Wirtschaftskammer Österreich

Datenschutz im Fokus
Das neue Datenschutzregime ab Mai 2018

12/13.10.2017

schönherr

austria | bulgaria | croatia | czech republic | european union | hungary | moldova | poland | romania | serbia | slovakia | slovenia | turkey | ukraine

führende
zentraleuropäische
Rechtsanwaltskanzlei

schönherr

austria | bulgaria | croatia | czech republic | european union | hungary | moldova | poland | romania | serbia | slovakia | slovenia | turkey | ukraine

schönherr

austria | bulgaria | croatia | czech republic | european union | hungary | moldova | poland | romania | serbia | slovakia | slovenia | turkey | ukraine

Datenschutz wurde international

- Ressourcenbündelung
- Ausgliederung
- Prozessoptimierung
- Informationsvernetzung
- Produktentwicklung
- etc…

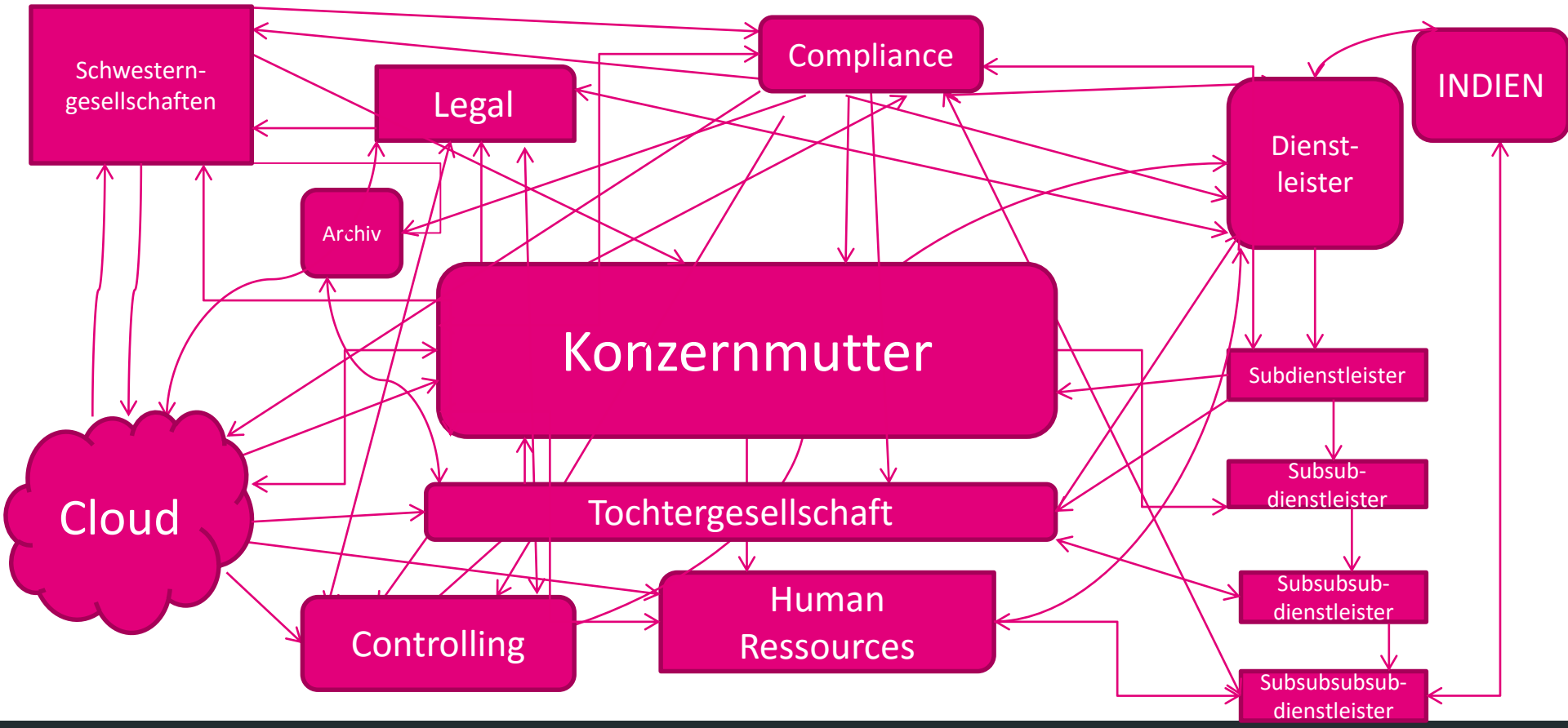
<u>Datenvernetzung!</u>

Die Datenvernetzung…

… zum Zeitpunkt, als das Datenschutzrecht entstanden ist

Die Datenvernetzung...

... heute



Das vernetzte Unternehmen

Die Bestandsaufnahme

- Weites Begriffsverständnis:
  - Internationaler Datentransfer: Datenübermittlung, Datensharing außerhalb Österreich, Datenzugriffe durch Personen außerhalb Österreichs
  - Unternehmen in nahezu allen Geschäftsbereichen betroffen: Server außerhalb Österreichs, Microsoft Outlook, BYOD, etc.
  - Datentransfer außerhalb Europas: Fiktion des unsicheren Drittlands

Das vernetzte Unternehmen

Das „unsichere“ Ausland

- Verschiedene Konzepte zur Sicherstellung eines "sicheren" internationalen Datentransfers:
  - EU-Kommissionsentscheidung: Sicheres Drittland
  - EU-Kommissionsentscheidung: "Safe Harbor"
  - EU-Kommissionsentscheidung: Standardvertragsklauseln
  - Binding Corporate Rules
  - Informierte Einzelzustimmung

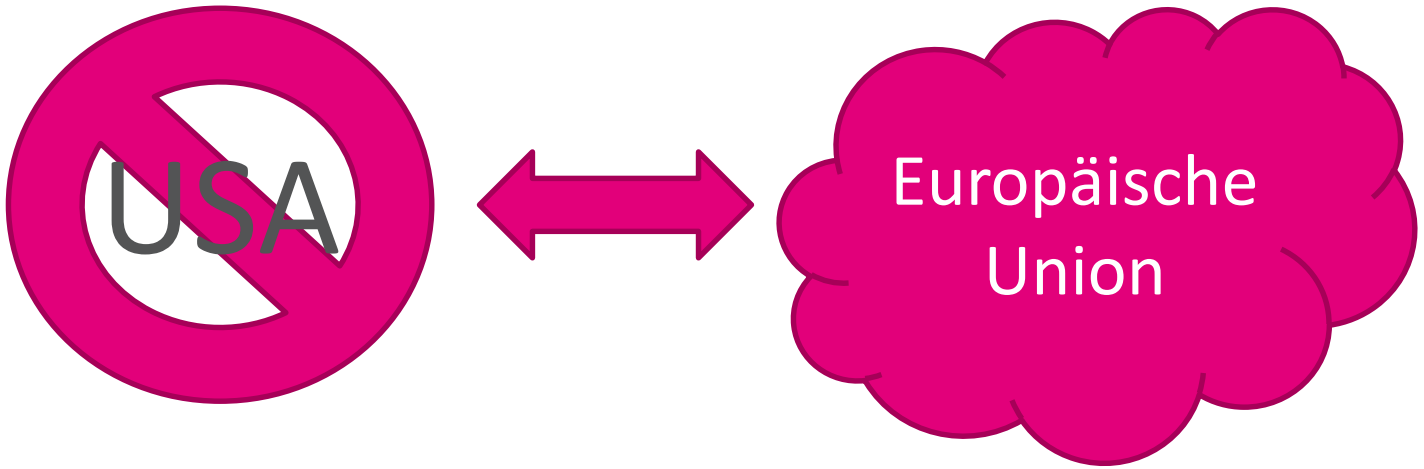
Die Cloud im vernetzten Unternehmen

Rechtliche Bestandaufnahme

- Österreichisches Unternehmen ist „datenschutzrechtlicher Auftraggeber“, dh es trägt die datenschutzrechtliche Verantwortung
- Cloud Provider ist im Regelfall „datenschutzrechtlicher Dienstleister“
- Dienstleister müssen gemäß § 10 DSG Gewähr für eine „rechtmäßige und sichere“ Datenanwendung bieten
- Österreichisches Unternehmen als Auftraggeber trifft diesbezügliche datenschutzrechtliche Verantwortung
- Cloud-Lösungen bedeuten internationale Datentransfers!

Das vernetzte Unternehmen

DER CRASH!



Das vernetzte Unternehmen

Das EuGH Urteil zu "Safe Harbor"

- EuGH RS 362/14 ("Facebook – Entscheidung"):
- EuGH hat nicht festgestellt, dass die USA "unsicher" seien
- Feststellung des EuGH: nationales US-Recht geht den "Safe Harbor" Prinzipien vor
- Kommissionsentscheidung enthielt keine Feststellungen zu den rechtlichen Wirkungen dieses Vorrangs nationalen Rechts
- Daher keine Möglichkeit zur Prüfung der "Adequacy" von Safe Harbor
- Im Prinzip: "Heber" aufgrund fehlender Sachverhaltsfeststellungen

Die Welt nach Safe Harbor

Die Auswirkungen des EuGH Urteils

- Wirkung des EuGH-Judikats geht über Facebook, USA und über "Safe Harbor" hinaus
- Thematik der "mangelnden Feststellung" betrifft alle Kommissionsentscheidungen, insbesondere auch Standardvertragsklauseln (Feststellungen vermutlich nicht möglich)
- Standardvertragsklauseln kürzlich an den EuGH herangetragen (durch den irischen High Court)
- Auch informierte Einzelzustimmung eine bloß theoretische Option: Aufklärung, Freiwilligkeit, Zustimmungswiderruf?

Der „Privacy Shield“

Entstehungsgeschichte & Zweck

- Annahme des „Privacy Shields“ durch die Europäische Kommission am 12.07.2016 als Nachfolgeregelung zu „Safe Harbor“
- Seit 01.08.2016 haben sich bereits mehrere hundert US - Unternehmen „Privacy Shield“ zertifizieren lassen
- Nachfolgekonzept zu „Safe Harbor“ mit verstärkten Garantien:
  - Federal Trade Commission (FTC) bekommt erweiterte Aufsichtsrechte
  - FTC Zusammenarbeit mit europäischen Datenschutzbehörden
  - US-seitiger Behördenzugriff auf Daten unter klar definierten Voraussetzungen, unter Aufsicht und im begrenzten Umfang (EuGH „Konnexitätsgedanke“ bei der Vorratsdatenspeicherung)
  - US-seitiger Ombudsmann wird eingerichtet für behauptete Geheimdienstverstöße
  - Jährliche Überprüfung der Einhaltung dieser Regelungen durch Europäische Kommission und US Department of Commerce

Der „Privacy Shield“

Entstehungsgeschichte & Zweck

- Unternehmensregulierung durch den „Privacy Shield“:
  - Selbstverpflichtung ähnlich „Safe Harbor“
  - Veröffentlichung der Selbstverpflichtungen, Durchsetzungsmöglichkeit der FTC
  - Selbstverpflichtung zur Befolgung von Entscheidungen europäischer Datenschutzbehörden
  - US-Unternehmen kann zur Beschwerdebeantwortung aufgefordert werden
  - Europäische Datenschutzbehörden können Beschwerden an die FTC und an das US Department of Commerce zustellen
  - Kostenloses Verfahren zur „alternativen Streitbeilegung“

Das neue Datenschutzrecht

EU-Datenschutzgrundverordnung (DSGVO)

- Im Mai 2016 wurde die EU-Datenschutzgrundverordnung verlautbart
- Nationale Datenschutzgesetze sollen durch ein einheitliches, unmittelbar anwendbares europäisches Datenschutzrecht ersetzt werden
- Die Datenschutzgrundverordnung sollte eine Modernisierung und Vereinheitlichung des Datenschutzrechts in Europa bewirken
- Inkrafttreten: Mai 2018

Das neue Datenschutzrecht

Bekannte Grundsätze

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datensparsamkeit bzw –minimierung
- Datenrichtigkeit, Datenintegrität und Vertraulichkeit
- Rechenschaftspflicht des Verantwortlichen

Das neue Datenschutzrecht

Bekannte Grundsätze

Verarbeitung ist nur zulässig, wenn eine in der DSGVO normierte Ausnahme bzw Rechtsgrundlage vorliegt (Art 6 DSGVO):

- Einwilligung
- Vertragserfüllung
- Erfüllung einer rechtlichen Verpflichtung
- Wahrung berechtigter Interessen des für die Verarbeitung Verantwortlichen sofern nicht die Interessen des Betroffenen überwiegen
- Lebenswichtige Interessen
- Ausübung öffentlicher Gewalt

Nutzung von Auftragsverarbeitern

Allgemeines zum Auftragsverarbeiter

- Art 28 ermöglicht dem Verantwortlichen die Datenverarbeitung im Auftrag vornehmen zu lassen (Dienstleister).
- Begriff des Auftragsverarbeiters in Art 4 Z 8 definiert als: " *eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des* Verantwortlichen *verarbeitet.* "
- Weiters wird in Art 28 geregelt:
  - Begründung der Auftragsverarbeitung und Rechtmäßigkeitsvoraussetzungen (Auswahlverantwortung)
  - Unterauftragnehmer in der Verarbeitungskette
  - Umfangreiches Pflichtenprogramm für Auftragsverarbeiter

Nutzung von Auftragsverarbeitern

Grundlage der Auftragsverarbeitung

- Grundlage der Auftragsverarbeitung ist ein schriftlicher Vertrag, der die Auftragsverarbeitung konkretisiert.

  - Bindung des Auftragsverarbeiters an den Verantwortlichen (Weisungsbindung).
  - Wesentliche Inhalte der Verarbeitung: Gegenstand und Dauer der Verarbeitung, Art und Zweck, Art der personenbezogenen Daten, Kategorien der Betroffenen, Rechte und Pflichten des Verantwortlichen.
  - Verpflichtung zur Vertraulichkeit bzw Verschwiegenheit.
  - Sicherheitsmaßnahmen iSd Art 32: Sicherung vor unberechtigten Zugriffen von innen und außen.
  - Unterauftragsverarbeitung
  - Unterstützung des Verantwortlichen bei der Wahrnehmung von Betroffenenrechten.
  - Unterstützung des Verantwortlichen bei den Pflichten nach Art 32 bis 36.
  - Löschung oder Rückgabe nach Ende der Auftragsverarbeitung.

Nutzung von Auftragsverarbeitern

Das Konzept der Auftragsdatenverarbeitung in der Cloud

- <u>Rollenverteilung:</u>
  - Verantwortlicher = Cloud-Nutzer
  - Auftragsverarbeiter = Cloud-Anbieter
- Cloud-Nutzer bleibt (als Verantwortlicher) in der Verantwortung der Daten:
  - Auswahlverantwortung
  - Spezifizierung der Pflichten im Auftragsverarbeitungsvertrag
  - Sonstige Grundlagen für internationalen Datentransfer außerhalb des EWR
  - Überbindung der Datenschutzpflichten an Unterauftragsverarbeiter

Internationale Datentransfers

Die Regelungen der DSGVO

- DSGVO regelt "Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen" (Art 44 bis 50 DSGVO)
- Wichtig: Begriff der "Übermittlung" erfasst **jede Form der Offenlegung**, auch an Dienstleister
- Konzept des "**Angemessenheitsbeschlusses**" wird in der DSGVO fortgetragen (Art 45)
- Falls kein "Angemessenheitsbeschluss" vorliegt: Datenübermittlung auf aufgrund "**geeigneter Garantien**" erlaubt (Art 46)
- Bestehen weder ein "Angemessenheitsbeschluss" noch geeignete Garantien, so kann die Übermittlung nur auf den **gesetzlichen Ausnahmekatalog** des Art 49 gestützt werden

Internationale Datentransfers

Grundlage I: Angemessenheitsbeschluss

- EU-Kommission kann für ein **Drittland**, für Gebiete eines Drittlands oder für **spezifische Sektoren** in diesem Drittland die Angemessenheit beschließen (Anwendungsfälle etw Schweiz, "Privacy Shield")
- Folge: Datenübermittlungen **ohne besondere Genehmigung** zulässig
- Art 45 sieht umfangreiche Beschlussvorgaben für die EU-Kommission vor
- Falls die Voraussetzungen für den Angemessenheitsbeschluss nachträglich wegfallen sind, hat die EU-Kommission ihren Angemessenheitsbeschluss (ohne Rückwirkung: § 45 Abs 5) zu widerrufen (wichtig va mit Blick auf "Privacy Shield")
- Von diesem Widerruf werden Datenübermittlungen aufgrund der Art 46 bis 49 "nicht berührt"

Internationale Datentransfers

Grundlage I: Angemessenheitsbeschluss

- Praxisrelevanz:
  - DSGVO anerkennt damit **Parallelkonzepte** für Drittländer (zB Standardvertragsklauseln)
  - Etwa **Absicherung** des "Privacy Shield" durch zusätzlichen Abschluss von Standardvertragsklauseln möglich
  - DSB sieht nach derzeitiger Rechtslage keinen Raum für Standardvertragsklauseln neben dem "Privacy Shield" (Antragsabweisung)
  - Hinkünftig: Rechtliches Interesse ableitbar aus Art 45 Abs 7 DSGVO
  - Abschluss paralleler Standardvertragsklauseln aus heutiger Sicht empfehlenswert

Internationale Datentransfers

Grundlage II: Geeignete Garantien

- Falls kein "Drittlandbeschluss" vorliegt: Übermittlung auf Basis "**geeigneter Garantien**" (Art 46 Abs 2):
  - Rechtsverbindliches und durchsetzbares Dokument zwischen Behörden
  - Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules)
  - Von der EU-Kommission erlassene **Standarddatenschutzklauseln**
  - "**Bottom up**": Von einer nationalen Aufsichtsbehörde angenommene Standarddatenschutzklauseln, die von der EU-Kommission genehmigt wurden
  - Genehmigte Verhaltensregeln (Art 40; Zielsetzung: KMUs)
  - Genehmigter Zertifizierungsmechanismus (Art 42)
  - **Wirkung**: **Keine behördliche Genehmigung erforderlich**

- Alternative "geeignete" Garantien (Art 46 Abs 3):
  - **Ad hoc Vertragsklauseln** (keine Standarddatenschutzklauseln)
  - Verwaltungsvereinbarungen zwischen Behörden
  - **Wirkung: Genehmigung durch die Aufsichtsbehörde erforderlich**

Internationale Datentransfers

Grundlage II: Geeignete Garantien

- Standarddatenschutzklauseln (auch: Standardvertragsklauseln):
  - Dürfen in ihrem Wortlaut nicht verändert werden
  - Können aber in einen Gesamtvertrag eingebettet werden (zB Intra Group Agreement)
  - Gesamtvertrag darf jedoch inhaltlich den Standarddatenschutzklauseln nicht widersprechen
  - Änderungen an den Standarddatenschutzklauseln = Verlust der rechtsprivilegierenden Wirkung, selbst bei einem "Mehr" an Betroffenenrechten
  - Es stehen Standarddatenschutzklauseln für Datenübermittlungen an Auftragsverarbeiter und an Verantwortliche zur Verfügung
  - **Neu**: Unter der DSGVO können auch Auftragsverarbeiter als Datenexporteure Standarddatenschutzklauseln schließen → Praxiserleichterung!

- Neu: Standarddatenschutzklauseln "bottom up":
  - Von der DSB angenommen und von der EU-Kommission geprüft
  - Zweck: **Ergänzung** der bestehenden Standarddatenschutzklauseln bei **besonderem Bedarf** (zB Cloud Services / Sub-Processors)

Internationale Datentransfers

Grundlage II: Geeignete Garantien

- Alternative "geeignete Garantien" - ad hoc Verträge:
  - **Individuelle Gestaltbarkeit**, zB Cloud Lösung bei der Verantwortlicher und Auftragsverarbeiter innerhalb Europas und Sub-Processor außerhalb Europas tätig sind
  - Realistischer Weise jedoch sollte in Art und Wesen Orientierung an Standardschutzklauseln stattfinden, denn:
  - **Genehmigung** durch die DSB erforderlich
- Alternative "geeignete Garantien" – Verhaltensregeln & Zertifizierungen:
  - **Verhaltensregeln** können zB für bestimmte Industrien (etwa Rechtsanwälte) erstellt werden
  - Rechtsverbindlichkeit für den EU-ausländischen Datenempfänger muss gewährleistet sein (zB Gruppenvertrag)
  - Werden von der DSB genehmigt, wirken genehmigungsbefreiend
  - Ebenso: **Zertifizierungskriterien**, deren Rechtsverbindlichkeit bei den EU-ausländischen Datenempfängern gewährleistet werden muss
  - Zertifizierung durch DSB oder akkreditierte Stelle
  - Aktuell wurden noch keine näheren Regelungen hierzu erlassen

Internationale Datentransfers

Grundlage III: Sonstige Konzepte

- Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules):
  - Genehmigung durch zust DSB nach **europaweitem Kohärenzverfahren**
  - DSGVO sieht detaillierte Inhaltsanforderungen vor (Art 47)
- Gesetzliche Erlaubnistatbestände (Art 49) - Auszug:
  - **Einwilligung** der Betroffenen (nach erfolgter Risikoaufklärung)
  - Übermittlung ist für **Vertragserfüllung unbedingt erforderlich** (auch vorvertragliche Pflichten umfasst, jedoch nur "auf Antrag" des Betroffenen)
  - Datenübermittlung liegt im **öffentlichen Interesse** oder ist zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** erforderlich
  - Datenübermittlung zum Schutz **lebenswichtiger Interessen** des Betroffenen, der aus rechtlichen oder psychischen Gründen nicht einwilligungsfähig ist
  - Übermittlung erfolgt aus einem **öffentlichen Register**
  - **Neu:** Falls keine dieser Tatbestände erfüllt ist nicht wiederkehrende Übermittlung mit begrenzter Betroffenenzahl zu zwingenden Interessen des Verantwortlichen erlaubt, wenn Betroffeneninteresse nicht überwiegt und diese informiert wurden
  - Behörde ist diesfalls **zu unterrichten**

Internationale Datentransfers

Praxistipp

- ✓ Verschaffen Sie sich einen Überblick über die **Datenflüsse** in Ihrem Unternehmen
- ✓ Verschaffen Sie sich einen Überblick über Ihre **Dienstleister** (EU-Ausland? Konzernintern?)
- ✓ Prüfen Sie die bisherigen **Rechtsgrundlagen** (Gesetz, überwiegendes Interesse, Zustimmung)
- ✓ Implementieren / adaptieren Sie Ihre bestehenden Datentransfers an die **neuen Konzepte** der DSGVO, etwa:
  - ✓ Parallelkonzept "Privacy Shield" und Standarddatenschutzklauseln
  - ✓ Ad hoc Verträge oder "bottom up" Standarddatenschutzklauseln
  - ✓ Binding Corporate Rules

Vielen Dank!

Günther Leissler

Counsel

T: +43 1 534 37 50227

E: g.leissler@schoenherr.eu

Ihre Begleitung zur Datenschutz-Grundverordnung:
Schönherr Privacy Academy
www.schoenherr.eu

schönherr