BRUNO SCHIERBAUM

Datenübermittlung ins Ausland – neue Vorgaben im BDSG (2)

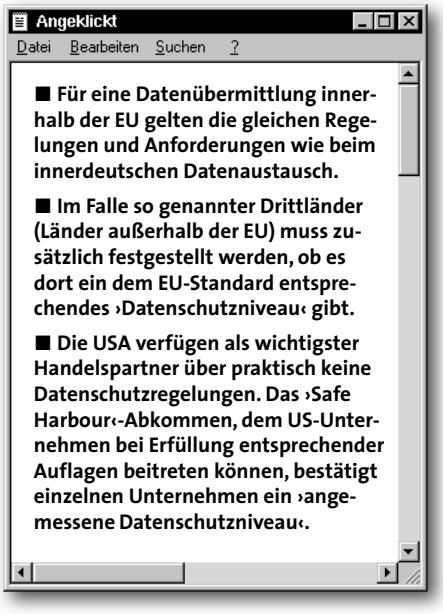
Auch im zweiten Teil dieses Artikels geht es um das sensible Thema der Übertragung von Personaldaten ins Ausland – und womöglich wird es sogar noch sensibler, denn hier geht es jetzt um die Datenübertragung in Länder, die ein schlechteres Datenschutzniveau aufweisen, als es die EU-Standards verlangen – vor allem die USA sind damit gemeint ...

Will ein Unternehmen personenbezogene Daten ins Ausland übertragen, sollte in einem ersten Schritt Folgendes geprüft werden: Erfolgt (1) die Übermittlung in EU-Staaten, für die die gleichen Regeln gelten wie für eine Datenübertragung innerhalb Deutschlands, oder erfolgt (2) die Übermittlung in ein Empfängerland außerhalb des EU-Bereichs, bei dem erst einmal festgestellt werden muss, ob das Niveau seiner Datenschutzregeln den EU-Standards (= ›angemessenes Datenschutzniveau‹) entspricht.

Im Anschluss an den ersten Teil des Artikel (cf 2/02 ab Seite 23) wird in diesem 2 Teil vor allem die Möglichkeiten einer Datenübermittlung bei ›nicht-angemessenem Datenschutzniveau‹ betrachtet.

Die zur Feststellung eines solchen ›angemessenen Datenschutzniveaus‹ erforderlichen Ermittlungen in einem so genannten Drittland, also einem Empfängerland außerhalb der EU, können allerdings sehr aufwändig sein. Deshalb sieht Artikel 25 Abs. 6 EG-Datenschutzrichtlinie vor, dass die EU-Kommission für ein gesamtes ›Drittland‹ die Feststellung eines angemessenen Datenschutzniveaus treffen kann. Eine solche positive Feststellung wurde zwischenzeitlich für Ungarn und die Schweiz bereits getroffen, wobei negative Feststellungen bis jetzt nicht vorgekommen sein dürften.

Für die Feststellung eines ›angemessenen Datenschutzniveaus‹ durch die EU-Kommission kommt der so genannten ›Artikel-29-Datenschutz-Gruppe‹ eine besondere Bedeutung zu. Der Name der Gruppe rührt daher, dass deren Bildung nach Artikel 29 EG-Datenschutzrichtlinie vorgeschrieben ist. In der ›Artikel-29-Datenschutz-Gruppe‹ sitzt unter anderen jeweils ein Vertreter der Kontrollbehörden eines jeden Mitgliedsstaats.



Die ›Artikel-29-Datenschutz-Gruppe‹ nimmt dabei die in Artikel 30 EG-Datenschutzrichtlinie verankerten Aufgaben *unabhängig* wahr. Sie kann also weder von einem Organ der Europäischen Gemeinschaft noch von einem der Mitgliedstaaten zu einem bestimmten Verhalten angewiesen werden. Vielmehr verlangt die Richtlinie von den EU-Staaten, alle Maßnahmen zu unterlassen, die die Unabhängigkeit der Datenschutz-Gruppe berühren können.

Die ›Artikel-29-Datenschutz-Gruppe‹ hat folgende Aufgaben:

- alle Fragen im Zusammenhang mit der Umsetzung der EG-Richtlinie erlassenen Vorschriften der einzelnen EU-Staaten zu prüfen;
- zum Datenschutzniveau in der EU und in Drittländern gegenüber der EU-Kommission Stellung zu nehmen;
- die Kommission bei jeder Vorlage zur Änderung der EG-Datenschutzrichtlinie zu beraten;
- Stellungnahmen zu den auf EU-Ebene erarbeiteten Verhaltensregeln zum Datenschutz abzugeben.

Die ›Artikel-29-Datenschutz-Gruppe‹ hat allerdings nur beratende Funktion und kann der EU-Kommission Vorschläge machen, beispielsweise für ein bestimmtes Land ein angemessenes Datenschutzniveau festzustellen. In diesem Zusammenhang gibt die ›Artikel-29-Datenschutz-Gruppe‹ Arbeitspapiere (= Working Papers) heraus, die Empfehlungen, Stellungnahmen, Diskussionsgrundlagen, Arbeitsunterlagen und Jahresberichte enthalten (siehe dazu info-Kasten in CF 2/02 Seite 26).

Ein besonderer Fall: die USA

Für die USA gibt es eine besondere Regelung. Da in den USA weder eine umfassende Datenschutzgesetzgebung besteht noch eine solche beabsichtigt ist, gestaltete sich das Feststellen eines ›angemessenen Datenschutzniveaus‹ schwierig. Wegen der engen wirtschaftlichen Beziehungen zwischen den Mitgliedstaaten der EU und den USA ist deshalb ein Rechtsrahmen mit der Bezeichnung ›US International Safe Harbor Principles‹ oder kurz ›Safe Harbor‹ (= sicherer Hafen) für die Daten aus Europa vereinbart worden. Die ›Safe Harbor‹-Prinzipien enthalten unter anderem die Datenschutzgrundsätze selbst und etliche in diesem Zusammenhang ›häufig gestellte Fragen‹ (= Frequently Asked Questions = FAQ)…[1].

Am 26. Juli 2000 hat die EU-Kommission festgestellt, dass der ›Safe Harbor‹-Rechtsrahmen ein angemessenes Datenschutzniveau gewährleiste. US-Unternehmen können sich nun freiwillig diesen Datenschutz-Prinzipien unterwerfen und sind dann privilegierte Empfänger für personenbezogene Daten aus Europa. Für europäische Unternehmen bedeutet das eine erhebliche Erleichterung. Sie brauchen sich lediglich durch Einsicht in die (derzeit in Vorbereitung befindliche) Liste des US-Handelsministeriums (Federal Trade Commission) davon zu überzeugen, dass ihr Geschäftspartner dem ›Safe Harbor‹ angehört.

Die wichtigsten ›Safe Harbor‹-Regeln sind in Stichworten:

1. Informationspflicht
2. Wahlmöglichkeit/Widerspruchsrecht

3. Weitergabe
4. Sicherheit
5. Datenintegrität
6. Auskunftsrecht
7. Durchsetzung

US-Unternehmen und -Organisationen haben also (1) eine *Informationspflicht* jedem von einer Datenübertragung betroffenen EU-Bürger gegenüber. Dazu gehört die Information, für welche Zwecke personenbezogene Daten empfangen/gesammelt werden, welche Organisationen die Daten möglicherweise auch noch nutzen können und wo die Grenzen dieser Nutzung sind. Zudem muss den betroffenen EU-Bürgern eine Kontaktadresse für Rückfragen mitgeteilt werden. Alle Informationen müssen auf Anfrage in *verständlicher* Form mitgeteilt werden.

Die Betroffenen müssen auch (2) die Möglichkeit haben zu wählen (*Wahlmöglichkeit*), ob ihre Daten an Dritte weitergegeben oder für einen Zweck verarbeitet werden dürfen, für den sie bei der Erhebung nicht bestimmt waren. Bei sensiblen Daten (Religion, Gewerkschaftszugehörigkeit usw.) benötigen die Organisationen außerdem in jedem Fall die ausdrückliche Zustimmung des Betroffenen. Die Wahlmöglichkeit beinhaltet auch ein *Widerspruchsrecht* des Betroffen in Bezug auf die Weitergabe der Daten und auf Änderung des Verarbeitungszwecks.

Soll eine *Weitergabe* von Daten im Rahmen der vereinbarten Nutzung stattfinden, darf das (3) nur dann geschehen, wenn der Empfänger der Daten ebenfalls dem ›Safe Harbor‹-Abkommen beigetreten ist oder eine schriftliche Erklärung abgibt, mit der er sich diesen Regeln unterwirft.

Aus Gründen der Daten-*Sicherheit* müssen US-Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, (4) angemessene Sicherheitsvorkehrungen treffen, um die Daten vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen.

Eine US-Organisation darf personenbezogene Daten (5) nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck, dem der Betroffene nachträglich zugestimmt hat, unvereinbar ist (*Datenintegrität*). Die Organisation muss zudem gewährleisten, dass die Daten für den vorgesehenen Zweck hinreichend zuverlässig, vollständig und aktuell sind.

1… Das Papier kann abgerufen werden über das Internet:

http://europa.eu.int/eur-lex/de/lif/dat/2000/de_300D0520.html

Im Rahmen eines *Auskunftsrechts* müssen (6) Privatpersonen (= Betroffene) Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt. Zudem müssen die Betroffenen die Möglichkeit haben, ihre personenbezogenen Daten korrigieren, ändern oder löschen zu lassen, wenn sie falsch sind.

Für einen effektiven Schutz der Privatsphäre müssen schließlich noch (7) Mechanismen geschaffen werden, die die Einhaltung oder *Durchsetzung* der Grundsätze des ›Safe Harbor‹ gewährleisten. Diese Mechanismen müssen mindestens Folgendes umfassen:

- leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden der betroffenen Personen behandelt werden und Schadensersatz geleistet wird;
- Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Unternehmen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden;
- Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Unternehmen die Einhaltung der Grundsätze zwar erklärt, aber sich trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Datenschutzgrundsätze einhalten.

Das ›Safe Harbor‹-Abkommen muss jährlich von jedem Mitglied (Unternehmen/Organisation) erneuert werden – und zwar beim US-Handelsministerium (Federal Trade Commission), das gleichzeitig auch für die Einhaltung der Grundsätze zuständig ist. Ansprechpartner für die Europäer bei Verletzungen der ›Safe Harbor‹-Grundsätze ist ebenfalls das US-Handelsministerium.

Betriebsvereinbarungen – als ›andere‹ Rechtsvorschriften

Die Datenübermittlung ins Nicht-EU-Ausland kann aber auch im Rahmen einer Betriebsvereinbarung geregelt werden, wobei eine solche Betriebsvereinbarung dann eine ›andere Rechtsvorschrift‹ im Sinne des § 4 Abs. 1 BDSG darstellt (eine Rechtsvorschrift also, durch die die Erfassung, Verarbeitung, Nutzung und *Übermittlung* von personenbezogenen Daten erlaubt werden kann).

Auch so können die ›schutzwürdigen Interessen‹ von Beschäftigten gewahrt werden. Dabei darf eine entsprechende Vereinbarung – wie im 1. Teil dieses Artikels bereits erwähnt – nicht hinter den Vorgaben des BDSG zurückbleiben. Dies wäre zum Beispiel dann der Fall, wenn die Betriebsvereinbarung *nicht* die Rechte der Betroffenen nach § 33 ff BDSG – die ohnehin unabdingbar sind – oder die Kontrolle des Datenschutzes (durch Betriebsrat, betrieblichen Datenschutzbeauftragten) regeln würde. Inzwischen gibt es eine Reihe von Fällen, in denen durch Vereinbarung zwischen deutschen und ausländischen Unternehmen die Wahrung eines angemessenen Datenschutzstandards sichergestellt wurde…[2].

Bei der Erstellung einer solchen Betriebsvereinbarung können die von der Europäischen Union verabschiedeten ›Standardvertragsklauseln für den Drittland-Transfer‹ gut hinzugezogen werden, auch wenn dieser Standardvertrag nicht speziell auf die Übermittlung von *Arbeitnehmer*-Daten abzielt. Die Regelungsinhalte einer solchen Betriebsvereinbarung unterscheiden sich auch nicht grundsätzlich von den Vereinbarungen, wie sie sonst zu den technischen Kontrollsystemen eines Betriebs abgeschlossen werden. Wichtig ist es, zum einen den Rahmen der Datenverarbeitung transparent zu machen und die Verarbeitung der Daten zum anderen auf den betrieblich erforderlichen Umfang (= enge Zweckbestimmung bezogen auf das Arbeitsvertragsverhältnis) einzugrenzen. Dies geschieht durch klare Festlegung der …

- eingesetzten Hardware,
- eingesetzten Software,
- personenbezogenen Daten,
- zugriffsberechtigten Personen,
- Schnittstellen,
- Auswertungen und
- Löschungsfristen.

Im Zuge der Übermittlung von Daten ins Ausland dürfen dabei grundsätzlich *keine umfassenderen* Verarbeitungs-/Auswertungsmöglichkeiten eröffnet werden als dies innerhalb der Bundesrepublik Deutschland zulässig wäre.

Zusätzlich sollten neben Datenschutz- und Datensicherungs-Maßnahmen (§ 9 BDSG) die Rechte der Arbeitnehmer (§§ 33 – 35 BDSG) und die Kontrollmöglichkeiten des Betriebsrats und des betrieblichen Datenschutzbeauftragten in der Betriebsvereinbarung festgelegt werden. Da im Ausland (jedenfalls außerhalb der Europäischen Union) bei Datenschutzverletzungen in der Regel keine Sanktionen vorgesehen sind und zusätzliche externe Kontrollorgane wie die deutschen Aufsichtsbehörden dort nicht eingerichtet sind, sollten auch Strafen für den Fall von Vertragsverletzungen vereinbart werden. Da eine Betriebsvereinbarung nicht automatisch auch im Ausland gilt, müssen beide Unternehmen in einem zusätzlichen Vertrag die Geltung der Vereinbarung festlegen.

Bruno Schierbaum, Kontakt: Beratungsstelle für Technologiefolgen und Qualifizierung (ver.di) Niedersachsen in Oldenburg, Telefon 0 44 11 - 8 20 68, **schierbaum@btq.de**

2… Siehe hierzu die entsprechenden Auszüge aus einer Vereinbarung, in einem Artikel von Thomas Barthel: ›Weltweit und (un)kontrollierbar?!‹ in c't 8-9/00 ab Seite 42.

info

Standardvertragsklauseln im Sinne von Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die

Übermittlung personenbezogener Daten in Drittländer

die kein angemessenes Schutzniveau gewährleisten

Die hier abgedruckten ›Standardvertragsklauseln sind keine leichte Lektüre. Autor und CF-Redaktion haben sich trotzdem entschlossen, sie hier komplett abzudrucken, weil sie eine Grundlage auch für entsprechende unternehmensbezogene Regeln sein können und zur Zeit auf anderem Wege kaum zu bekommen sind (auch nicht über das Internet). Der folgende Text muss und sollte deshalb nur durchgearbeitet werden, wenn er konkret gebraucht wird.

Die Daten exportierende Organisation XYZ

und

die Daten importierende Organisation ZYX:

vereinbaren folgende Vertragsklauseln (nachstehend: Klauseln), um ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen für die Übermittlung der in Anlage 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Exporteur an den Importeur bereitzustellen.

Klausel 1 [...]

Klausel 2
Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die Kategorien personenbezogener Daten und ihre Übermittlungszwecke, sind in Anlage 1 aufgeführt, die Bestandteil der Klauseln ist.

Klausel 3
Drittbegünstigtenklausel

Die betroffenen Personen können diese Klausel und die Klausel 4 Buchstaben b), c) und d), Klausel 5 Buchstaben a), b), c) und e); Klausel 6 Absätze 1 und 2 sowie Klauseln 7, 9 und 11 als Drittbegünstigte geltend machen. [...]

Klausel 4
Pflichten des Datenexporteurs

Der Datenexporteur verpflichtet sich und garantiert:

(a) dass die Verarbeitung der personenbezogenen Daten, einschließlich der Übermittlung, durch ihn entsprechend den einschlägigen Vorschriften des Mitgliedstaates, in dem der Datenexporteur ansässig ist, erfolgt ist bzw. bis zum Zeitpunkt der Übermittlung erfolgen wird (gegebenenfalls einschließlich der Mitteilung an die zuständige Stelle dieses Mitgliedstaates) und dass sie nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

(b) dass die betroffene Person, sofern die Übermittlung besondere Datenkategorien einbezieht, davon in Kenntnis gesetzt worden ist oder vor der Übermittlung wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau bietet;

(c) dass er den betroffenen Personen auf Anforderung eine Kopie dieser Klauseln, wie sie vereinbart wurden, zur Verfügung stellt und

(d) Anfragen der Kontrollstelle bezüglich der Verarbeitung einschlägiger personenbezogener Daten durch den Datenimporteur sowie Anfragen betroffener Personen bezüglich der Verarbeitung ihrer personenbezogenen Daten durch den Datenimporteur innerhalb eines angemessenen Zeitraums und in zumutbarem Maße beantwortet.

Klausel 5
Pflichten des Datenimporteurs

Der Datenimporteur verpflichtet sich und garantiert:

(a) dass er seines Wissens keinen nationalen Gesetzen unterliegt, die ihm die Erfüllung seiner Vertragsverpflichtungen unmöglich machen und dass er im Fall einer Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien auswirkt. die die Klauseln bieten, den Datenexporteur und die Kontrollstelle des Landes, in dem der Datenexporteur ansässig ist, hiervon informieren wird. In einem solchen Fall ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten

(b) dass er die personenbezogenen Daten verarbeitet in Übereinstimmung mit den verbindlichen Datenschutzgrundsätzen der Anlage 2 oder

dass er, falls sich die Parteien durch Ankreuzen des entsprechenden Kästchens weiter unten ausdrücklich damit einverstanden erklärt haben und vorausgesetzt, dass die verbindlichen Datenschutzgrundsätze der Anlage 3 beachtet werden, die Daten in jeder anderen Hinsicht verarbeitet in Übereinstimmung mit

– den einschlägigen nationalen Rechtsvorschriften (in der Anlage zu diesen Klauseln) zum Schutz der Grundrechte und -freiheiten natürlicher Personen, insbesondere des Rechts auf Schutz der Privatsphäre, im Hinblick auf die Verarbeitung personenbezogener Daten, die in dem Land, in dem der Datenexporteur ansässig ist, auf die für die Verarbeitung Verantwortlichen anzuwenden sind oder

– den einschlägigen Bestimmungen in Entscheidungen der Kommission nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG, mit denen festgestellt wird, dass ein Drittland nur für bestimmte Tätigkeitsbereiche ein angemessenes Schutzniveau gewährleistet, vorausgesetzt, dass der Datenimporteur in diesem Drittland ansässig ist und nicht unter diese Bestimmungen fällt, sofern diese Bestimmungen dergestalt sind, dass sie auf die Übermittlung anwendbar sind.

(c) dass er alle sachdienlichen Anfragen, die. sich auf die von ihm durchgeführte Verarbeitung der personenbezogenen Daten, die Gegenstand der Übermittlung sind, beziehen und die der Datenexporteur oder die betroffenen Personen an ihn richten, unverzüglich und genau bearbeitet und bei allen Anfragen der zuständigen Kontrollstelle mit dieser kooperiert und die Feststellung der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten respektiert;

(d) dass er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung zur Verfügung stellt; die Prüfung wird vom Datenexporteur oder einem vom Datenexporteur gegebenenfalls in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt, dessen Mitglieder unabhängig sind und über die erforderlichen Qualifikationen verfügen;

(e) dass er den betroffenen Personen auf Anfrage eine Kopie der Vertragsklauseln zur Verfügung stellt und die Stelle benennt, die für Beschwerden zuständig ist.

Klausel 6
Haftung

1. Die Parteien vereinbaren, dass betroffene Personen, die durch eine Verletzung der Bestimmungen in Klausel 3 Schaden erlitten haben, berechtigt sind. von den Parteien Schadensersatz für den erlittenen Schaden zu verlangen. Die Parteien vereinbaren, dass sie nur von der Haftung befreit werden können, wenn sie nachweisen, dass keine von ihnen für die Verletzung dieser Bestimmungen verantwortlich ist.

2. Der Datenexporteur und der Datenimporteur vereinbaren, dass sie gesamtschuldnerisch für Schäden der betroffenen Personen haften, die durch eine Verletzung im Sinne von Absatz 1 entstehen. Im Falle einer Verletzung dieser Bestimmungen kann die betroffene Person gegen den Datenexporteur oder den Datenimporteur oder beide gerichtlich vorgehen.

3. Die Parteien vereinbaren, dass, wenn eine Partei haftbar gemacht wird für eine Verletzung im Sinne von Absatz 1 durch die andere Partei, die zweite Partei der ersten Partei alle Kosten, Schäden, Ausgaben und Verluste, die der ersten Partei entstanden sind, in dem Umfang ersetzt in dem die zweite Partei haftbar ist.

Klausel 7
Schlichtungsverfahren und Zuständigkeit

1. Die Parteien vereinbaren, dass sie im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Vertragsparteien, die unter Berufung auf die Drittbegünstigung nach Klausel 3 nicht auf gütlichem Wege beigelegt wird, die Entscheidung der betroffenen Person akzeptieren entweder:

a) an einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle teilzunehmen; oder

b) den Streitfall den Gerichten des Mitgliedstaates zu unterbreiten, in dem der Datenexporteur ansässig ist.

2. Die Parteien vereinbaren, dass nach Absprache zwischen der betroffenen Person und der relevanten Partei die Klärung eines bestimmten Streitfalls einem Schiedsgericht unterbreitet werden kann, vorausgesetzt dass diese Partei in einem Land ansässig ist, das das New Yorker Übereinkommen über die Vollstreckung von Schiedssprüchen ratifiziert hat.

3. Die Parteien vereinbaren, dass die Absätze 1 und 2 unbeschadet der materiellen oder Verfahrensrechte der betroffenen Person gelten, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen.

Standardvertragsklauseln

Anlage 1

Diese Anlage ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.

Der Datenexporteur ist ... (bitte erläutern Sie kurz Ihre Tätigkeiten, die für die Übermittlung von Belang sind): ...

Der Datenimporteur ist ... (bitte erläutern Sie kurz Ihre Tätigkeiten, die für die Übermittlung von Belang sind): ...

Die übermittelten personenbezogenen Daten beziehen sich auf folgende Kategorien von betroffenen Personen (bitte erläutern): ...

Die Übermittlung ist zu folgenden Zwecken erforderlich (bitte angeben): ...

Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte angeben): ...

Die übermittelten personenbezogenen Daten gehören zu folgenden Kategorien sensibler Daten (bitte angeben): ...

Die übermittelten personenbezogenen Daten dürfen nur folgenden Empfängern oder Kategorien von Empfängern bekannt gemacht werden (bitte angeben): ...

Die übermittelten personenbezogenen Daten dürfen nur (bitte angeben): ... (Monate/Jahre) aufbewahrt werden.

Standardvertragsklauseln

Anlage 2

Verbindliche Datenschutzgrundsätze im Sinne von Klausel 5 Buchstabe b) Absatz 1:

Diese Datenschutzgrundsätze sind im Lichte der Bestimmungen (Grundsätze und entsprechende Ausnahmen) der Richtlinie 95/46/EG auszulegen*.

Sie gelten vorbehaltlich der nach den nationalen Rechtsvorschriften für den Datenimporteur geltenden zwingenden Anforderungen, die nicht weiter gehen, als es in einer demokratischen Gesellschaft unter Zugrundelegung der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgeführten Interessen erforderlich ist; d.h. die Anforderungen müssen notwendig sein für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen oder den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

1) Zweckbindung

Die Daten sind für die spezifischen Zwecke in Anlage 4 der Klauseln zu verarbeiten und anschließend zu verwenden oder weiter zu übermitteln. Die Daten dürfen nicht länger aufbewahrt werden, als es für die Zwecke erforderlich ist, für die sie übermittelt werden.

2) Datenqualität und -verhältnismäßigkeit

Die Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Sie müssen angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiterverarbeitet werden, nicht exzessiv sein.

3) Transparenz

Die betroffenen Personen müssen Informationen über die Zweckbestimmungen der Verarbeitung und die Identität des im Drittland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies erforderlich ist, um eine angemessene Verarbeitung sicherzustellen, und sofern diese Informationen nicht bereits vom Datenexporteur erteilt wurden

4) Sicherheit und Vertraulichkeit

Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen gegen die Risiken der Verarbeitung zu treffen, beispielsweise gegen den unzulässigen Zugriff auf Daten. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Auftragsverarbeiter, dürfen die Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5) Recht auf Zugriff, Berichtigung, Löschung und Widerspruch

Nach Artikel 12 der Richtlinie 95/46/EG muss die betroffene Person das Recht haben, auf alle sie betreffenden Daten, die verarbeitet werden, zuzugreifen sowie je nach Fall das Recht haben auf Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung gegen die in dieser Anlage aufgeführten Grundsätze verstößt, insbesondere wenn diese Daten unvollständig oder unrichtig sind. Die betreffende Person muss auch aus zwingenden berechtigten Gründen, die mit ihrer persönlichen Situation zusammenhängen, Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können

*** Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. ABl. L 281 vom 23. 11. 1995**

6) Beschränkung der Weiterübermittlung

Weiterübermittlungen personenbezogener Daten vom Datenimporteur an einen anderen für die Verarbeitung Verantwortlichen, der in einem Drittland ansässig ist, das weder angemessenen Schutz bietet noch unter eine von der Kommission gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Entscheidung fällt (nachstehend: Weiterübermittlung), dürfen nur stattfinden, wenn eine der folgenden Bedingungen erfüllt ist:

a) Die betroffenen Personen haben der Weiterübermittlung eindeutig zugestimmt, falls bestimmte Datenkategorien betroffen sind, oder haben in anderen Fällen die Möglichkeit erhalten, sich dagegen auszusprechen.

Die betroffenen Personen müssen mindestens folgende Informationen erhalten und zwar in einer Sprache, die sie verstehen:

– die Zwecke der Weiterübermittlung,

– die Identität des in der Gemeinschaft ansässigen Datenexporteurs,

– die Kategorien weiterer Empfänger der Daten und Empfängerländer sowie

– eine Erklärung darüber, dass die Daten nach der Weiterübermittlung von einem für die Verarbeitung Verantwortlichen verarbeitet werden können, der in einem Land ansässig ist, das kein angemessenes Schutzniveau für die Privatsphäre des Einzelnen gewährleistet; oder

b) der Datenexporteur und der Datenimporteur stimmen dem Beitritt eines weiteren, für die Verarbeitung Verantwortlichen zu den Klauseln zu, der dadurch zu einer Partei dieser Klauseln wird und dieselben Verpflichtungen wie der Datenimporteur eingeht.

7) Besondere Datenkategorien

Werden Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie Daten über Gesundheit oder Sexualleben und Daten über Straftaten, strafrechtliche Verurteilungen oder Sicherheitsmaßnahmen verarbeitet, so sollten zusätzliche Garantien entsprechend der Richtlinie 95/46/EG vorliegen, insbesondere angemessene Sicherheitsmaßnahmen wie die strenge Verschlüsselung für Übermittlungszwecke oder Aufzeichnungen über Zugriffe auf sensible Daten.

8) Direktmarketing

Werden Daten zum Zwecke des Direktmarketings verarbeitet, müssen wirksame Verfahren vorgesehen sein, die der betroffenen Person jederzeit die Möglichkeit des ›Opt-Out‹ [Austiegsmöglichkeit] geben, so dass sie sich gegen die Verwendung ihrer Daten für derartige Zwecke entscheiden kann.

9) Automatisierte Einzelentscheidungen

Die betroffenen Personen haben das Recht, keiner Entscheidung unterworfen zu werden, die allein auf der automatisierten Datenverarbeitung beruht, wenn keine anderen Maßnahmen zur Wahrung der berechtigten Interessen der Person nach Artikel 15 Absatz 2 der Richtlinie 95/46/EG ergriffen werden. Erfolgt die Übermittlung mit dem Ziel, eine automatisierte Einzelentscheidung im Sinne von Artikel 15 der Richtlinie 95/46/EG, d.h. eine Entscheidung, die rechtliche Folgen für die Person nach sich zieht oder sie erheblich beeinträchtigt und die ausschließlich auf Grund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie dies beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens usw., zu treffen, so muss die natürliche Person das Recht haben, die Gründe für diese Entscheidung zu erfahren.

Standardvertragsklauseln

Anlage 3

Verbindliche Datenschutzgrundsätze im Sinne von Klausel 5 Buchstabe b) Absatz 2

1) Zweckbindung

Die Daten sind für die spezifischen Zwecke in Anlage 1 der Klauseln zu verarbeiten und anschließend zu verwenden oder weiter zu übermitteln. Die Daten dürfen nicht länger aufbewahrt werden, als es für die Zwecke erforderlich ist, für die sie übermittelt werden.

2) Recht auf Zugriff, Berichtigung, Löschung und Widerspruch

Nach Artikel 12 der Richtlinie 95/46/EG muss die betroffene Person das Recht haben, auf alle sie betreffenden Daten, die verarbeitet werden, zuzugreifen sowie je nach Fall das Recht haben auf Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung gegen die in dieser Lage aufgeführten Grundsätze verstößt, insbesondere wenn diese Daten unvollständig oder unrichtig sind. Die g betreffende Person muss auch aus zwingenden berechtigten n Gründen, die mit ihrer persönlichen Situation zusammen-hängen , Widerspruch gegen die Verarbeitung der sie betref-fenden Daten einlegen können.

3) Beschränkung der Weiterübermittlung

Weiterübermittlungen personenbezogener Daten vom Datenimporteur an einen anderen für die Verarbeitung Verantwortlichen, der in einem Drittland ansässig ist, das weder angemessenen Schutz bietet noch unter eine von der Kommission gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Entscheidung fällt (nachstehend: Weiterübermittlungen), dürfen nur stattfinden, wenn eine der folgenden Bedingungen erfüllt ist:

a) Die betroffenen Personen haben der Weiterübermittlung ausdrücklich zugestimmt, falls bestimmte Datenkategorien betroffen sind, oder haben in anderen Fällen die Möglichkeit erhalten, sich dagegen auszusprechen.

Die betroffenen Personen müssen mindestens folgende Informationen erhalten und zwar in einer Sprache, die sie verstehen:

– die Zwecke der Weiterübermittlung,

– die Identität des in der Gemeinschaft ansässigen Datenexporteurs,

– die Kategorien weiterer Empfänger der Daten und Empfängerländer sowie

– eine Erklärung darüber, dass die Daten, nach der Weiterübermittlung von einem für die Verarbeitung Verantwortlichen verarbeitet werden können, der in einem Land ansässig ist, das kein angemessenes Schutzniveau für die Privatsphäre des Einzelnen gewährleistet; oder

b) der Datenexporteur und der Datenimporteur stimmen dem Beitritt eines weiteren, für die Verarbeitung Verantwortlichen zu den Klauseln zu, der dadurch zu einer Partei dieser Klauseln wird und dieselben Verpflichtungen wie der Datenimporteur eingeht.