

Teilnehmerscript Datenverarbeitung im Ausland



Inhaltsverzeichnis

Datenverarbeitung im Ausland	1
„Verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG	1
Datenverarbeitung im Auftrag	1
Weitergabe von Daten an Dritte im Ausland	2
Was ist ein „angemessenes Schutzniveau“?	2
Übermittlung von personenbezogenen Daten trotz ungenügendem Datenschutzniveau im Empfängerstaat	3
Sonderfall: Konzernmutter in den USA	3
Datenschutzniveau in den USA	3
Das „Safe-Harbour“-Abkommen	4
Links auf Details:	4
Möglichkeiten der Mitbestimmung	5

Datenverarbeitung im Ausland

Sehr häufig erleben wir, dass die Datenverarbeitung nicht im Betrieb selbst, sondern woanders erledigt wird, und dieses „Woanders“ ist nicht selten eine Stelle im Ausland. Das geschieht meistens in einer dieser beiden Konstellationen:

- Das Unternehmen in Deutschland leistet die Datenverarbeitung nicht selbst, sondern beauftragt ein anderes Unternehmen (im Ausland) damit, die Datenverarbeitung zu leisten.
- Das deutsche Unternehmen ist eine Tochter innerhalb eines internationalen Konzerns. Die Datenverarbeitung wird innerhalb des Konzerns von einem anderen Unternehmen, das aber nicht der deutschen Konzerntochter, sondern der im Ausland ansässigen Konzernmutter untersteht, oder von der Konzernmutter selbst geleistet.

„Verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG

§ 3 Abs. 7 BDSG definiert die „verantwortliche“ Stelle als Person oder Stelle, die personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt oder dies durch andere tun lässt.

Die Definition der „Stelle“ im BDSG stimmt nicht unbedingt mit der des „Betriebes“ i. S. d. §§ 1 und 4 BetrVG überein. Als „Stelle“ i. S. d. BDSG wird eine Instanz mit eigener Rechtspersönlichkeit verstanden, worauf ja auch der Begriff „Person“, der in § 3 Abs. 7 BDSG ausdrücklich genannt wird, hinweist. Eine „verantwortliche Stelle“ im Sinne des Datenschutzes ist daher vor allem die juristische Person, also das Unternehmen, und weniger der einzelne Betrieb, der vielleicht nur ein Teil innerhalb des Unternehmens ist.

Insofern ist die juristische Person, also z. B. die einzelne GmbH oder AG innerhalb des Konzerns, verantwortlich für den Datenschutz. Andere juristische Personen, auch wenn sie sich z. B. als Schwesterunternehmen im gleichen Konzern befinden, oder auch die Konzernmutter sind andere Stellen, an die Daten ggf. weitergegeben werden.

Datenverarbeitung im Auftrag

Wenn der erste der beiden oben geschilderten Fälle zutrifft, dann ist § 11 BDSG anzuwenden: Die verantwortliche Stelle – also das Unternehmen in Deutschland als Auftraggeber – muss dafür sorgen und ist dafür verantwortlich, dass die Stelle, an die die personenbezogenen Daten weitergegeben werden, die Vorschriften des Bundesdatenschutzgesetzes und anderer Gesetze einhält.

Dies gilt unabhängig vom Standort der Stelle, also z. B. auch, wenn es sich um einen Dienstleister im Ausland handelt. Hier macht das BDSG aber in § 3 Abs. 8 einen Unterschied zwischen solchen Stellen, die im EWR oder außerhalb des EWR angesiedelt sind: Stellen innerhalb des EWR sind nicht „Dritte“ im Sinne des BDSG, an solche Stellen ist eine Weitergabe personenbezogener Daten problemlos möglich.

Für alle anderen Staaten sind die Anforderungen höher: Hier ist § 4b Abs. 2 BDSG anzuwenden, in dem in Satz 2 bestimmt wird, dass die Übermittlung nur stattfinden darf, wenn bei der empfangenden Stelle ein „angemessenes Datenschutzniveau“ gewährleistet ist. Das kann dadurch gewährleistet sein, dass die verantwortliche Stelle, also der Auftraggeber in

Deutschland, durch geeignete Maßnahme, eine umfassende vertragliche Regelung und angemessene Überprüfung etc. dafür sorgt, dass dies der Fall ist.

Voraussetzung für die Anwendbarkeit des § 11 BDSG ist aber, dass die verantwortliche Stelle in Deutschland der Stelle, an die die Daten weitergegeben werden, überhaupt Vorschriften machen kann. Dass dies unmöglich ist, ist z. B. dann anzunehmen, wenn es sich dabei um die im Ausland ansässige Konzernmutter handelt, denn die macht ja umgekehrt der deutschen Konzerntochter Vorschriften.

Eine weitere Voraussetzung ist die, dass die Daten allein zu dem Zweck an die andere Stelle weitergegeben werden, im Auftrag der verantwortlichen Stelle in Deutschland zu handeln, also z. B. die Lohn- und Gehaltsbuchhaltung zu leisten oder andere Leistungen zu erbringen, von der ausschließlich die verantwortliche Stelle als Auftraggeberin profitiert.

Wenn die personenbezogenen Daten aber z. B. an die Konzernmutter oder einen von der Konzernmutter beauftragten Dienstleister weitergegeben werden, muss man in aller Regel davon ausgehen, dass die Konzernmutter eigene Interessen bei der Nutzung der Daten verfolgt, und die deutsche Konzerntochter nicht die alleinige Hoheit darüber hat, was mit den Daten geschieht.

In diesen Fällen ist eine Anwendung des § 11 BDSG nicht möglich, und man muss von einer Weitergabe der Daten an Dritte i. S. d. § 3 Abs. 8 BDSG ausgehen, für die § 4b BDSG dann anzuwenden ist, wenn dieser Dritte im Ausland sitzt.

Weitergabe von Daten an Dritte im Ausland

Bei der Weitergabe von Daten an Dritte im Ausland wird ebenfalls unterschieden zwischen Empfängern innerhalb des EWR und solchen außerhalb des EWR. Hier ist noch einmal anzumerken, dass „Dritte“ i. S. d. BDSG auch die Konzernmutter oder ein Schwesterunternehmen innerhalb des Konzerns sind. „Verantwortliche Stelle“ ist die juristische Person bzw. die Niederlassung in Deutschland, die Weitergabe an eine andere juristische Person ist in jedem Fall eine Weitergabe an Dritte.

Für die Weitergabe von Daten an Stellen innerhalb des EWR gilt § 4b Abs. 1 BDSG: Die Weitergabe ist dann zulässig, wenn dies im Rahmen der Verarbeitung und Nutzung der Daten auf der Grundlage der §§ 28 bis 30 BDSG geschieht, und die Erhebung, Speicherung etc. der Daten nach diesen Paragraphen zulässig ist. Für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Verhältnis zwischen Arbeitgeber und Arbeitnehmer ist hier vor allem § 28 BDSG von Bedeutung.

Sobald aber Daten an Stellen außerhalb des EWR weitergegeben werden sollen, greift wieder die verstärkte Schutzwirkung des § 4b Abs. 2 Satz 2 BDSG: Danach hat eine Übermittlung dann zu unterbleiben, wenn die empfangende Stelle, bzw. der Staat, in dem diese Stelle sitzt, kein „angemessenes Schutzniveau“ hat.

Was ist ein „angemessenes Schutzniveau“?

Die Vorschrift, dass eine Übermittlung zu unterbleiben hat, wenn bei der empfangenden Stelle ein „angemessenes Schutzniveau“ nicht gewährleistet sei, ist, gelinde gesagt, etwas vage. „Angemessen“ bedeutet jedenfalls noch nicht „gleichwertig“. Es ist in der Praxis jedoch kaum möglich, zu beurteilen, ob ein im Staat, in dem die empfangende Stelle sitzt, ggf. gültiges Regelwerk zum Datenschutz im Vergleich zum Datenschutzniveau der EU gleichwer-

tige oder zumindest angemessene Vorschriften enthält, oder ob die empfangende Stelle selbst sich einem Regelwerk unterwirft, das angemessen ist.

Es gibt hier zwei Lösungsmöglichkeiten, um die Angemessenheit des Schutzniveaus im Staat, in dem die empfangende Stelle sitzt, zu beurteilen:

- Lt. der EG-Richtlinie zum Datenschutz kann die EU-Kommission entscheiden, dass ein Drittstaat ein angemessenes Datenschutzniveau hat. Diese Entscheidung ist für die EU-Mitgliedstaaten bindend. Bisher ist diese Entscheidung in Bezug auf die Argentinien, die Inseln Guernsey und Man, Kanada und die Schweiz ergangen. Eine Übermittlung personenbezogener Daten in diese Staaten ist also zulässig.
- Ein angemessenes Schutzniveau ist dann anzunehmen, wenn der Drittstaat die Datenschutzkonvention des Europarates ratifiziert und Instanzen zu ihrer praktischen Umsetzung bestellt hat.

Übermittlung von personenbezogenen Daten trotz ungenügendem Datenschutzniveau im Empfängerstaat

Wenn im Drittstaat, in dem die empfangende Stelle ihren Sitz hat, kein angemessenes Datenschutzniveau sichergestellt ist, so kann unter gewissen Umständen, nämlich in Anwendung von § 4c BDSG, dennoch eine Übermittlung von personenbezogenen Daten an diese Stelle zulässig sein. Wir zählen hier nur die Fälle auf, die im Zusammenhang mit einem Arbeitsverhältnis von Bedeutung sind.

- Wenn der Betroffene seine Einwilligung gegeben hat (§ 4c Abs. 1 Nr. 1 BDSG).
- Wenn dies erforderlich ist, um einen Vertrag zwischen dem Betroffenen und der verantwortlichen Stelle zu erfüllen (§ 4c Abs. 1 Nr. 2 BDSG). Das rechtfertigt jedoch noch nicht, dass Daten z. B. an die Konzernmutter übermittelt werden, weil dort die Gehaltsabrechnung stattfindet: Es ist ja nicht erforderlich, dass die Gehaltsabrechnung im Ausland stattfindet; die verantwortliche Stelle könnte sie ja auch selbst leisten.
- Wenn die Aufsichtsbehörde die Übermittlung genehmigt, weil die verantwortliche Stelle ausreichende Garantien hinsichtlich der Wahrung der Persönlichkeitsrechte der Betroffenen gibt, z. B. durch geeignete Verträge oder dadurch, dass die empfangende Stelle verbindliche Regelungen einhält (§ 4c Abs. 2 BDSG). Hierzu gibt es von der EU-Kommission genehmigte Standardvertragsklauseln.

Sonderfall: Konzernmutter in den USA

Ein Sonderfall liegt vor, wenn Daten an eine Stelle – etwa die Konzernmutter – übermittelt werden sollen, die ihren Sitz in den USA hat.

Datenschutzniveau in den USA

Kurz gesagt kann man feststellen, dass in den USA kein auch nur annähernd mit dem Schutzniveau in der EU vergleichbares Regelwerk zum Datenschutz besteht. Das hat verschiedene Ursachen:

- In der US-Verfassung gibt es keinen ausdrücklichen Schutz der Persönlichkeitsrechte bzw. der Privatsphäre („privacy“). Dieser Schutz ist erst im Laufe der Zeit durch Verfassungszusätze und die Rechtsprechung entwickelt worden, geht jedoch nicht so weit, wie dies z. B. im Grundgesetz Deutschlands der Fall ist.
- Es gibt zwar allerlei Gesetze, die den Schutz der Privatsphäre vor dem Zugriff durch Bundesbehörden sicherstellen („Privacy Act“, „Privacy Protection Act“ und andere), diese Gesetze gelten jedoch nur auf Bundesebene und im Verhältnis zwischen Bürger und bundesstaatlichen Organen. Entsprechende Gesetze in den Einzelstaaten sind entweder nicht vorhanden oder sehr unterschiedlich ausgeprägt, betreffen aber jedenfalls nur das Verhältnis der Bürger zum Staat, nicht zu privaten Stellen.
- Aufgrund der streng föderalen Struktur der USA gibt es kein Bundesgesetz, das z. B. dem Bundesdatenschutzgesetz entspricht und den Datenschutz zwischen Bürgern und privaten Stellen regelt. Die Zuständigkeit für den Schutz der Privatsphäre gegenüber anderen Privaten liegt tendenziell bei den Einzelstaaten. Jedoch ist zu erkennen, dass der Bund hier Gesetzgebungskompetenzen an sich zieht.

Das Problem ist also, dass die USA kein „angemessenes Schutzniveau“ hinsichtlich des Datenschutzes gewährleisten können, eine Übermittlung von personenbezogenen Daten an Stellen in der USA also demnach nicht bzw. nur im Rahmen der Ausnahmeregelungen des § 4c BDSG zulässig wäre.

Das „Safe-Harbour“-Abkommen

Um dieses Problem zu lösen, haben die EU-Kommission und das US-Handelsministerium eine Abmachung getroffen, die die Übermittlung personenbezogener Daten an bestimmte Unternehmen erlaubt.

Unternehmen, die sich bestimmten Prinzipien unterwerfen, dürfen personenbezogene Daten aus der EU empfangen (vergleichbar mit der Regelung in § 4c Abs. 2 BDSG). Diese Prinzipien sind in einem Regelwerk enthalten, das sich „Grundsätze des ‚sicheren Hafens‘ zum Datenschutz“ („safe harbour principles“) nennt. Die Einhaltung dieser Regelungen durch das Unternehmen, das sich ihnen unterwirft, wird durch die Federal Trade Commission der USA überwacht. Meistens lassen sich die betreffenden Unternehmen durch eine neutrale Stelle überprüfen und erhalten ein entsprechendes Zertifikat.

Links auf Details:

Hier können Sie weitere Details zu dieser Lösung sowie Fragen des Datenschutzes in Drittstaaten erfahren:

Dokument über die Entscheidung der EU-Kommission mit den Grundsätzen des „sicheren Hafens“ als Anhang:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:DE:NOT>

Auflistung aller Unternehmen, die sich den Safe-Harbour-Grundsätzen unterworfen haben (englischer Text):

<http://www.export.gov/safeharbor/>

<http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>

Möglichkeiten der Mitbestimmung

Der Betriebsrat hat nur ein sehr eingeschränktes Mitbestimmungsrecht hinsichtlich des Datenschutzes. Über seine Aufsichtspflichten (§ 80 Abs. 1 Nr. 1 BetrVG) hat der Betriebsrat zwar die Möglichkeit, zu überprüfen, ob die zum Schutz der Arbeitnehmer geltenden Vorschriften eingehalten werden, hat aber keine eigenen Instrumente, deren Einhaltung zu erzwingen.

Dennoch gibt es zwei Möglichkeiten, hier auf dem Wege der zwingenden Mitbestimmung Einfluss zu nehmen:

- Wenn der Betriebsrat auch kein Mitbestimmungsrecht im Hinblick auf die Einhaltung des Datenschutzes hat, so hat er doch die Möglichkeit, auf dem Weg über die zwingende Mitbestimmung bei § 94 Abs. 1 BetrVG Einfluss zu nehmen: Die personenbezogenen Daten, die ins Ausland übermittelt werden sollen, müssen ja irgendwie erfasst und ins System eingegeben werden. Dazu werden i. d. R. Bildschirmmasken verwendet. Diese Bildschirmmasken sind Personalfragebogen i. S. d. § 94 Abs. 1 BetrVG, ihr Inhalt ist also Gegenstand zwingender Mitbestimmung.
- Zumindest die Handhabung aller Daten, die Aussagen über das Verhalten oder die Leistung der Arbeitnehmer erlauben, unterliegt der zwingenden Mitbestimmung durch den Betriebsrat auf Grund des § 87 Abs. 1 Nr. 6 BetrVG. Gerade im Zusammenhang mit Personalinformations- und -abrechnungssystemen gilt das für einen Großteil der Daten. Also kann der Betriebsrat auch hier auf einer Mitbestimmungspflicht beharren.

Darüber hinaus gilt: Die Aufsichtspflicht des Betriebsrats und damit verbunden die Informationspflicht des Arbeitgebers (§ 80 Abs. 2 BetrVG) verpflichten den Arbeitgeber, den Betriebsrat umfassend zu unterrichten. Der Betriebsrat kann z. B. einfordern,

- dass der Arbeitgeber ihm Einblick in die Verträge mit den ausländischen Stellen, die die personenbezogenen Daten von Arbeitnehmern empfangen, gewährt, damit er prüfen kann, ob die Verträge den von der EU vorgeschlagenen Standardvertragsklauseln (s. o. Seite 3) entsprechen.