischen Geheimdienst und Informationsaustausch mit NSA gegen europäische Menschenrechte verstößt
- D: Bestrebungen, Cloud Computing EU-rechts- und datenschutzkonform auszugestalten (Vorschläge an EU Organe)

# Konsequenzen für die Vertragsgestaltung

## Risiken erkennen und abwenden

- Weitergabe an US Behörden oft versteckt
  - Erlaubnis zur Weitergabe oft kompliziert umschrieben und in anderen Punkten versteckt
  - Oft weite Formulierungen ("to fully comply with court orders")
  - offener Diskurs mit Vertragspartner führt oft zur (negativer) Klarheit
- Besondere Vorsicht im regulatorischen Umfeld
  - strengere Regelungen (VAG, BWG, WAG)
  - saubere Mandantentrennung ?
- Erlaubnis zum Einsatz von Subunternehmern oft zu weitgehend
  - oft nicht explizit genannt, sondern nur pauschal erlaubt
  - unbegrenzte Anzahl an Subunternehmern ohne Ablehnungsrecht nicht datenschutzkonform
  - Vorlage einer aktuellen Liste aller Subunternehmer vereinbaren

# Konsequenzen für die Vertragsgestaltung

## Cloud Computing / Outsourcing

- Datenherausgabe auf "need to know" Basis
- Bei US Anbietern
  - genaue Prüfung, wo Daten verarbeitet werden
  - welche Subdienstleister/Datencenter werden eingesetzt?
  - Öffnungsklausel für Datenherausgabe nach ausländischem Recht?
  - Vereinbarung, dass Daten nur innerhalb EWR verarbeitet werden
  - Verschlüsselung; outsourcendes Unternehmen hat einzigen Schlüssel
  - Problem Incidents
- Nutzung von EU-Clouds als Alternative
- Forcieren von Anbieter innerhalb des EWR

# VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

**Dr Axel Anderl, LLM (IT-Law)**

T: +43 1 533 47 95 – 23

F: +43 1 533 47 95 – 50231

E: axel.anderl@dbj.at

**DORDA BRUGGER JORDIS Rechtsanwälte** · Universitätsring 10 · 1010 Wien · www.dbj.at

IFLR European Awards - Austrian Law Firm of the Year 2013
International Law Office - Austrian Client Choice Awards 2012, 2013 and 2014
International Law Office - Information Technology Award for Austria 2014 & 2015
International Law Office - E-Commerce Award for Austria 2012 & 2013