Übermittlung personenbezogener Daten ins Ausland

September | 2014

Wichtige Datenschutzinformationen für Ihr Unternehmen

DPN
Datenschutz & Informationssicherheit

Inhalte | Datenschutzinformationen | September 2014

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Fabio Pastars

Liebe Leserin, lieber Leser,

in der letzten Ausgabe haben wir die Auftragsdatenverarbeitung und ihre Bedeutung für den unternehmerischen Alltag behandelt. Dabei haben wir uns bei der Beschreibung der aufgeführten Beispiele auf eine Verarbeitung innerhalb Deutschlands beschränkt.

In dieser Ausgabe gehen wir einen Schritt weiter und thematisieren die Übermittlung von personenbezogenen Daten ins Ausland, denn aufgrund der aktuellen technischen und organisatorischen Entwicklungen verlieren Landesgrenzen im Umgang mit personenbezogenen Daten immer mehr an Bedeutung.

Je nach Art und Umfang der Verarbeitung und Ort des Empfängers der Datenübermittlung kann es sich dabei auch durchaus um eine Datenverarbeitung im Auftrag handeln. Wir zeigen Ihnen aber auch auf, dass es viele Übermittlungen geben kann, die niemals als Auftragsdatenverarbeitung eingestuft werden können, obwohl sie augenscheinlich alle Kriterien dazu erfüllen.

Sehr häufig stellen wir fest, dass die Prüfung auf Zulässigkeit sowie die Ermittlung der Voraussetzungen von Datenübermittlungen außerhalb Deutschlands oftmals knifflig sind und es den verantwortlichen Mitarbeitern aufgrund der Komplexität der Voraussetzungen und der fehlenden Erfahrung teilweise schwer fällt, die richtige Einschätzung zu treffen.

Deshalb greifen wir das Thema in dieser Aufgabe bewusst auf und bieten Ihnen damit eine kompakte Entscheidungshilfe. Leider können wir Ihnen nur einen groben Überblick verschaffen, zu umfangreichen Abhandlungen reicht der verfügbare Platz in dieser Ausgabe nicht aus.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung in Anspruch nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung. Sie erreichen uns unter der Telefonnummer + 49 (2163) 341 371 - 0 oder per E-Mail an f.pastars@dpn-datenschutz.de.

Mit besten Grüßen

Fabio Pastars

DIN EN ISO/IEC 17024 zertifizierter Datenschutzbeauftragter

Wann findet das Bundesdatenschutzgesetz Anwendung?

Das Territorial- oder Sitzlandprinzip

Das Bundesdatenschutzgesetz basiert auf dem Territorial- oder Sitzlandprinzip. Für die Anwendbarkeit des BDSG ist es Voraussetzung, dass die verantwortliche (und Daten verarbeitende) Stelle ihren Sitz in Deutschland hat. Der Ort der Verarbeitung ist dabei unerheblich und kann sich auch außerhalb Deutschlands befinden.

Daraus folgt, dass Unternehmen mit Sitz in der EU oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) den jeweiligen nationalen Gesetzen unterliegen, auch wenn sie personenbezogene Daten in Deutschland erheben, verarbeiten oder nutzen. Grundlage für die jeweiligen nationalen Datenschutzgesetze der EU-Mitgliedsstaaten ist die EU-Datenschutzrichtlinie 95/46/EG. Sie wurde 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr erlassen. Die Mindeststandards für den Datenschutz, die in der Richtlinie beschrieben sind, müssen von allen EU-Mitgliedsstaaten durch Umsetzung in nationales Recht sichergestellt werden.

Anwendung findet das BDSG aber wiederum dann, wenn EU/EWR-Unternehmen eine Niederlassung in Deutschland betreiben und durch diese personenbezogene Daten im Inland erheben, verarbeiten oder nutzen.

Das BDSG gilt aber auch dann, wenn eine in einem Drittstaat niedergelassene Stelle für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten auf Mittel zurückgreift, die sich in Deutschland befinden. Ein klassisches Beispiel ist der Server, auf dem personenbezogene Daten gespeichert und zum Abruf oder zur Nutzung bereitgehalten werden. Dabei genügt es, wenn die in einem Drittstaat niedergelassene Stelle bestimmenden Einfluss auf den Server hat, ohne dass dieser in ihrem Besitz oder Eigentum steht. Die rechtliche Zuordnung des Servers ist irrelevant.

Davon ausgeschlossen ist eine bloße Übermittlung von Daten, wie sie etwa bei E-Mail Servern geschieht.

Definition Ausland | Angemessenheit des Datenschutzniveaus

Ausland ist nicht gleich Ausland

Die Bedeutung des Wortes „Ausland“ bedarf sicherlich keiner näheren Erläuterung, damit ist eindeutig jeder Ort außerhalb der Bundesrepublik Deutschland gemeint. Dennoch gibt es tatsächlich Unterschiede aus Sicht des Bundesdatenschutzgesetzes.

EU / EWR

Hierunter fallen alle EU-Mitgliedsstaaten sowie alle Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (Island, Norwegen und Liechtenstein). Durch die Umsetzung der EU-Datenschutzrichtlinie ist in allen zuvor genannten Staaten von einem einheitlichen Datenschutzniveau auszugehen. Allgemein spricht man daher von einem einheitlichen und „angemessenen Datenschutzniveau“ innerhalb der EU bzw. EWR. Datenverkehr in eines dieser Länder ist wie eine Übermittlung im Inland anzusehen und wird auch als solche nach den Grundsätzen des § 4b Absatz 1 BDSG behandelt.

Drittstaaten mit angemessenem Datenschutzniveau

Es gibt Staaten, für die die EU-Kommission ein den EU-Staaten vergleichbares Datenschutzniveau festgestellt hat. Für Unternehmen mit Sitz in einem dieser Staaten ist daher ebenfalls von einem angemessenen Datenschutzniveau auszugehen. Folgende Staaten hat die EU-Kommission bis heute als angemessen eingestuft: Andorra, Argentinien, Australien, Kanada, Schweiz, Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland und Uruguay.

Drittstaaten ohne angemessenes Datenschutzniveau

Alle sonstigen Staaten, wie zum Beispiel USA, Russland und Indien, gelten aufgrund des geringen Datenschutzniveaus als unsicher. Eine Übermittlung in solche Staaten muss unterbleiben, wenn der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat, was aufgrund des geringen Datenschutzniveaus anzunehmen ist.

Ausnahmen trotz fehlender Angemessenheit des Datenschutzniveaus

§ 4c BDSG – Ausnahmen

Eine Übermittlung personenbezogener Daten in Staaten ohne angemessenes Datenschutzniveau ist jedoch unter einer der folgenden Voraussetzungen zulässig:

- ✓ Es liegt eine Einwilligung des Betroffenen vor. Er muss ausreichend über seine betroffenen Daten sowie das bestehende Datenschutzniveau des Empfängers der geplanten Übermittlung informiert werden. Nur dann gilt seine Einwilligung, die ausnahmslos schriftlich erfolgen sollte, als zulässig.

- ✓ Die Übermittlung ist zum Abschluss oder zur Erfüllung eines Vertrages mit dem Betroffenen notwendig. Auch hier muss er vorab hinreichend über die geplante Übermittlung und den Zweck informiert werden. Typische Beispiele sind Hotelreservierungen oder Warenbestellungen in Drittstaaten.

- ✓ Die Übermittlung ist zum Abschluss oder zur Erfüllung eines Vertrags erforderlich, der von der verantwortlichen Stelle im Interesse des Betroffenen mit einem Dritten geschlossen wurde oder geschlossen werden soll.

- ✓ Die Übermittlung ist für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich.

- ✓ Die Übermittlung ist für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich.

- ✓ Die Übermittlung erfolgt aus einem Register, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Erforderliche Prüfung in zwei Stufen

Der Düsseldorfer Kreis hat im September 2013 einen Beschluss verfasst, der beschreibt, wie eine Prüfung der Zulässigkeit von Übermittlungen personenbezogener Daten in Drittstaaten erfolgen muss.

1. Stufe

Zunächst muss die bloße Zulässigkeit der Übermittlung personenbezogener Daten geprüft werden. Zulässig ist eine Übermittlung mit Einwilligung des Betroffenen oder wenn eine andere Rechtsvorschrift die Übermittlung vorsieht oder erlaubt. Hier finden die §§ 28 und 32 BDSG (für eigene Geschäftszwecke und Beschäftigtendatenschutz) Anwendung. Zu beachten ist, dass auch im Falle einer vorliegenden Auftragsdatenverarbeitung nach § 11 BDSG die Übermittlung selbst zulässig sein muss.

Besonderheit Auftragsdatenverarbeitung und Drittstaat

In § 3 Abs. 8 BDSG heißt es: *„Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen."* Daraus folgt, dass eine Übermittlung an Stellen in Drittstaaten aus Sicht des BDSG nicht als „echte" Auftragsdatenverarbeitung gelten kann und deshalb immer die Einwilligung der Betroffenen vorliegen oder eine andere Rechtsvorschrift die Übermittlung rechtfertigen muss. Dennoch muss die verantwortliche Stelle auch dabei die Anforderungen des § 11 BDSG erfüllen, denn andernfalls stünden die Betroffenen bei einer Verarbeitung ihrer Daten im Drittstaat schlechter als bei einer Verarbeitung im Inland bzw. im EWR.

2. Stufe

Auf der zweiten Stufe gilt es zu prüfen, ob im Land des Empfängers ein angemessenes Datenschutzniveau herrscht oder ob eine der Ausnahmen nach § 4c BDSG Anwendung finden kann.

Ergebnis

Zulässig ist eine Übermittlung nur dann, wenn auf beiden Stufen ein positives Ergebnis ermittelt werden kann.

Angleichung durch ausreichende Garantien

Wenn im Land des Empfängers kein angemessenes Datenschutzniveau besteht, kann dies nach § 4c Abs. 2 BDSG durch ausreichende Garantien ausgeglichen werden. Dabei können vielfältige Möglichkeiten zur Anwendung kommen. Nachfolgend finden Sie eine Übersicht der gängigsten Lösungen.

1. Individuelle Vertragsregelungen

Zwischen den betroffenen Parteien kann ein individueller Vertrag über den Umgang mit personenbezogenen Daten geschlossen werden. Dieser muss durch die Aufsichtsbehörde genehmigt werden, wobei es sich um einzelne Übermittlungen oder bestimmte Arten von Übermittlungen handeln kann.

2. Binding Corporate Rules (BCR)

Verbindliche Unternehmensregelungen sind ebenfalls als individuelle Regelungen anzusehen und eher in multinationalen Konzernen anzutreffen. Diese können dann sinnvoll sein, wenn Teile des Konzerns in Ländern ohne angemessenem Datenschutzniveau agieren und konzernweit einheitliche Regelungen statt vieler individueller Verträge gelten sollen.

Charakteristisch für BCR ist, dass sie für alle beteiligten Unternehmen rechtlich verbindlich vereinbart werden und im Innenverhältnis als Handlungsanweisungen gegenüber den Mitarbeitern umgesetzt sein müssen. Die Entwicklung solcher Regelungen, die juristischer Beratung bedürfen, ist sehr kostenintensiv und die notwendige Genehmigung durch die Aufsichtsbehörde sicherlich auch sehr zeitaufwendig.

3. EU-Standardvertragsklauseln

Eine weitere Möglichkeit zur Herstellung eines angemessenen Datenschutzniveaus besteht in der Nutzung der EU-Standardvertragsklauseln, die durch Beschluss der EU-Kommission zuletzt im Februar 2010 aktualisiert wurden.

Sie finden Anwendung, wenn personenbezogene Daten in Drittländern verarbeitet werden sollen, in denen kein angemessenes Datenschutzniveau herrscht. Die Auftragsvergabe kann durch Anwendung dieser Klauseln ein angemessenes Datenschutzniveau erreichen. Bei unverändertem Abschluss zwischen Datenexporteur und Datenimporteur ist keine Genehmigung durch die Aufsichtsbehörde notwendig, damit ist eine Auftragsvergabe relativ schnell und einfach umsetzbar.

Zu beachten ist aber, dass der Abschluss der EU-Standardvertragsklauseln lediglich zur Herstellung eines angemessenen Datenschutzniveaus führt. Darüber hinaus ist für die eigentliche Beauftragung eine separate Datenschutzvereinbarung notwendig, die inhaltlich den Anforderungen des § 11 BDSG genügen muss. Da das BDSG kein Konzernprivileg kennt, gilt dies auch für Unternehmen innerhalb eines Konzerns, sofern keine Binding Corporate Rules existieren.

Der Auftragnehmer kann unter bestimmten Voraussetzungen auch Subunternehmer einschalten. So muss der Auftraggeber zuvor in die Beauftragung eines Subunternehmers eingewilligt haben und die Bedingungen der EU-Standardvertragsklauseln müssen an den Unterauftragnehmer vertraglich weitergereicht werden. Er muss also dieselben Pflichten auferlegt bekommen wie der Auftragnehmer. Dies kann gewährleistet werden, indem der Unterauftragnehmer in den Vertragsschluss einbezogen wird und auf den EU-Standardvertragsklauseln zwischen Datenexporteur und Datenimporteur mitunterzeichnet.

Angemessenes Datenschutzniveau in Drittstaaten

4. Safe Harbor - Sonderfall USA

Auch die USA gelten als Drittland ohne angemessenes Datenschutzniveau, da dort mangels gesetzlicher Normen keine ausreichenden Garantien im Sinne des Datenschutzes bestehen. Um europäischen Unternehmen dennoch eine Übermittlung von personenbezogenen Daten in die USA zu ermöglichen, hat die EU-Kommission im Juli 2000 das Safe-Harbor-Abkommen mit den USA vereinbart. US-Unternehmen können sich freiwillig auf die Grundsätze dieses Abkommens verpflichten. Durch diese Selbst-Zertifizierung wird für diese Unternehmen ein angemessenes Datenschutzniveau angenommen.

Allerdings reicht es für das Daten exportierende Unternehmen nicht aus, sich auf die Behauptung einer gültigen Safe-Harbor-Zertifizierung des importierenden Unternehmens zu verlassen. Die Kontrollpflicht nach § 11 Abs. 4 BDSG ist auch hier anzuwenden, so dass der Datenexporteur sich mindestens vergewissern muss, ob die Zertifizierung beim Datenimporteur tatsächlich vorliegt und noch Gültigkeit besitzt. Weiterhin muss sich der Datenexporteur nachweisen lassen, dass das importierende Unternehmen gegenüber den Betroffenen seinen Informationspflichten, die in den Safe-Harbor-Principles festgelegt sind, nachkommt.

Die Informationspflichten erstrecken sich auf die Information des Betroffenen über den Zweck der Erhebung und Verwendung, über die Kontaktmöglichkeiten zum Datenimporteur, über eine eventuelle Weitergabe der Daten an Dritte und über die verfügbaren Mittel zur Einschränkung der Datenverwendung und -weitergabe.

Die Prüfung der genannten Sachverhalte muss das exportierende Unternehmen dokumentieren und nachweisen können.

In der Praxis zeigen sich hier jedoch oft Mängel, so dass es sinnvoller sein kann, die Übermittlung durch den Abschluss von EU-Standardvertragsklauseln oder verbindlichen Unternehmensregelungen zu legitimieren. Aber auch hier gilt, dass die Safe-Harbor-Zertifizierung lediglich zur Herstellung eines angemessenen Datenschutzniveaus führt und für die eigentliche Beauftragung eine separate Datenschutzvereinbarung nach § 11 BDSG notwendig ist.

PRISM und Patriot Act

Aktuelle Entwicklung seit PRISM

Als Konsequenz des Abhörskandals durch die NSA hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits im Juli 2013 erklärt, Übermittlungen personenbezogener Daten in die USA zukünftig nicht mehr zuzustimmen, bis die NSA-Affäre geklärt ist. Dies betrifft jedoch nur die zustimmungspflichtigen Lösungen wie individuelle vertragliche Regelungen oder Binding Corporate Rules.

Zwar können die Aufsichtsbehörden auch Datenübermittlungen aussetzen, die auf Safe Harbor oder den EU-Standardvertragsklauseln basieren. Dies aber immer nur für einzelne Übermittlungen eines Unternehmens und nur dann, wenn das Risiko einer Verletzung der Vorgaben als hoch eingestuft werden muss.

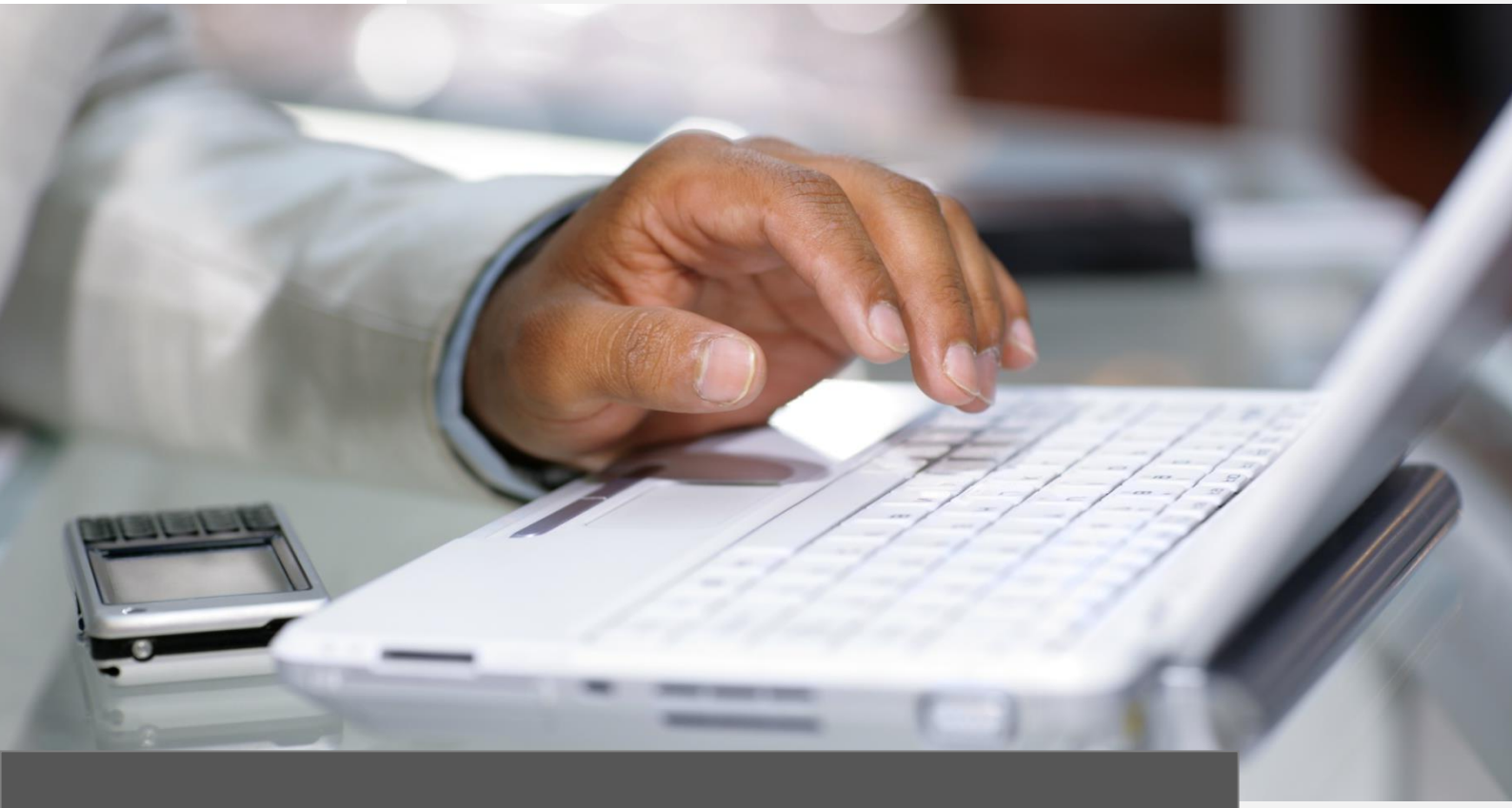
Grundsätzlich ist es jedoch legitim oder geboten, sich aktuell tiefgründige Gedanken über die tatsächliche Sicherheit von US-Unternehmen zu machen und solche Vorhaben kritischer zu prüfen.

Patriot Act – Nutzung von US-Clouds deutlich erschwert

Dieses US-Bundesgesetz ist 2001 zur Bekämpfung von Terrorismus erlassen worden und ermöglicht den US-Geheimdienstbehörden auf Anforderung Zugang zu allen bei US-Unternehmen und auch deren weltweiten Tochterunternehmen gespeicherten Daten zu erhalten, unabhängig des physikalischen Standortes der Daten und den gesetzlichen Bestimmungen, die für die jeweilige verantwortliche Stelle gelten.

Deutsche Unternehmen sind jedoch an das BDSG gebunden und müssen sicherstellen, dass die von ihnen verarbeiteten Daten Dritten nicht unbefugt zur Kenntnis gelangen. Das können sie zum Beispiel in der Form sicherstellen, dass ausschließlich Cloud Dienste genutzt werden, die eine Speicherung der Daten innerhalb des EWR garantieren und nicht zu einem US-Unternehmen gehören.

September | 2014



Impressum

DPN
Datenschutz & Informationssicherheit

DPN Datenschutz GmbH & Co. KG
Hochstraße 2
41379 Brüggen
Tel.: +49 (2163) 341 371 - 0
Fax: +49 (2163) 341 371 - 9
Web: www.dpn-datenschutz.de
E-Mail: info@dpn-datenschutz.de

Amtsgericht Krefeld, HRA 6213
Ust-IdNr.: DE275528415
p.h.G.: DPN Verwaltung GmbH
Geschäftsführer: Fabio Pastars
Amtsgericht Krefeld, HRB 14208

Redaktion:
Fabio Pastars

Bildnachweise:
Diese Datenschutzbroschüre wurde für die ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei der Firma ccvision.de gekauft und lizensiert.