DEUTSCH-SCHWEIZERISCHE JURISTENVEREINIGUNG E.V.

# IUS-NEWS 2/2017

**Herausgeber:** DSJV e.V
**Vorstand:**
Monika McQuillen (Präsidentin),
Marc Kotyrba (Finanzvorstand),
Jan Bangert (Generalsekretär)

**Erweiterter Vorstand:**
Dr. Robert Bernet, Dr. Kai Bischoff, Dr. Julia Blind, Dr. Bernd Ehle, Dr. Bernd Hauck, Dr. Dirk Jestaedt, Prof. Dr. Christian Kersting, Dr. Simone Nadelhofer, Dr. Berthold Schanze, Dr. Marc Scheunemann, Michael Schmidt, Martina Ziffels

## Der rechtmäßige Umgang mit Daten in Deutschland: Datenschutzrechtliche Übermittlung

*Die Übermittlung personenbezogener Daten in die USA steht erneut auf dem juristischen und politischen Prüfstand. Das neu geschaffene privacy-shield Abkommen, das den rechtssicheren Datentransfer in die USA sicherstellen soll, wird derzeit mit Klagen vor dem Europäischen Gerichtshof angegriffen. Gleichzeitig droht die EU-Kommission der neuen US-Administration mit einer Kündigung des Abkommens, wenn dessen Inhalte nicht eingehalten würden. Grund genug für Unternehmen und deren Rechtsberater, sich auch angesichts der kommenden europäischen Datenschutzgrundverordnung (DSGVO) mit dem Problem Datenübermittlung zu befassen, nicht nur bei einer Übermittlung in die USA.*

### 1. Die Datenübermittlung als Datenverarbeitung

Regelmäßig stellt der Transfer personenbezogener Daten eine erlaubnispflichtige Datenverarbeitung dar. Das bedeutet, dass auch die bloße Übermittlung von einer Einwilligung oder einer gesetzlichen Erlaubnis gedeckt sein muss, § 4 Abs. 1 des deutschen Bundesdatenschutzgesetzes (*BDSG*). Im Übrigen sind regelmäßig folgende Konstellationen bei der Datenübermittlung zu beachten:

a. Datenübermittlung vs. Auftragsdatenverarbeitung:

Die derzeitige Rechtslage in Deutschland trennt ausdrücklich zwischen einer erlaubnispflichtigen Datenübermittlung und der erlaubnisfreien (und daher privilegierten) Auftragsdatenverarbeitung. Die Abgrenzung kann im Einzelfall schwierig sein, wenn es darauf ankommt, ob dem Datenempfänger eine echte Funktion übertragen wird (dann eher erlaubnispflichige Datenübermittlung)

.

oder bloße, weisungsgebundene Hilfsaufgaben zukommen (dann eher privilegierte Auftragsdatenverarbeitung). Die Auftragsdatenverarbeitung muss weder von einer Einwilligung gedeckt noch muss sie gesetzlich erlaubt sein. Sobald Daten die EU verlassen, ist allerdings auch bei einer Auftragsdatenverarbeitung eine erlaubnispflichtige Übermittlung gegeben, die Privilegierung entfällt.

b. Kein Konzernprivileg:

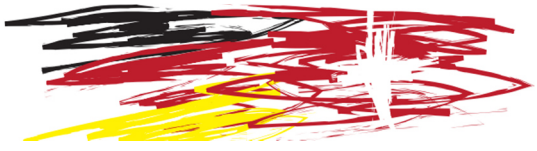
Das Datenschutzrecht kennt kein Konzernprivileg. Das bedeutet, dass auch die konzerninterne Datenübermittlung zwischen Tochtergesellschaften oder von Tochter- an Muttergesellschaft (und umgekehrt) im Ausgangspunkt untersagt ist und daher von einer Einwilligung oder einer gesetzlichen Erlaubnis gedeckt sein muss.

c. Sachverhalte mit Drittstaatenbezug – insbesondere USA:

Ein Dauerbrenner des deutschen und europäischen Datenschutzrechts ist die Übertragung personenbezogener Daten in Drittstaaten, also Staaten außerhalb der EU. Nach dem aufsehenerregenden Safe-Harbor-Urteil des EuGH sorgt mittlerweile das sog. *privacy-shield* Abkommen für ein angemessenes Datenschutzniveau in den USA, sodass eine Datenübermittlung insoweit zulässig sein kann. Solange das Abkommen wirksam und nicht z.B. durch ein Urteil des EuGH für nichtig erklärt wird, werden Unternehmen auf das *privacy-shield* vertrauen können, wenn das Empfänger-Unternehmen nach diesem zertifiziert ist. Auch können weiterhin die EU-Standardvertragsklauseln verwendet werden oder genehmigte sog. Binding Corporate Rules.

## 2. Was tun als Datenübermittler?

Ein Unternehmen, das Daten an ein anderes Unternehmen übermitteln will, hat sich zunächst zu fragen, ob dies im Rahmen einer sog. Auftragsdatenverarbeitung gem. § 11 BDSG erfolgen soll. Liegt eine Auftragsdatenverarbeitung vor, muss sichergestellt sein, dass die nach § 11 BDSG zwingend erforderlichen vertraglichen Vorkehrungen getroffen sind. Liegt nach der rechtlichen Evaluierung dagegen eine erlaubnispflichtige Datenübermittlung vor, ist zu prüfen, ob diese von einer Einwilligung gedeckt oder alternativ gesetzlich erlaubt ist. Hier gelten die allgemeinen datenschutzrechtlichen Maßstäbe. Die Sonderfälle des konzerninternen Datenflusses sowie der Drittstaatenbezug sind stets zu berücksichtigen. Im Übrigen gilt Folgendes: Sobald die Daten rechtmäßig an einen Dritten übermittelt wurden, begründet dies seine datenschutzrechtliche Verantwortlichkeit. Verstößt der Dritte sodann eigenmächtig gegen Datenschutzrecht, ist dies dem ursprünglichen Datenübermittler i.d.R. nicht mehr zurechenbar.



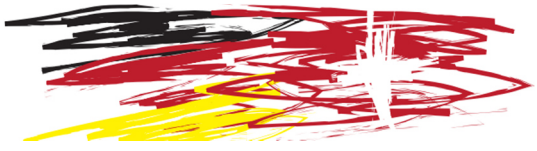
### 3. Was tun als Datenempfänger?

Auch der Datenempfänger wird sich mit datenschutzrechtlichen Fragen auseinandersetzen müssen. Das Erheben, hier das planmäßige In-Empfang-Nehmen sowie das nachfolgende Speichern von Daten, stellt eine erlaubnispflichtige Datenverarbeitung im Sinne des BDSG dar. Eine seltene Ausnahme mag hier für aufgedrängte Datenbestände gelten, die man ohne eigenes Zutun von einem Dritten erhalten hat. Auch der Datenempfänger wird sich daher fragen müssen, ob seine Datenverarbeitung von einer Einwilligung gedeckt oder gesetzlich erlaubt ist. Er kann dabei nicht ohne Weiteres auf die Aus- oder Zusagen des Datenübermittlers vertrauen, denn mit der Datenerhebung wird er die datenschutzrechtlich verantwortliche Stelle samt aller damit einhergehenden Pflichten. Falschangaben mögen im Ernstfall zum Schadensersatz berechtigten, gegenüber Behörden und Betroffenen bleibt der Datenempfänger aber voll in der Pflicht. Es gibt also keinen „gutgläubigen Erwerb“ von personenbezogenen Daten.

### 4. Neuerungen durch die DSGVO?

Ab Mai 2018 gilt mit der DSGVO das neue, einheitliche europäische Datenschutzrecht, das Datenschutzverstöße mit empfindlichen Bußgeldern belegt. Die Neuerungen im Bereich der Datenübermittlung betreffen zum einen die Frage nach der Privilegierung der Auftragsdatenverarbeitung und deren vertragliche Ausgestaltung. Hier ist Anpassungsbedarf erforderlich, sowohl bei der rechtlichen Vorabprüfung als auch bei der Gestaltung der Verträge. Auftragsdatenverarbeiter unterliegen künftig einer deutlich größeren Verantwortung und müssen eigene Verarbeitungsverzeichnisse führen; daneben bleibt der Auftraggeber in der Verantwortung.

Zum anderen ist die Übermittlung in Drittstaaten teils neu gestaltet worden: Hier stellen sich auf erster Stufe die grundlegende Frage, wann eine Übermittlung eine erlaubnispflichtige Datenverarbeitung darstellt – die rechtlichen Vorgaben hierzu werden deutlich unklarer. Auf der zweiten Stufe, der stets notwendigen Absicherung eines angemessenen Datenschutzniveaus im Empfängerland, verschärft die DSGVO einerseits die bisherigen Vorgaben, andererseits gibt sie Unternehmen eine Reihe neuer Instrumente an die Hand: Beispielsweise eine Zertifizierung oder die Genehmigung von Verhaltensregeln als Instrument der Selbstregulierung können im Einzelfall deutlich praktikabler sein, als die bereits bisher zur Verfügung stehenden Optionen von EU-Standardvertragsklauseln oder Binding Corporate Rules. Zum Stichtag im Mai 2018 umgestellt werden muss die Datenübermittlung in Drittländer allerdings nicht, wenn sie schon bislang rechtskonform erfolgte: Solange die Kommission und die



Aufsichtsbehörden nicht tätig werden, gelten Angemessenheitsbeschlüsse wie das *privacy-shield*, die EU-Standardvertragsklauseln und genehmigte Binding Corporate Rules auch nach Inkrafttreten der DSGVO fort.

Zu einer generellen Erlaubnis des konzerninternen Datenflusses hat sich der Verordnungsgeber schließlich nicht durchringen können, auch diese müssen daher weiterhin gerechtfertigt werden. Unternehmen sind in der Verantwortung, die neuen Maßgaben umzusetzen, um auch künftig die Datenübermittlung rechtssicher zu gestalten.

Dr. Kristina Schreiber
kristina.schreiber@loschelder.de

Dr. Simon Kohm
simon.kohm@loschelder.de