e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Internationaler Datenaustausch

Spionage, Sabotage, Daten-Desaster und der Safe Harbour-K.O

e|s|b Rechtsanwälte

Stuttgart Leipzig Dresden Berlin Prag Warschau

Dr. Jens Bücking,
RA und Fachanwalt für IT-Recht, Datenschutzbeauftragter,
Lehrbeauftragter an der Hochschule für Technik Stuttgart, Prof. assoc. an der E.N.U. Kerkrade, VOI certified expert „Risk Management & Compliance“

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

IT-Abhängigkeit …

- 93% der Unternehmen, die infolge eines Totalausfalls mindestens 10 Tage ohne Rechenzentrum auskommen mussten, meldeten innerhalb eines Jahres Insolvenz an (*National Archives and Records, 2012*)
- 70% der Unternehmen, bei denen es zu katastrophalen Datenverlusten kam, mussten innerhalb von 18 Monaten aufgeben (*Britisches Wirtschaftsministerium, 2012)*
  - Nach anderen Umfragen sind es sogar 90% von Unternehmen, für die der Verlust betriebskritischer Daten dazu führte, dass innerhalb von 2 Jahren der Geschäftsbetrieb eingestellt werden musste (London Chamber of Commerce Research, 2012)
  - Jedoch unterhalten lediglich 35% der kleinen und mittelständischen Unternehmen (KMU) grundlegende Pläne zum Umgang mit IT-Desaster-Szenarien (Gartner, 2013)

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Wirtschaftsspionage: NSA/FBI, GCHQ & Co.

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Wirtschaftsspionage

- Europol, Bundeswirtschaftsministerium, Interpol, BitKom:
- Täglich werden in Deutschland Daten von 20 Mio. Telefonaten und 10 Mio. Internetverbindungen allein durch den US-Geheimdienst NSA gespeichert (2013).
- Deutschland ist zudem das wichtigste Spionageziel in der EU. Dabei geht es nicht nur um Terrorschutz sondern auch um Wirtschaftsinteressen (bekannt seit 2008!).
- Hiervon ist mutmaßlich die Hälfte aller Unternehmen betroffen (BitKom 2015).

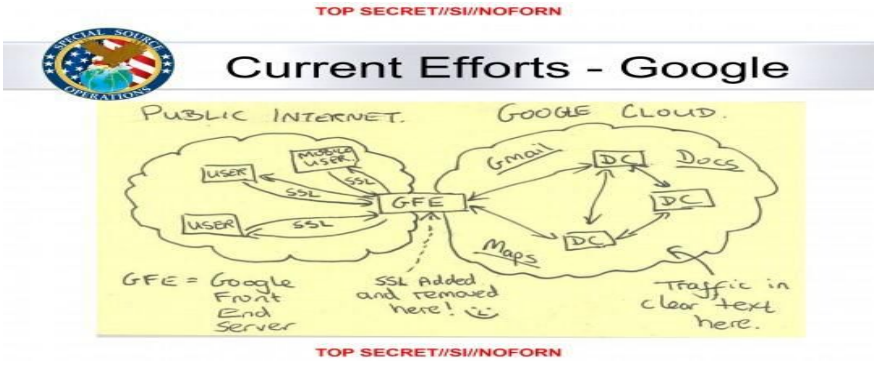
RA Dr. Jens Bücking [jens.buecking@kanzlei.de] © e|s|b Rechtsanwälte ® 2016 - kanzlei.de

“Mutti” knows best

IT-Sicherheit:
“Alternativlos”

NSA, FBI & Co.

- Google Mail, Maps, Docs
  - https://twitter.com/washingtonpost/status/395592546640203776/photo/1
    http://www.zeit.de/digital/datenschutz/2013-10/google-yahoo-nsa
- Eine Folie der NSA, die der Washington Post vorliegt, zeigt, wie bei Google öffentliches Internet und die interne Cloud verbunden sind. Werden Daten übertragen, werden sie ver- oder entschlüsselt.
- An dieser Stelle der Folie zeichnete ein Mitarbeiter ein Smiley.



e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Wirtschaftsspionage/-Sabotage

- Umfragen beziffern Schäden auf über 50 Mrd. Euro, weltweit 290 Mrd.
- Umsatzeinbußen lt. BitKom 2015 infolge
  - Plagiierung geistigen Eigentums
  - Verluste durch Ausfall, Diebstahl oder Beeinträchtigung von
    - IT-Systemen,
    - Betriebsabläufen und
    - Daten
  - (Diebstahl sensibler digitaler Dokumente, sabotierte IT-Systeme und das Abhören elektronischer Kommunikation)
- Laut *Bloomberg* werden gerade auch Anwalts- und Steuerkanzleien gehackt.
- Angegriffen wird überwiegend *nicht*, um an *bestimmte* Informationen zu gelangen
  - die Mehrzahl der Fälle zielt auf reine Sabotage (DoS-Attacken etc.).

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Wirtschaftsspionage-Schland

- High-Tech-Mittelstandsland Deutschland
  - V.a. Mittelständler erleben jeden Tag Spionageangriffe.
    - Mehr als 50% schützt sich unzureichend gegen Angriffe.
      - Angriffe zielen auf die Neuentwicklung von Produkten und Produktionsverfahren (F&E, IP),
      - Ausschreibungen in großen Bau- und IT-Projekten
    - 3.300 EUR/Jahr für Sicherheit (2012, zztl. Tendenz weiter sinkend) ist zu wenig.
    - Aktuellste Daten und Statistiken: http://www.kanzlei.de/publikationen (Verne WP Update 2016)

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Welche Rechtsthemen ergeben sich hieraus?

- Sicherheitsmängel lösen zugleich beim Unternehmen Haftung aus
  - z.B. gegenüber Kunden
  - Mitbewerbern oder vertikal abhängigen Unternehmen (IT-SIG/KRITIS)
  - Dritten (z.B. Nutzern von mit Schadcode infizierten Webseiten (IT-SiG)
- Alternative: Verlagerung in die Cloud (ggf. mit Transport- und Ablageverschlüsselung)?
  - 5 der 10 weltgrößten Serverfarmen in den in Verdacht geratenen USA.
  - Zudem Rechtsrisiken:
  - Safe Harbor K.O.,
  - Angriff Irlands auf Model Clauses,
  - Fragilität von Privacy Shield,
  - Genehmigungsstopp BCR (Binding Corporate Rules = Verbindliche Unternehmensrichtlinien zum Datenschutz (auch) im Konzern)
  - – *die Datenschutzbehörden machen mobil!*

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Rechtsrisiko Datenschutz: Stichproben/Anhörungen

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

Bayer. Landesamt für Datenschutzaufsicht - Postfach 6.05 - 91511 Ansbach

[redacted]

Ihr Zeichen
Ihre Nachricht vom

Unser Zeichen (Bitte bei Antwort angeben)
Ihre Ansprechpartnerin/Ihr Ansprechpartner
[redacted]

E-Mail: [redacted]
Telefon / Fax
0981 53-
[redacted]

Erreichbarkeit
[redacted]

Datum
[redacted]

Aufsichtliche Kontrolle nach § 38 Bundesdatenschutzgesetz (BDSG);

Anlagen
1 Info-Blatt "Firmeninformation zum Datenschutz"
1 Info-Blatt "Der betriebliche Datenschutzbeauftragte"
1 Info-Blatt "Verfahrensverzeichnis und Verarbeitungsübersicht"
1 Info-Blatt "Verpflichtung auf das Datengeheimnis"
1 Checkliste "Datensicherheit"

Sehr geehrte Damen und Herren,

in unserer Funktion als Datenschutzaufsichtsbehörde nach § 38 BDSG für den nicht-öffentlichen Bereich in Bayern prüfen wir laufend stichprobenartig bayernweit die Umsetzung der datenschutzrechtlichen Vorschriften in den Unternehmen.

Zur Durchführung unserer Kontrolltätigkeit (vgl. § 38 Abs. 3 BDSG) bitten wir Sie zunächst um Beantwortung folgender Fragen:

- Wird Altpapier datenschutzgerecht entsorgt?
- Werden E-Mails mit personenbezogenen Daten nur verschlüsselt versendet?
- Wie ist das Unternehmen für die Aufarbeitung einer eventuellen Datenpanne nach § 42a BDSG vorbereitet? Gibt es dazu einen Notfallplan?

Datenübermittlungen, DV im Auftrag durch Dritte: Der Safe Harbor-K.O.

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Neue Pflichten und zugleich Haftungswegweiser:

IT-Sicherheitsgesetz und EU-Cybersicherheits-Richtlinie

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

IT-SIG 2015: Neue Standards für die IT-Sicherheit EU-weit

- Neue – und erweiterte - Sicherheitspflichten durch das IT-SIG:
  - Unterschiedliche Kategorien von Unternehmen (→ KRITIS)
  - Verpflichtungen in Bezug auf die Sicherheit ihrer Systeme und Daten
- Den Betreibern kritischer Infrastrukturen (KRITIS) droht bei Versäumung oder Schlechterfüllung der Pflichtenkataloge des IT-SIG neben empfindlichen
  - Ordnungsmitteln, die über die bloßen Bußgelder hinaus bis zur …
  - Untersagung bzw. Sperrung ihrer Dienste reichen können…

RA Dr. Jens Bücking [jens.buecking@kanzlei.de] © e|s|b Rechtsanwälte ® 2016 - kanzlei.de

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Keine Haftung für Datenschäden/IT-Folgeschäden bei angemessener IT-Sicherheit

- IT-SiG 2015 und NIS-Richtlinie 2016:
  - Neue Security-Standards für KRITIS-Branchen
  - Sicherheitsvorgaben für Internetanbieter (inkl. Suchmaschinen, Cloudprovider, Plattformen)
- Übertragbarkeit auf alle Branchen?
  - Zumindest belastbare Hinweise, was an Mindeststandards geschaffen werden muss, um der Haftung zu entgehen
    - des Unternehmens gegenüber Dritten
    - des Managements gegenüber dem Unternehmen
- Regierungsbegründung zum IT-SiG:
  - Die getroffenen technischen und organisatorischen Vorkehrungen sind zu dokumentieren und nach dem Maßstab des Standes der Technik zu bewerten
  - damit gegebenenfalls ein sachkundiger Dritter die umgesetzten Maßnahmen substanziell überprüfen und ein Gericht zu einem Urteil hinsichtlich der Verantwortlichkeiten im verkehrssicherungspflichtigen oder nebenvertraglichen Bereich gelangen kann.

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Sektoren „Kritischer Infrastrukturen“

Informationstechnik und Telekommunikation

Energie

Wasser

Gesundheit

Transport und Verkehr

Ernährung

Finanz- und Versicherungswesen

RA Dr. Jens Bücking [jens.buecking@kanzlei.de] © e|s|b Rechtsanwälte ® 2016 - kanzlei.de

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

EU-Richtlinie zur Cybersicherheit (NIS-Richtlinie)

- Verabschiedet am 06.07.2016: Neben dem Energie-, Banken-, Verkehrs- und Gesundheitsbereich („Betreiber wesentlicher Dienste“) sollen auch
- Internetdienste wie Suchmaschinen, Cloudanbieter und Plattformbetreiber verpflichtet sein …
  - Maßnahmen zu ergreifen, um ihre Widerstandsfähigkeit gegen Cyberangriffe zu verbessern
  - größere Zwischenfälle den nationalen Behörden zu melden.
- In bestimmten Fällen besteht sogar eine Veröffentlichungspflicht.

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Digitale Dienste nach EU-Richtlinie zur Cybersicherheit (NIS-Richtlinie

Online-Suchmaschinen

Online-Marktplätze

Cloud-Computing-Dienste

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Verkehrssicherungspflicht/Haftung: „Herausgefilterte“ Mindeststandards

- Das IT-SiG nennt „Verschlüsselung“ explizit; zusammen mit der Gesetzesbegründung und der Ansicht der Rechtsexperten kommen hinzu:
- Organisatorisch: Sicherheits- und Notfallkonzepte , d.h. insbes.
  - Es ist ein Sicherheitskonzept auszuarbeiten, das die Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle gewährleistet und das datenschutzrechtliche Trennungsgebot berücksichtigt.
  - In Notfallplänen sind Reaktionen auf Angriffe und Desaster-Szenarien festzulegen und in regelmäßigen Abständen Notfälle testweise zu simulieren.
  - Ein „Information Security Management“ (Sicherheitsorganisation, IT-Risikomanagement etc.) , das kritische Cyber-Assets identifiziert und managt, Maßnahmen zur Angriffsprävention und -erkennung betreibt, und ein Business Continuity Management (BCM) implementiert hat.
  - Wie immer dabei: Der “alte Bekannte” DR/Business Continuity Management (BCM)

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Verkehrssicherungspflicht/Haftung: „Herausgefilterte“ Mindeststandards

- Technisch:
  - Konfigurationsfehlerfreie Internet- und spezielle Sicherheitssoftware (Firewall, Malware-Scanner, Intrusion Detection- und Data Loss Prevention-Systeme etc.)
    - Regelmäßige Sicherheitssoftware-Updates
    - In sensiblen Bereichen (Nutzerzugriffe, Kunden, Webshops, Plattformen zum Infoaustausch) ist spezielle Software zu verwenden, die die Verwundbarkeit des Systems in kurzen Abständen scannt
  - Nutzerdaten, aber auch statistische Daten wie Cookies und die Backups sind stets nach den entsprechenden Standards zu verschlüsseln; Schlüssel und Passwörter sind sowohl gegen innerbetriebliche wie auch gegen Zugriffe von außen zu sichern.
- Organisatorisch:
  - Sicherheits-Policies
  - Administratorenseite: Recherche- und Fortbildungspflicht in Bezug auf neue Bedrohungsszenarien und Sicherheitsupdates

RA Dr. Jens Bücking [jens.buecking@kanzlei.de] © e|s|b Rechtsanwälte ® 2016 - kanzlei.de

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

„Herausgefilterte“ Mindeststandards kompakt

Technisch:

- Verschlüsselung
- Konfigurationsfehlerfreie Internet- und spezielle Sicherheitssoftware (Firewall, Malware-Scanner, Intrusion Detection- und Data Loss Prevention-Systeme etc.)
- Regelmäßige Sicherheitssoftware-Updates
- In sensiblen Bereichen (Nutzerzugriffe, Kunden, Webshops, Plattformen zum Infoaustausch) spezielle Software, die die Verwundbarkeit des Systems in kurzen Abständen scannt
- Nutzerdaten, aber auch statistische Daten wie Cookies und die Backups
  - nach den entsprechenden Standards verschlüsseln;
  - Schlüssel und Passwörter sowohl gegen innerbetriebliche wie auch gegen Zugriffe von außen zu sichern.

Organisatorisch:

- Sicherheitskonzept iSd TOM-Katalogs: Das die Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle gewährleistet und das datenschutzrechtliche Trennungsgebot berücksichtigt.
- Notfallpläne
  - Inkl. Reaktionen auf Angriffe und Desaster-Szenarien
  - in regelmäßigen Abständen Notfälle testweise zu simulieren.
- TOM
  - zu dokumentieren
  - nach dem Maßstab des Standes der Technik zu bewerten
  - damit sachkundiger Dritter die umgesetzten Maßnahmen substanziell überprüfen und ein Gericht zu einem Urteil hinsichtlich der Verantwortlichkeiten im verkehrssicherungspflichtigen oder nebenvertraglichen Bereich gelangen kann.
- „Information Security Management“
  - Sicherheitsorganisation
  - IT-Risikomanagement
  - Inkl. Maßnahmen zur Angriffsprävention und –erkennung
  - Inkl. Business Continuity Management (BCM)
- Administratorenseite: Recherche- und Fortbildungspflicht in Bezug auf neue Bedrohungsszenarien und Sicherheitsupdates

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Cloud-Computing

nach dem Safe Harbor-KO

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT (20.08.2015)

- *Cloud ist Auftragsdatenverarbeitung (ADV)*

- Das Gesetz schreibt eine Reihe von Einzelheiten vor, die zum Schutz der pD darin ausdrücklich festgelegt werden müssen. Von besonderer Bedeutung sind dabei die t.-o. Maßnahmen (TOM/Datensicherheitsmaßnahmen), die der Auftragsdatenverarbeiter zum Schutz der Daten treffen muss.

- Diese Maßnahmen müssen im schriftlichen Auftrag konkret und spezifisch festgelegt werden. Fehlen konkrete Festlegungen hierzu, stellt dies eine Ordnungswidrigkeit dar, die mit Geldbuße bis 50 TEUR geahndet wird.

- Welche vertraglichen Festlegungen zu den TOM getroffen werden müssen, kann nicht pauschal beantwortet werden, sondern richtet sich nach dem Datensicherheitskonzept des jeweiligen Dienstleisters und den von diesem zum Einsatz gebrachten spezifischen Datenverarbeitungssystemen

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Möglichkeiten der Haftungsbegrenzung

- Maßnahmen der IT-Compliance, die vertraglich auf den Cloud-Anbieter übertragen werden müssen, sind daher - nach Möglichkeit durch eine unmittelbare Vertragsstrafe abgesichert - insbesondere

  - Pflicht zur Geheimhaltung und Beachtung von Zugriffsrechten
  - Implementierung verbindlicher Sicherheitskonzepte
  - Einhaltung von IT-Notfallkonzepten
  - Pflichten im Reporting und Auditing
  - Regress und Schadloshaltung bei Schadensfällen
  - Exit-Konzept
  - Sicherheiten
  - Zuverlässigkeit des Anbieters: Vorlage von Zertifizierungen, ggf. Audits etc.

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Es war schon bisher schwer, compliant zu sein – unsichere Drittstaaten und die US-Cloud

- 4 Möglichkeiten, in ansteigender Komplexität
  - Safe Harbor-Abkommen USA/EU (USA als „unsicherer Drittstaat“)
  - EU Model Clauses (Standardvertragsklauseln zur Auftragsverarbeitung ADV)
  - Verbindliche Unternehmensrichtlinien (BCR)
  - Einzelfallabwägung in Bezug auf jede Kategorie von zu übermittelnden Datensätzen
- To do
  - Safe Harbor-Kriterienkataloge mussten vom Datenexporteur selbst überprüft werden, zusätzlich ADV-Vertrag und Zusicherung des TOM-Kataloges erforderlich
  - Beim EU-Standardvertrag: ebenso
  - BCR: ebenso, zudem langwierig, kompliziert, teuer, genehmigungspflichtig, „Sippenhaft“ der EU-Töchter
  - Inzwischen faktischer K.O. durch EuGH-Urteil vom 06.10.2015

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

„Inzwischen faktischer K.O. durch EuGH-Urteil vom 06.10.2015“

- Nach dem Urteil blieben zwar prinzipiell noch 2 Optionen:
  - EU-Standardklauseln, BCR, ABER:
    - Lt. Urteil zweifelhaft, ob ein legaler Datenexport in die USA überhaupt noch als standardisierter Geschäftsprozess ohne eine detaillierte *Einzelfallabwägungsdokumentation* möglich ist:
    - EU-Standardklauseln und BCR: Ausreichend, um den Schutz der pD von EU-Bürgern zu gewährleisten?
      - Bezweifelt u.a. vom Irischen DSB und vom ULD/DSB Schl.-Holstein
        - Patriot Act, Gag Order, National Security Letters
        - Systematische Spähangriffe, Geheimgerichte, kein Rechtsschutz: Grundrechtsverstoß
    - Dann verbliebe den EU-Unternehmen nur die Einzelfallprüfung einer Datenübertragung, oder: „Begründe den Export jedes einzelnen Datensatzes!“

RA Dr. Jens Bücking [jens.buecking@kanzlei.de] © e|s|b Rechtsanwälte ® 2016 - kanzlei.de

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Ersatzlösung „Privacy Shield“?

- EU-Kommission stimmt „Privacy Shield“ am 12.07.2016 zu,
  - so dass sich seit 08/2016 Unternehmen, die Daten zwischen EU/USA transferieren wollen, bescheinigen lassen können, den Anforderungen des PS zu genügen.
  - Vor allem Wirtschaft hatte eine solche schnelle Einigung zwischen der EU/USA herbeigesehnt.
- Also: Neue Rechtsgrundlage zur Übermittlung von pD in die USA, Nachfolger bzw. Ersatz der „gekippten“ SH-Regelung.
  - Idee: Staatliche Zugriffe sollen beschränkt und effektive Schutzmaßnahmen und Aufsichtsmechanismen eingeführt, die Rechte der EU-Bürger wirksam und unter Wahrung rechtlichen Gehörs geschützt werden.
- Führende EU-Datenschützer: PS droht selbes Schicksal wie SH.

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Alternativlos? Angriff auf die „EU model clauses“

- Irland will nach Safe Harbor nun auch die Standardvertragsklauseln vom EuGH überprüfen lassen.
- Wenig Alternativen: Mangels eines Nachfolgers waren Unternehmen wie Facebook auf alternative juristische Grundlagen für die gleiche Praxis ausgewichen, ohne dass der Schutz europäischer Daten in den USA verbessert wurde.
  - Dass diese Alternativen aber auch wirklich rechtmäßig sind, war bereits angesichts der klaren Worte des EuGH zweifelhaft (ähnlich Art. 29-Gruppe)
  - Unterdessen fiel es der EU-Kommission sichtlich schwer, Unterstützung für den „Privacy Shield zu finden“, der eigentlich Safe Harbor rechtssicher ersetzen soll. Die EU-Datenschützer beanstanden die Unzulänglichkeit der Regelung.
  - Wenn Irlands Datenschützer nun vorpreschen, könnte das darauf hindeuten, dass sie nicht an die legale Umsetzung des PS glauben und daher das Augenmerk auf die empfohlene Ausweichlösung der Standardklauseln richten.
- Ein juristischer K.O. droht damit auch den Ausweichoptionen „Privacy Shield“ und „EU-Standardvertragsklauseln“.

Fazit

- Eine DÜ in die USA kann nicht mehr allein auf SH gestützt werden. Soweit DS-Behörden Kenntnis über ausschließlich auf SH gestützte DÜ in die USA erlangen, werden sie diese untersagen.
- Auch die Zulässigkeit der Datentransfers in die USA auf Grundlage von Standardvertragsklauseln oder Binding Corporate Rules (BCR) steht in Frage. Bis zu einer anderweitigen Äußerung der Art. 29-Gruppe kann jedoch davon ausgegangen werden, dass ein Datentransfer auf Basis von Standardvertragsklauseln oder BCR durch die deutschen Behörden nicht sanktioniert wird.
- Die Behörden werden Datentransfers in die USA eigenständig und unabhängig von etwaigen Kommissionsentscheidungen prüfen.
- Neue Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen sollen derzeit nicht erteilt werden.
- Einwilligungen können nur unter engen Bedingungen Grundlage für den Transfer von pD sein. Grundsätzlich darf der Datentransfer jedoch nicht wiederholt, massenhaft oder routinemäßig erfolgen.
- Beim Export von Beschäftigtendaten oder wenn gleichzeitig auch Daten Dritter betroffen sind, kann die Einwilligung nur in Ausnahmefällen eine zulässige Grundlage für eine DÜ in die USA sein.

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Was bleibt noch?

- Man müsste dem Thema IN DIE CLOUD ganz legal ausweichen können!
- Indem man weder eine DÜ noch eine US-DV im Auftrag durchführen lässt sondern die alleinige Funktionsherrschaft über seine Daten behält.
- Im Ergebnis müsste es so sein, dass eine Art Black Box an die Cloud gestellt wird, in der die beim Cloudanbieter gebuchte DV blind die Rechenjobs abarbeitet.
- Kernfrage: Kann die Cloud-Storage-Infrastruktur das Kontroll-Element auf selbem Level wie On-Premise halten?

RA Dr. Jens Bücking [jens.buecking@kanzlei.de] © e|s|b Rechtsanwälte ® 2016 - kanzlei.de

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Hybride Multi-Cloud-Lösung?

- Ziele: Vermeidung der unzulässigen DÜ in Drittstatten, aber auch der Notwendigkeit eines Bündels von ADV mit zB Amazon & Co.
  - Oft ist Kunde KMU → im Massengeschäft sind Cloudbedingungen nicht verhandelbar
- Ziel/Bedingung: Jederzeitige Datenherrschaft
  - Keine „Abwanderung“ von pD – als „DÜ“ im Rechtssinne – „in die Cloud hinein“
  - Speicherort gerade nicht in die Richtung der Public-Cloud zur dauerhaften Datenspeicherung, sondern diametral – das Unternehmen müsste sich die Cloud-Services „aus der Cloud heraus“ ins Haus holen.
  - Dabei würden lediglich der Vorgang des „Computing“ selbst (im flüchtigen Arbeitsspeicher), aber keine Speicherressourcen der Cloud an sich in Anspruch genommen.

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Hybride Multi-Cloud-Lösung

- Reine Infrastrukturnutzung?
  - Keine DÜ, noch nicht einmal ADV,
  - wenn die verantwortliche Stelle sich lediglich fremder Infrastruktur zur Durchführung von DV bedient („verlängerter Arm-Theorie“).
    - Erstanlegung der Admin-Datensätze: Einwilligung im Einzelfall, Abwägung der Interessen
  - Maßgebend ist hier die der jederzeitige Beibehalt der Funktionsherrschaft über den DV-Vorgang

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Hybride Multi-Cloud-Lösung

- „Verlängerter Arm“ der On Premise-IT?
  - Kernfrage: Kann die Hybrid Cloud-Storage-Infrastruktur das Kontroll-Element auf selbem Level wie On-Premise halten?
  - Findet die DV statt, ohne dass die Daten in die Public Cloud des Anbieters verschoben werden?
    - Trennung von „Compute“ und „Store“:
    - Wenn die Daten auf dem eigenen Storage-System des Unternehmens gespeichert bleiben und ansonsten nur eine „blinde“ DV im Arbeitsspeicher stattfindet, könnte argumentiert werden, dass die vollständige Kontrollhoheit gewährleistet ist.
    - Zugriffswege und DV abgeschottet (sichere Verbindung/DV)? Wenn ja:
      - Diese Konstellation unterfällt als technische Verlängerung der unter ausschließlicher Eigenkontrolle stehenden IT-Ressourcen des Unternehmens u.U. nicht den strengen Voraussetzungen an zulässige DÜ in Drittstaaten und
      - stellt sich (wohl) auch nicht als – umfänglich vertraglich und kontrolltechnisch abzusichernde – ADV dar (str.).

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

No way out? Ran an die Cloud!

- „Verlängerter Arm-Theorie“:
  - IT-Infrastrukturerweiterung *an (nicht: in)* die Cloud
    - Cloud-Anwendung wird ins Haus geholt
    - „Black Box“: Blinde DV unter Kontrollhoheit des Unternehmens
    - Trennung Storage and Compute
- Hybride Multi-Cloud-Lösung als ernsthafte Alternative

e|s|b Rechtsanwälte
Stuttgart|Berlin|Dresden|Leipzig|Prag|Warschau

Vielen Dank für Ihr Interesse!

Weitere Informationen unter
www.kanzlei.de