4/2015

INTERVIEW
mit Giovanni Buttarelli,
Europ. Datenschutzbeauftragter

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Cloud-Computing

Neue Arbeitswelt: BYOD in Unternehmen
Karin Ludwig

Cloud-Computing im Anwendungsbereich von Patriot Act, FISA und Freedom Act
Axel Anderl/Nino Tlapak

Interne Nutzung von Cloud-Dienstleistungen in Unternehmen
Judith Leschanz/Verena Ehrnberger

Checkliste Cloud-Computing
Hans-Jürgen Pollirer

Grundrechtswidrigkeit verwaltungsstrafrechtlicher Evidenzen
Michael Suda

Crash-Cam im Auto
Gerald Trieb

Datenschutz-GVO: Die Folgenabschätzung
Hans-Jürgen Pollirer

ISSN 2313-5409

dako.manz.at

MANZ

P.b.b. Verlag Manz 1230 Wien, Gutheil Schoder Gasse 17

Axel Anderl/Nino Tlapak
Rechtsanwalt/Rechtsanwaltsanwärter

Cloud-Computing im Anwendungsbereich von Patriot Act, FISA und Freedom Act

Wann können amerikanische Behörden auf Daten in der Cloud zugreifen? Cloud-Computing birgt neben klaren wirtschaftlichen Vorteilen durch hohe Skalierbarkeit, geteilte Ressourcen und der neben bedarfsbasierten Nutzung auch rechtliche Risiken am vorwiegend von US-Anbietern dominierten Markt. Im folgenden Problemaufriss werden die Einflüsse des „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" („Patriot Act"), „Foreign Intelligence Surveillance Act" („FISA") und „Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act" („Freedom Act") dargestellt.

Rechtsgrundlagen in den USA

Patriot Act, FISA und Freedom Act bauen aufeinander auf und enthalten Bestimmungen, die US-Behörden weitgehende, unmittelbare Datenzugriffe ermöglichen. Der Anwendungsbereich geht dabei wegen der exzessiven Auslegung weit über das US-Territorium hinaus: Die ursprüngliche Stoßrichtung des FISA war die Überwachung ausländischer Geheimdienste. Diese Bestimmungen wurden schließlich durch den Patriot Act, einem Änderungsgesetz zur Terrorismusbekämpfung, erweitert. Die für Cloud-Computing wichtigste Änderung befindet sich in Sec 215 Patriot Act, der § 1861 FISA dahingehend abändert, dass für den Antrag auf Zugang von US-Behörden zu Geschäftsunterlagen aller Art *(„any tangible things")* allein der Verdacht der Verbindung zu Terrorismus und Spionage ausreicht.[1] Damit gibt es – abgesehen von grundrechtlichen Ausnahmen für US-Staatsbürger – de facto keine inhaltliche Beschränkung mehr für die Herausgabeverpflichtung. Die Nichtbefolgung einer Anordnung auf Herausgabe gilt als Missachtung des Gerichts und ist mit Strafe und Bußgeld nach richterlichem Ermessen bedroht.

Wenn Informationen aus Gründen der nationalen Sicherheit benötigt werden, kann ein Datenzugriff auch ohne Zwischenschaltung eines Gerichts erfolgen!

Parallel dazu wurde die Möglichkeit für US-Geheimdienste geschaffen, ohne richterliche Genehmigung oder Information der Betroffenen Datenbanken proaktiv nach Stichwörtern zu durchsuchen. FISA ermöglicht damit generell Zugriffe auf Daten aller Art von Personen, die rechtlich oder tatsächlich in der Lage sind, Zugang zu den begehrten Daten zu erhalten.[2] Sec 505 Patriot Act führt zudem auch zu einem erweiterten Anwendungsbereich der *„National Security Letters"*: So kann ein direkter Datenzugriff auch ohne Zwischenschaltung eines Gerichts erfolgen. Dafür genügt es, dass Informationen für eine Untersuchung zu Zwecken der nationalen Sicherheit benötigt werden.[3] Auch der im Juni erlassene Freedom Act erlaubt der National Security Agency weiterhin, die Festnetz- und Handyanschlüsse aller US-Amerikaner zu überwachen, doch muss die Datenspeicherung in Zukunft durch die jeweilige Telefongesellschaft erfolgen. Nur bei begründetem Terrorverdacht und nach Gerichtsbeschluss dürfen die Daten abgerufen werden. Pikantes Detail: Die Spionage im Ausland ist von der Reform und Einschränkung nicht betroffen. Hier gilt weiter die schrankenlose Überwachung.

US-Recht vs Europäisches Datenschutzrecht

Die weite Auslegung der Herausgabeansprüche durch die amerikanischen Behörden führt dazu, dass auch hinsichtlich in Europa gespeicherter Daten Anordnungen erlassen werden können, wenn eine faktische Zugriffmöglichkeit des Verpflichteten besteht. Nach den US-Gerichten würde der internationale Kampf gegen Terrorismus stets private Interessen und Rechte überwiegen.[4] Dabei ist den US-Gerichten durchaus bekannt, dass einer Zugriffsanordnung in Europa idR das europäische Datenschutzrecht entgegensteht: Daten dürfen nur dann übermittelt werden, wenn aufgrund eines bestimmten Rechtfertigungsgrundes die Geheimhaltungsinteressen der Betroffenen nicht verletzt werden. Genau dies ist in der Praxis aber mangels Zustimmung des Betroffenen (der idR nicht einmal informiert wird) oft nicht der Fall: Eine gesetzliche Ermächtigung zur Datenübermittlung fehlt, weil nur inländische Materiengesetze des Bundes und der Länder eine rechtliche Basis bilden können.[5] Das Anerkennen ausländischer Vorschriften oder Anordnungen würde nämlich dazu führen, dass das europäische Datenschutzniveau untergraben werden könnte.[6] Da keine anderen Rechtfertigungsgründe greifen, ist eine Übermittlung an US-Behörden daher grundsätzlich unzulässig. Selbst bei Zulässigkeit wäre in Österreich aber jedenfalls eine Genehmigung der Datenschutzbehörde einzuholen.[7]

Nach der Auffassung von US-Gerichten überwiegt der Kampf gegen Terrorismus stets private Interessen.

Eine Übermittlung von Daten an Anbieter, von denen bekannt ist oder zu erwarten ist, dass sie personenbezogene Daten an US-Behörden übermitteln, kann daher zu einer gesellschafts- und aufsichtsrechtlichen Haftung führen:[8] Dies gilt insb dann, wenn Da-

[1] *Becker/Nikolaeva*, Das Dilemma der Cloud-Anbieter zwischen US Patriot Act und BDSG, CR 2012/170, 171 mwN. [2] *Becker/Nikolaeva*, CR 2012/170, 171 mwN [3] *Becker/Nikolaeva*, CR 2012/170, 171 mwN. [4] Vgl ua Minpeco SA vs Conticommodity Services Inc; The American Law Institute, Restatement of the Law, Third, Foreign Relations Law of the United States, Sec 442. [5] *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 8 Anm 5. [6] So explizit auch die Art-29-Datenschutzgruppe in ihrer Stellungnahme 1/2006 vom 1. 2. 2006. [7] Siehe §§ 12, 13 DSG. [8] Siehe § 84 AktG bzw § 25 GmbHG.

ten sehenden Auges ohne sachliche Rechtfertigung oder zusätzliche, effektive Sicherheitsvorkehrungen oder Absicherungen überlassen werden.

PRAXISTIPP

Daher ist es wichtig, die unterschiedlichen Risikoszenarien zu evaluieren und den Anbieter für den Anlassfall – auch im Hinblick auf die verarbeitete Datenart und ihren Wert – entsprechend auszuwählen bzw mögliche Gegenmaßnahmen zu etablieren.

Auswahl des Cloud-Anbieters

Aufgrund der Undurchsetzbarkeit von US-Strafen in Europa auf Basis der völkerrechtlichen Grundsätze der Gebiets- und Personalhoheit ist das Risiko eines möglichen Datenzugriffs der US-Behörden in der Praxis von der konzernrechtlichen Verflechtung des Anbieters abhängig:

US-Gesellschaften

Bei einem **Cloud-Anbieter**, der **in den USA niedergelassen** ist und die Daten in den USA oder auch in Europa (ohne Gründung einer Tochtergesellschaft) speichert, sind etwaige US-Anordnungen unmittelbar vollstreckbar. Die drohenden und faktisch durchsetzbaren gerichtlichen Sanktionen gegen das Unternehmen werden idR wohl zu einer Befolgung etwaiger Anordnungen führen. Die dem Unternehmen in Europa drohenden Strafen sind dagegen – auch mangels Vollstreckbarkeit in den USA – kein geeignetes Mittel, um die Übermittlung an US-Behörden zu verhindern. Maximal durch eine effektive Gerichtsstandsvereinbarung oder Schiedsklausel durchsetzbare, hohe Konventionalstrafen für Verstöße gegen das heimische Datenschutzrecht können ein Gegengewicht bilden.

PRAXISTIPP

Problematisch bleibt, dass die Anordnung und Datenübermittlung in der Praxis oft ohne Benachrichtgung des Betroffenen erfolgen, sodass rein faktisch keine Möglichkeit zur Kenntnis- und Rechtsverfolgung besteht.

Etwas ausgewogener stellt sich die Problematik dar, wenn die Daten an eine **europäische Tochter eines US-Unternehmens** überlassen werden. Hier richtet sich die gerichtliche Anordnung in der Regel gegen die Mutter, die sie mit Weisung gegenüber ihrer Tochter durchsetzen müsste. Die Tochter darf diese Weisung grundsätzlich nicht befolgen, weil sie eine nichtige Anhaltung zu rechtswidrigem Verhalten ist.[9] Bei einer Verweigerung drohen allerdings der Mutter direkte Konsequenzen und würden diese im Konzern wohl gegen die Rechtsfolgen in Europa abgewogen werden. Es ist aber naheliegend, dass die Mutter den Druck entsprechend an die Tochter weitergibt (zB Abberufung der Geschäftsführer). Insgesamt besteht ein geringeres Risiko der unzulässigen Übermittlung an US-Behörden als bei einer direkten Datenüberlassung an ein reines US-Unternehmen. Ob eine solche dennoch stattfindet, wird sich vorwiegend danach richten, wie stark die Niederlassung in Europa selbst verankert ist, wie wichtig der europäische Markt und die konkrete Strafandrohung der Anordnung sind. Am Ende des Tages besteht realistischerweise aber ein ernstes Risiko einer unzulässigen Datenübermittlung. Auch hier kann zur Abfederung auf die Schaffung eines Gegenpols durch Konventionalstrafen zurückgegriffen werden.

Europäische Muttergesellschaft mit US-Tochtergesellschaft

Bei diesem Szenario befinden sich die Daten bei einer Muttergesellschaft in Europa, die eine US-Tochter hat. Wenn eine Herausgabe von Daten verweigert wird, droht „nur" der Tochter ein Bußgeld nach US-amerikanischen Recht. Selbst dies ist aber fraglich, weil sie ja rechtlich oder tatsächlich meist nicht in der Lage ist, etwaige gegen die Mutter gerichtete Anordnungen umzusetzen und Zugang zu den begehrten Daten zu erhalten. Das Risiko der unzulässigen Übermittlung an US-Behörden ist in diesem Szenario im Ergebnis zwar nicht ausgeschlossen, aber deutlich geringer. Dazu müsste der US-Markt für das europäische Unternehmen schon eine überwiegende Bedeutung haben oder eine sehr hohe Sanktion drohen.

Gesellschaft ohne Verflechtung in die USA

Befinden sich die Daten bei einem Anbieter mit Sitz in oder außerhalb der EU ohne konzernrechtliche oder persönliche Verbindung zu einem US-Unternehmen, so besteht kein unmittelbares Risiko einer Datenübermittlung an US-amerikanische Behörden. Es fehlt hier an einem dem US-Recht unterworfenen Adressat, gegen den etwaige Strafen und Bußgelder vollstreckbar wären. Offen bleibt die Frage, ob in Einzelfällen der politische Druck stark genug sein kann, um auch solche Gesellschaften direkt oder über den Umweg der jeweiligen Regierung zu einer Herausgabe begehrter Daten zu verpflichten.[10]

Restrisiko Geheimdienstzugriffe

Das bleibende faktische Restrisiko eines versteckten Zugriffs der Geheimdienste auf Daten kann dagegen nie gänzlich ausgeschlossen werden. Derartige Zugriffe können aber auch von einem sorgfältigen Unternehmer nicht vorhergesehen oder abgewendet werden und sie betreffen genauso die vom Unternehmen selbst gespeicherten Daten.

PRAXISTIPP

Sofern die üblichen Datensicherheitsmaßnahmen ergriffen wurden und bei Auslagerung an Anbieter in Ländern mit europäischen Datenschutzstandard, kann bei einem dennoch erfolgten Zugriff der Geschäftsführung kein Vorwurf eines Sorgfaltsverstoßes gemacht werden.

Dako 2015/44

[9] Vgl *Reich-Rohrwig* in *Straube* (Hrsg), GmbHG § 25 Rn 44. [10] Vgl zB die Thematik rund um die Fluggastdaten; dazu *Haidinger*, Speicherung von „Fluggastdaten" (PNR) auch in Europa? Dako 2015, 48.

Zum Thema

Über die Autoren

Dr. Axel Anderl, LL.M., ist Rechtsanwalt, Partner und Leiter des IT/IP und Media Desk bei DORDA BRUGGER JORDIS Rechtsanwälte GmbH.
E-Mail: axel.anderl@dbj.at
Mag. Nino Tlapak, LL.M., ist Rechtsanwaltsanwärter im Team von Axel Anderl bei DORDA BRUGGER JORDIS Rechtsanwälte GmbH.
E-Mail: nino.tlapak@dbj.at