BTQ | INFO 2/14

Beratungsstelle für Technologiefolgen und Qualifizierung im Bildungswerk der Vereinten Dienstleistungsgewerkschaft (ver.di) im Lande Hessen e.V.

INHALT

Auftragsdatenverarbeitung

„Wer Angst hat, dass seine Daten abgefangen werden, sollte Dienste suchen, die nicht über amerikanische Server laufen."
Dieses Zitat stammt von dem deutschen Innenminister Hans-Peter Friedrich nach dem NSA-Skandal. Hintergrund ist die Verarbeitung von Daten auf amerikanischen Servern in einer sog. Cloud durch die ermöglicht wurde, dass unzählige Kommunikationsvorgänge bis hin zu denen von Kanzlerin Merkel ausgespäht wurden.
Nun stellen die USA einen datenschutzrechtlichen Sonderfall dar, da sie kein Datenschutzniveau aufweisen können, das nach deutschen Maßstäben als angemessen bezeichnet werden kann. Aus wirtschaftlichen Erwägungen wurde zwischen der EU-Kommission und dem US-Handelsministerium eine Abmachung getroffen, wonach Unternehmen aus den USA dann taugliche Datenempfänger sind, wenn sie sich den Grundsätzen des sogenannten sicheren Hafens (safe harbor principles) verpflichten. Ob das im Einzelfall eingehalten wird, wird auf eine Beschwerde hin kontrolliert. Aber das war wohl bislang nicht der Fall.
Es ist mittlerweile wenig aufsehenerregend und selbstverständlich, dass die Datenverarbeitung, zumindest Teile davon, außerhalb der eigenen IT-Abteilung verarbeitet werden. Wenn es um die Daten der Beschäftigten geht, lauten die Fragen, die von Betriebsräten zunächst gestellt werden: Sind die Daten sicher? Ist der Anbieter seriös und in Deutschland ansässig?
Eine gängige und häufige Assoziation zum Thema Auftragsdatenverarbeitung ist, dass Daten an einen Dienstleister übermittelt werden, dort nach Weisung des Auftraggebers verarbeitet und ihm dann in entsprechend aufgearbeiteter Form wieder zur Verfügung gestellt werden.
Das Bundesdatenschutzgesetz versteht entsprechend § 11 unter Auftragsdatenverarbeitung, dass personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet und genutzt werden. Verarbeitung bedeutet unter anderem aber auch die Löschung, also das „Unkenntlich machen" gespeicherter, personenbezogenen Daten (vgl. § 3 Abs. 4 Ziffer 5 BDSG), mit der Folge, dass auch die Datenvernichtung durch eine andere Stelle eines Vertrages nach § 11 BDSG bedarf (s. a. DIN 66399 Datenträgervernichtung). Der Auftragsdatenverarbeitung gleichgestellt wird in § 11 Abs. 5 BDSG auch, „wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann". Das betrifft dann nicht nur die Verarbeitung in einer – unbestimmten – Cloud, sondern auch andere Formen der Datenverarbeitung auf fremden Rechnern oder im Fall einer IT-Unterstützung durch Dritte, d. h. auch in diesen Fällen muss der Auftraggeber mit dem Dienstleister einen Vertrag nach § 11 BDSG abschließen.

Fortsetzung auf Seite 2

Liebe Leserinnen und Leser,

Die Entwicklung der Personaldatenverarbeitung könnte man sehr kurz auf die Formel bringen: Outsourcing + Globalisierung = wer hat unsere Daten und wo sind sie?

In der Tat ist es so, dass es nicht mehr der Dienstleister um die Ecke oder in der gleichen Stadt ist, der sich um die IT-Belange von Unternehmen kümmert, sondern es sind mittlerweile global agierende Großunternehmen, die ihre Kompetenzen und Kapazitäten anbieten und die Daten zunehmend in der sogenannten Cloud (Cloud Computing s. Kasten 1) erheben und verarbeiten. Es mag unwahrscheinlich klingen, aber mittlerweile ist es in vielen Unternehmen nur noch mit großem Aufwand möglich, über den derzeitigen Verbleib und Aufenthaltsort von personenbezogenen Daten der Beschäftigten eine Aussage zu treffen. Auf was Betriebsräte bei der Auslagerung der Datenverarbeitung achten sollten, wo ihre rechtlichen Möglichkeiten liegen und was alles noch, vielleicht bislang eher unbeachtet, ausgelagerte Datenverarbeitung sein könnte, darauf wollen wir in diesem BTQ-Info eingehen.

Wie immer viel Spaß beim Lesen
wünscht Ihnen …

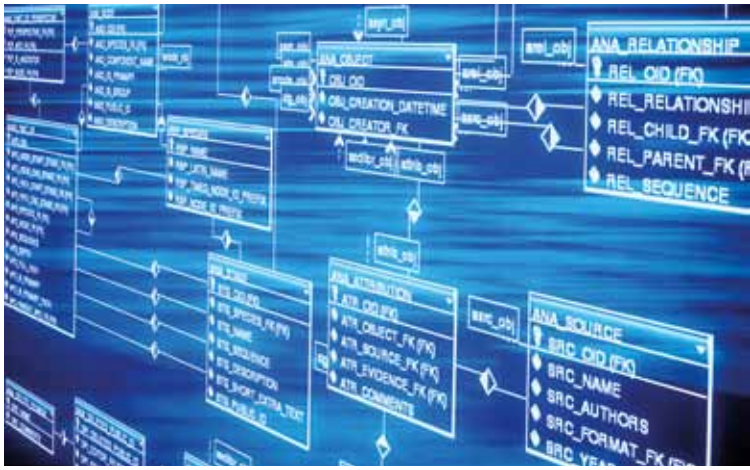
BTQ Kassel
Angersbachstr. 4 · 34127 Kassel
t 05 61 / 77 60 04
f 05 61 / 77 60 57
info@btq-kassel.de
www.btq-kassel.de
V.i.S.d.P.: Regine Franz

ISSN 1869-036X

Der Gesetzgeber ging davon aus, dass eine Verarbeitung durch andere Stellen einer besonderen Regelung bedarf und hat daher in § 11 BDSG festgelegt, welche konkreten Anforderungen in einem solchen Vertrag erfüllt sein müssen.
Wesentliches Kriterium bei der Auftragsdatenverarbeitung ist, dass der Auftraggeber verantwortliche Stelle bleibt (§ 3 Abs. 7 BDSG) und sich im Schadensfall einer Verantwortlichkeit nicht ohne weiteres dadurch entziehen kann, dass er die Schuld dem Dienstleister gibt. Das bedeutet auch, dass der Auftragnehmer die Daten ausschließlich im Rahmen der Weisungen des Auftraggebers verarbeiten darf. Im Bereich der Verarbeitung personenbezogener Daten von Beschäftigten hat dies zur Folge, dass auch im Fall der externen Verarbeitung dieser Daten der Auftragnehmer die einschlägigen Betriebsvereinbarungen einhalten muss.

Auftragsdatenverarbeitung in Konzernen

In Konzernen oder konzernähnlichen Strukturen werden Datenverarbeitungsprozesse häufig bei der „Mutter" gebündelt. Soweit dies durch kumulierte Daten, also z. B. Statistiken zu Steuerungszwecken erfolgt, ist dies datenschutzrechtlich unbedenklich, da keine personenbezogenen Daten im Spiel sind. Soweit personenbezogene Daten verarbeitet werden, muss auch in diesem Rechtsverhältnis ein Vertrag gemäß § 11 BDSG abgeschlossen werden, auch wenn es mitunter so angesehen wird, dass „der Schwanz mit dem Hund wackelt".
Will die Konzernmutter diese Daten für andere eigene Zwecke nutzen, dann handelt es sich nicht mehr um eine Auftragsdatenverarbeitung, sondern um eine Übermittlung – man spricht auch von einer sog. Funktionsübertragung –, deren rechtlichen Voraussetzungen in aller Regel erst mal nicht vorliegen. In jedem Fall ist dieses Vorgehen dann auch nicht mehr datenschutzrechtlich durch § 11 BDSG gedeckt, sondern es bedarf einer anderen Rechtsgrundlage, in der Regel einer Betriebsvereinbarung.
Für Betriebsräte besteht im Falle einer Auftragsdatenverarbeitung ein Kontrollrecht nach § 80 Abs. 1 Ziffer 1 BetrVG, nämlich ob die einschlägigen Datenschutzregelungen eingehalten werden. Das Kontrollrecht kann zum einen durch Einsicht in den Vertrag vorgenommen werden, einen Anspruch auf Aushändigung von Kopien hat er allerdings nicht. Hier können Betriebsräte die Kriterien des § 11 BDSG als Checkliste benutzen, um zu überprüfen, ob dessen Anforderungen im Vertrag realisiert wurden. Neben der Kontrolle des Vertrages hinsichtlich der Einhaltung datenschutzrechtlicher Regelungen und der Betriebsvereinbarungen geht dem Betriebsrat grundsätzlich nicht das Recht auf Kontrolle vor Ort verloren. Allerdings muss er darauf hinwirken, dass der Arbeitgeber das Kontrollrecht des Betriebsrates vor Ort in den Vertrag mit dem Dienstleister aufnimmt, denn anderenfalls kann sich der Dienstleister auf sein Hausrecht berufen und dem Betriebsrat völlig legitim den Zugang und eine Kontrolle verweigern.



Die Anforderungen an eine rechtmäßige Auftragsdatenverarbeitung

Der Vertrag zwischen dem Arbeitgeber als Auftraggeber und einem Dienstleister muss vor allem Regelungen enthalten hinsichtlich:

1. Gegenstand und die Dauer des Auftrags,
2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. der nach §9 zu treffenden technischen und organisatorischen Maßnahmen,
4. der Berichtigung, Löschung und Sperrung von Daten,
5. der nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. der etwaigen Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. der Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitteilungspflichtiger Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. des Umfangs der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. der Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Im Vertrag müssen Gegenstand und Dauer des Vertrages konkret bestimmt sein, möglich ist auch eine unbefristete Dauer mit einer Kündigungsfrist. Der sog. Gegenstand muss soweit definiert sein, dass genau daraus hervorgeht, um welche Daten es sich handelt, z. B. Personenstammdaten oder Kommunikationsdaten (u. a. Telefon, E-Mail). Es reicht nicht, als Zweck allgemein „Personaldatenverarbeitung" zu benennen. Ebenso konkret müssen die Anforderungen der Ziffer 2 definiert werden. Der Arbeitgeber kann sich beispielsweise bestimmte Verarbeitungen und Nutzungen für sich vorbehalten.
Zur Ausfüllung der Anforderungen nach Ziffer 3 – technisch-organisatorische Maßnahmen (s. Kasten 2) ist häufig in Verträgen zu lesen, „diese sind erfüllt". Das reicht nicht aus! Es müssen die konkreten Maßnahmen benannt werden, wie Zutrittsschutz nur für bestimmte legitimierte Personen, Zutritt nur durch Schranken, abgeschlossene Bereiche, passwortgeschützter Zugang, 4-Augen-Prinzip etc.
Zu Ziffer 4 ist konkretisierend zu vereinbaren, dass z. B. der Auftragnehmer nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren hat und wie ggf. zu verfahren ist, wenn ein Betroffener sich direkt an den Auftragnehmer wendet.
Zu Ziffer 5 kommen Regelungen in Betracht wie u. a. Nachweis der Bestellung eines geeigneten Datenschutzbeauftragten, Einhaltung der technisch-organisatorischen Maßnahmen, die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde.
Aus Sicht des Betriebsrats ist ein besonderes Augenmerk angebracht, wenn der Arbeitgeber nach Ziffer 6 die Möglichkeit zur Begründung eines Unterauftragsverhältnisses einräumt. Hierbei muss sichergestellt sein, dass dem Betriebsrat seine Kontroll- und Einsichtsrechte nicht verloren gehen und vor allem der Inhalt von Betriebsvereinbarungen nicht unterlaufen werden kann.
Bei den Kontrollrechten nach Ziffer 7 kann sich der Betriebsrat einklinken, um auch hier gewährleistet zu wissen, dass er seine Kontrollrechte auch in den hausrechtgeschützen Räumlichkeiten und IT-Einrichtungen in dem anderen Unternehmen durchführen kann. Die Maßnahmen nach Ziffer 8 und 9 konkretisieren die Tatsache, dass der Arbeitgeber auch im Falle einer Auftragsdatenverarbeitung Verantwortlicher im Sinne des Datenschutzrechtes

bleibt und muss sich daher angemessene Rechte vorbehalten.
Der Verbleib der Daten nach Beendigung des Auftragsverhältnisses ist von Bedeutung, um zu gewährleisten, dass der Auftragnehmer nach Beendigung des Vertrages keine Nutzungsmöglichkeiten mehr für die Daten behält.
Weitere Vorschläge zur Gestaltung eines Auftragsdatenverarbeitungsvertrages finden sich z. B. unter https://www.gdd.de/aktuelles/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg.
Außerdem muss sich der Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen. Das Ergebnis ist zu dokumentieren (11 Abs. 2 S. 4 und 5 BDSG).
Der Betriebsrat kann im Rahmen seines Kontrollrechts die Vorlage dieser Prüfdokumentationen verlangen und sollte, soweit diese nicht vorliegen, den Arbeitgeber darauf hinweisen, dass es sich um eine (fortgesetzte) Ordnungswidrigkeit handelt.

Geänderte Anforderungen an die Auftragsdatenverarbeitung seit 01. 09. 2009

Soweit der zu prüfende Vertrag vor dem 1. September 2009 geschlossen und danach nicht geändert wurde, ist die Wahrscheinlichkeit, dass der Vertrag nicht (mehr) rechtskonform ist, relativ hoch. Das BDSG wurde in 2009 novelliert, deren Änderungen zu verschiedenen Zeitpunkten entsprechend der sog. BDSG-Novellen I – III in Kraft traten. Die Änderung der Anforderungen u. a. an die Auftragsdatenverarbeitung erfolgte mit der BDSG-Novelle II, die am 1. September 2009 in Kraft trat und u. a. die Einführung eines Bußgeldtatbestandes bei Nichteinhaltung der Anforderungen des § 11 BDSG zur Folge hatte. Danach handelt gem. § 43 Abs. 1 Ziffer 2b ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. Finden sich die nachstehend aufgeführten Punkte in einem Vertrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise, kann dies mit einem Bußgeld bis 50.000 Euro belegt werden (vgl. § 43 Abs. 3, S. 1 BDSG).

Datentransfer ins Ausland

Die oben genannten Ausführungen gelten immer dann, wenn die Auftragsdatenverarbeitung in Deutschland, in einem Mitgliedstaat der Europäischen Union oder in

einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraums erfolgt. Juristisch ist eine Auftragsdatenverarbeitung in anderen als den dort genannten Ländern nicht möglich. Dies ergibt sich aus einem Umkehrschuss aus § 3 Abs. 8 Satz 3 BDSG: 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.
Konkret bedeutet dies, dass eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG nie stattfinden kann, soweit es sich um Länder handelt, die nicht Inland und weder Mitgliedstaat der Europäischen Union noch in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraums angesiedelt sind, da es sich juristisch um Dritte handelt und die Weitergabe von personenbezogenen Daten an Dritte immer eine Übermittlung ist. Das bedeutet allerdings nicht, dass ohne vertragliche Regelungen ein Auftrag zu Verarbeitung von Daten erteilt werden könnte. Der deutsche Gesetzgeber geht davon aus, dass in den genannten Ländern aufgrund der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr das Datenschutzniveau dem deutschen entspricht. Für die Legitimation einer Auftragsvergabe an Dritte müssen die einschlägigen Voraussetzungen der §§ 4b und 4c BDSG vorliegen oder eine andere Rechtsgrundlage, damit die Weitergabe legitimiert ist. Im Falle der Verarbeitung von Beschäftigtendaten wird in aller Regel der Mitbestimmungstatbestand gemäß § 87 Abs. 1 Ziffer 6 BetrVG einschlägig sein, d. h. das Vorliegen der datenschutzrechtlichen Voraussetzungen allein genügt nicht, die Daten in Ländern außerhalb des Binnenraums[1] verarbeiten zu lassen, sondern es bedarf einer zusätzlichen Zulässigkeitsvereinbarung zwischen Betriebsrat und Arbeitgeber, um diesen Datentransfer zu legitimieren. Unabhängig davon müssen als Mindestvoraussetzungen die datenschutzrechtlichen Vorgaben erfüllt sein. Die Übermittlung unterbleibt von vornherein gemäß § 4b Abs. 1 Satz 2 BDSG, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Nach Abs. 3 wird die Angemessenheit des Schutzniveaus unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind. Insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.
So muss das Drittland, in das die Daten übermittelt werden sollen, ein „angemessenes Schutzniveau" vorweisen. Die Beurteilung, ob in einem anderen Land ein angemessenes Schutzniveau besteht, ist gemäß Abs. 5 eine Ermessensentscheidung der übermittelnden Stelle, wobei der Betriebsrat hier aufgrund der erforderlichen Vereinbarung ein gehöriges Wort mitzusprechen hat.
Das BDSG definiert nicht, was unter einem angemessenen Schutzniveau zu verstehen ist, allerdings geben die Feststellungen der Kommission auf der Grundlage von Art. 31 Abs. 2 der EG-Datenschutzrichtlinie eine Entscheidungshilfe, da dort Länder gelistet wurden, die nach Ansicht der Kommission über ein angemessenes Schutzniveau verfügen. Das sind derzeit die Schweiz, Ungarn, Kanada, Argentinien, Vogtei Guernsey, Vogtei Jersey, Färöer, Andorra, Israel und Neuseeland. Bei einer Übermittlung personenbezogener Daten in diese Länder wird davon ausgegangen, dass das Daten-

1 Zum Binnenraum zählen z. B. auch die französischen Überseedepartements, die Azoren, Madeira und die Kanarischen Inseln, Island, Norwegen, Liechtenstein, nicht dazu gehören z. B. Färöer Inseln, Guernsey, Jersey

schutzniveau dem der Bundesrepublik vergleichbar ist. Bei mitbestimmungspflichtigen Verarbeitungen – und das ist immer dann gegeben, sobald die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten mitbestimmungspflichtig und gegebenenfalls auch schon in einer Betriebsvereinbarung geregelt ist – reicht die Einhaltung der gesetzlichen Bestimmungen allein nicht aus, sondern es muss eine zusätzliche Rechtsgrundlage, nämlich eine Betriebsvereinbarung, mit dem Betriebsrat abgeschlossen werden, die die Übermittlung legitimiert. Dort kann zum Beispiel die Verarbeitung auf Länder eingeschränkt werden, die nach Ansicht der EU-Kommission über ein angemessenes Datenschutzniveau verfügen und die Zusicherung des Arbeitgebers, dass die Kontrollrechte des Betriebsrats gewährleistet bleiben.

Kasten 1

Cloud Computing beinhaltet Technologien und Geschäftsmodelle um IT-Ressourcen dynamisch zur Verfügung zu stellen und ihre Nutzung nach flexiblen Bezahlmodellen abzurechnen. Anstelle IT-Ressourcen, beispielsweise Server oder Anwendungen, in unternehmenseigenen Rechenzentren zu betreiben, sind diese bedarfsorientiert und flexibel in Form eines dienstleistungsbasierten Geschäftsmodells über das Internet oder ein Intranet verfügbar.
(Quelle: Gabler-Wirtschaftslexikon, http://wirtschaftslexikon.gabler.de/Definition/Cloud-Computing.html#definition)

Bei Datenübermittlungen an eine Stelle in einem sogenannten (unsicheren) Drittstaat, die also weder in einem EWR-Staat noch in einem Staat liegt, für den die Kommission eine Angemessenheitsentscheidung getroffen hat, muss die Daten übermittelnde Stelle wiederum selbst das Datenschutzniveau des Staates überprüfen (§ 4b Abs. 3 und 5 BDSG). Wie eingangs ausgeführt, besteht u. a. in den USA – aber auch in Indien, Japan und China – kein angemessenes Datenschutzniveau. Eine Übermittlung von personenbezogenen Daten wäre also zunächst einmal, unbesehen der Rechte des Betriebsrats, unzulässig. Um den Wirtschaftsverkehr nicht zu behindern, stellt die Europäische Kommission drei Musterverträge zur Verfügung, die keiner Genehmigung durch die Aufsichtsbehörde bedürfen, unter dem Vorbehalt, dass keine Änderungen vorgenommen wurden. Im Falle von Änderungen im Standardvertrag zugunsten des Betroffenen ist mit der Aufsichtsbehörde zu klären, ob eine Genehmigungspflicht besteht.
Will der Arbeitgeber einen individuellen Vertrag abschließen, ist die Einschaltung der Aufsichtsbehörde erforderlich. Der Vertrag bedarf gemäß § 4c Abs. 2 BDSG einer Genehmigung.
Bei verbindlichen Konzernregelungen zum Datenschutz geht man davon aus, dass in der Regel eine Genehmigung erforderlich ist. Die Aufsichtsbehörden vertreten unterschiedliche Auffassungen darüber, ob beim Einsatz von Konzernverträgen eine Genehmigungspflicht besteht. Daher wird die Klärung des Sachverhalts mit der zuständigen Aufsichtsbehörde empfohlen, dass die geschieht, sollte der Betriebsrat im Auge behalten.
Zu weiteren Möglichkeiten, personenbezogene Daten in das EU-Ausland zu übermitteln, gehören die Verwendung neben den genannten EU-Standardvertragsklauseln, die Safe Harbor Zertifizierung (für Unternehmen mit Sitz in den USA) sowie Binding Corporate Rules (für den gesamten Konzern).
Die Wirksamkeit von Safe-Harbor-Zertifizierungen in den USA ist allerdings seit der NSA-Affäre erneut durch die Datenschutzbehörden in Frage gestellt worden, da es sich um eine Selbstverpflichtung der Unternehmen handelt. Diese Unternehmen können sich die vom US-Handelsministerium erlassenen Grundsätze des „Safe Harbor" anerkennen und sich entsprechend zertifizieren lassen. Damit kann der Status „angemessenes Datenschutzniveau" erreicht werden. Wer wissen will, wie das ausgehen kann, sollte dieses BTQ-Info wieder von vorne lesen …

Impressum

Herausgegeber: BTQ Kassel
Redaktion: BTQ Kassel
Gestaltung: K.Design, Wiesbaden
Druck: Druckerei Riehm, Kassel
Autorin und Bearbeitung:
Ass. jur. Regine Franz, Geschäftsf. BTQ Kassel
Bildnachweis:
Seite 1: voyager624/Fotolia; Seite 2:castillo-dominici/iStockphoto; Seite 3: Kzenon/Fotolia

Kasten 2

Anlage zu § 9 Satz 1 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Eine Maßnahme nach Satz 2 Nr. 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

BTQ Kassel