Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

Informationen zur Prüfung: „Internationaler Datenverkehr“ durch Datenschutzaufsichtsbehörden

Inhaltsverzeichnis

1. Anlass der Prüfung

Im Zuge der immer stärkeren Vernetzung und Globalisierung der Geschäftsprozesse in der Privatwirtschaft finden inzwischen bis weit in den Mittelstand hinein in erheblichem Umfang Übermittlungen personenbezogener Daten – insbesondere von Kunden- und Mitarbeiterdaten – in Staaten außerhalb der EU und des EWR statt. Betroffen sind hiervon nicht nur große international tätige Konzerne, sondern auch kleinere und mittlere Unternehmen, z.B. wenn sie für bestimmte Geschäftsprozesse auf Leistungen von sog. Cloud-Computing-Anbietern (z.B. Software as a Service) zurückgreifen. Erfahrungen aus den Beratungen der Aufsichtsbehörden insbesondere im Nachgang zur Entscheidung des Europäischen Gerichtshofs vom 6. Oktober 2015 zu Safe Harbor (Rechtssache C-362/14) zeigten, dass manche verantwortlichen Stellen sich gar nicht bewusst sind, dass und welche personenbezogenen Daten sie in Drittländer übermitteln oder, sofern sie sich dessen bewusst waren, verunsichert waren, auf welcher Grundlage sie dies datenschutzkonform durchführen können. Unabhängig von der Bewertung der für den internationalen Datenverkehr zur Verfügung stehenden Mittel, ist durch Verabschiedung des EU-US-Privacy Shields eine neue Situation eingetreten, die von einer großen Anzahl der deutschen Datenschutzaufsichtsbehörden als sinnvoller Zeitpunkt für eine koordinierte Prüfung des internationalen Datenverkehrs angesehen wird.

2. Rechtsvoraussetzungen für die Übermittlung personenbezogener Daten in Drittstaaten

Die Übermittlung personenbezogener Daten in sog. **Drittstaaten** – d.h. Staaten außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR; dies sind die EU-Mitgliedstaaten sowie Norwegen, Island und Liechtenstein) – erfordert gegenüber „innereuropäischen“ Übermittlungen die Erfüllung zusätzlicher datenschutzrechtlicher Anforderungen. Übermittlungen in Drittstaaten sind nur zulässig, wenn sie auf eine spezifische Grundlage gestützt werden können. Welche Grundlagen dafür grundsätzlich zur Verfügung stehen, ist in dem Anschreiben zu dieser Prüfung erläutert.

3. Ablauf der Prüfung

Es handelt sich um eine koordinierte Prüfungsaktion, an der die Datenschutzaufsichtsbehörden aus Bayern, Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und, Sachsen-Anhalt beteiligt sind und innerhalb ihres jeweiligen Zuständigkeitsbereichs mehrere Unternehmen und ggf. sonstige ihrer Aufsicht unterliegende Stellen anschreiben.

4. Ziel der Prüfung

Ziel der Prüfung ist es, dass sich die verantwortlichen Stellen (Unternehmen und sonstige Stellen) einen Überblick darüber verschaffen,

- ob und wenn ja, im Rahmen welcher Geschäftsprozesse das Unternehmen bzw. die sonstige Stelle personenbezogene Daten in Staaten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums übermittelt,
- und, falls solche Übermittlungen stattfinden, auf welcher datenschutzrechtlichen Grundlage dies erfolgt.

Nach den Erfahrungen der Datenschutzaufsichtsbehörden finden aufgrund der zunehmenden Vernetzung und Globalisierung der Geschäftsprozesse sowie im Rahmen von Outsourcing inzwischen bis weit in den Mittelstand hinein Übermittlungen personenbezogener Daten – insbesondere von Kunden- und Mitarbeitern – in Staaten außerhalb der EU und des EWR statt. Unternehmen und andere datenverarbeitende Stellen sollten sich bewusst sein, dass solche Übermittlungen häufiger vorkommen als bisweilen auf den ersten Blick angenommen. Gerade bei Inanspruchnahme externer Dienstleister und von Softwareprodukten „aus der Cloud“ werden häufig personenbezogene Daten, insbesondere solche von Mitarbeitern und/oder Kunden, in Staaten außerhalb der EU und des EWR übermittelt.

Um Unternehmen und anderen datenverarbeitenden Stellen die Beantwortung der Fragen 1 und 2 zu erleichtern, sollen Verarbeitungsvorgänge identifiziert werden, im Rahmen derer personenbezogene Daten in Drittstaaten übermittelt werden können. Dies dient auch dazu, dass die Datenschutzaufsichtsbehörden Kenntnisse darüber erhalten, ob, und wenn ja, auf welcher Grundlage und im Rahmen welcher Geschäftsprozesse Unternehmen und andere datenverarbeitende Stellen personenbezogene Daten in Drittstaaten übermitteln. Dies dient auch einer möglichen näheren Untersuchung bestimmter Produkte (etwa im Bereich Cloud Computing) und einer gezielten Schwerpunktbildung, um bei Bedarf aufsichtlich tätig werden zu können. Daher werden unter Nr. 3 des Fragebogens gezielt einige Bereiche abgefragt, in denen es nach den Erfahrungen der Datenschutzaufsichtsbehörden häufig solche Übermittlungen gibt. Hingegen erfolgt durch Angaben in dem Fragebogen keine generelle Freigabe des jeweils bezeichneten Datenumgangs durch die Aufsichtsbehörde.

- Übermittlungen in Drittstaaten kommen häufig bei international tätigen Unternehmensgruppen/Konzernen vor. Oft werden bestimmte Leistungen zentral durch eine bestimmte Gesellschaft für alle Unternehmen des Konzerns erbracht (sog. Shared Services). Dazu können etwa Leistungen aus

den Bereichen IT-Service, Reisemanagement für Mitarbeiter, Personalverwaltung, E-Mail-Server, Marketing, „Knowledge-Datenbanken“ u.a. gehören.

- Ein weiterer Bereich ist die Inanspruchnahme externer Cloud-Computing-Dienste, oft in der Form des sog. Software as a Service. Bei vielen Cloud-Computing-Anbietern handelt es sich um US-amerikanische Unternehmen. Cloud-Computing-Lösungen gibt es inzwischen für viele der üblichen Datenverarbeitungsprozesse in Unternehmen, z.B. Personalrecruiting / Bewerbermanagement, Customer-Relationship-Management, Organisation von Geschäftsreisen usw.. Anzutreffen sind ferner „Office-Lösungen aus der Cloud“, d.h. Pakete wie etwa Microsoft Office 365 oder Google Apps for Work. Die Verarbeitung der Daten im Rahmen solcher Dienste findet häufig zumindest in Teilen außerhalb der EU und des EWR statt.

- Zur Übermittlung personenbezogener Daten in Drittstaaten kommt es auch im Rahmen des Supports oder der Fernwartung von Hard- und/oder Software (z.B. „follow-the-sun“-Support). Hierbei schalten sich Mitarbeiter z.B. des Herstellers einer bestimmten Unternehmenssoftware und ggf. weitere Dienstleister zur Problemlösung (oft aus einem Nicht-EU-Staat) auf die informationstechnischen Systeme des (Unternehmens-)Kunden auf, wobei grundsätzlich die Möglichkeit der Kenntnisnahme von personenbezogenen Daten (dies ist ausreichend für Qualifizierung als Übermittlung im datenschutzrechtlichen Sinn!) besteht.

Gegenstand der vorliegenden Prüfung ist nur die Übermittlung auf der sog. zweiten Stufe, d.h. die Rechtsfragen, die sich aus der Tatsache ergeben, dass Daten nicht nur übermittelt, sondern in einen Drittstaat übermittelt werden (§§ 4b, 4c BDSG). Eine Prüfung auf der sog. ersten Stufe, d.h. die Frage der Rechtmäßigkeit der Übermittlung gem. § 4 Abs. 1 BDSG, erfolgt nicht. Dies betrifft insbesondere auch die unter Punkt 3 des Fragebogens zu benennenden Produkte.

5. Erläuterungen zum Fragenbogen

Im Folgenden finden Sie Erläuterungen zu dem Fragebogen, die zum besseren Verständnis der gestellten Fragen beitragen und Ihnen das Ausfüllen erleichtern sollen. Die folgende Nummerierung orientiert sich dabei an der Nummerierung des Fragebogens.

1 Übermittlung personenbezogener Daten in die USA

1.1 Bitte geben Sie an, ob Ihr Unternehmen überhaupt personenbezogene Daten in die USA übermittelt. In Betracht kommen sowohl Übermittlungen an „verantwortliche Stellen“ als auch solche an Stellen, die die Daten als Auftragsdatenverarbeiter erhalten. Falls ihre Antwort hier „nein“ lautet, gehen Sie bitte weiter zu 2.

Personenbezogene Daten sind alle „Einzeleingaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (§ 3 Abs. 1 BDSG). Maßgeblich ist somit stets, ob die Person, auf die sich eine Angabe bezieht, zumindest mit Zusatzwissen (z.B. durch das

Unternehmen, bei dem jemand angestellt ist) identifiziert werden könnte. Neben Angaben wie z.B. Name, Funktionsbezeichnung, Telefonnummer, E-Mail-Adresse, postalische Adresse, Bankverbindungsdaten, Daten zur Leistung oder zum Verhalten zählen hierzu z.B. auch persönliche Kennungen, die Nutzern einer Online-Plattform zugeordnet sind und mit der sich der Nutzer bei der Plattform anmeldet, selbst wenn die Kennung selbst keine Bestandteile des „Klarnamens“ des Nutzers enthält.

1.2 Bitte geben Sie an, ob es sich bei den übermittelten Daten um solche von Mitarbeitern, von (End-) Kunden[1] und/oder ggf. von anderen Betroffenen (z.B. Ansprechpartner bei Geschäftspartnern, Lieferanten, Abnehmern etc.) handelt.

1.3 Bitte geben Sie an, auf welcher Grundlage Ihr Unternehmen derzeit personenbezogene Daten in die USA übermittelt. Bitte betrachten Sie dabei alle Fälle, in denen Ihr Unternehmen personenbezogene Daten in die USA übermittelt; sofern mehrere Antworten zutreffend sind, kreuzen Sie bitte alle zutreffenden Antworten an.

Sofern EU-Standardvertragsklauseln als Grundlage genutzt werden, geben Sie bitte an, ob diese unverändert genutzt werden (dann „Standardvertrag“ ankreuzen) oder ob es datenschutzrechtliche Zusatzklauseln gibt. Gerade große Cloud-Dienstleister bieten ihren Kunden oft einen Standardvertrag an, der um weitere datenschutzrechtliche Regelungen ergänzt ist (z.B. gibt es manchmal zusätzliche Regelungen zur Auftragskontrolle oder zur Erteilung von Unteraufträgen). In diesem Fall kreuzen Sie bitte „Standardvertrag mit Zusatzregelungen/Änderungen“ an. Rein „äußerliche“ Änderungen wie etwa die Verwendung eines Deckblatts, und geringfügige Ergänzungen, die ausschließlich der Erfüllung der Voraussetzungen des § 11 Abs. 2 BDSG dienen, stellen dagegen keine „Änderung“ des Standardvertrags in diesem Sinne dar und lösen daher noch keine Genehmigungspflicht aus; gleiches gilt für solche Änderungen, die unzweifelhaft ausschließlich vorteilhaft für die datenschutzrechtliche Position der Betroffenen sind, sowie für rein geschäftliche Klauseln, die keinerlei Auswirkung auf die datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien haben – liegen lediglich solche Änderungen vor, kreuzen Sie daher bitte „Standardvertrag“ an.

Sofern ein Vertrag genutzt wird, der „von vornherein“ bzw. gar nicht die EU-Standardvertragsklauseln beinhaltet, kreuzen Sie bitte „Einzelvertrag“ an.

1.4 Seit 1. August 2016 ist der EU-U.S. Privacy Shield in Kraft. Für US-Unternehmen ist es seit diesem Zeitpunkt möglich, sich gemäß dem Privacy Shield zertifizieren zu lassen. Datenübermittlungen dürfen auf der Grundlage des Privacy Shield nur an solche US-Unternehmen erfolgen, die sich zertifiziert haben. Falls Sie Daten auf der Grundlage des Privacy Shield übermitteln, geben Sie bitte an, wie Sie vorab überprüft haben, ob das Daten empfangende US-Unternehmen eine gültige Privacy-Shield-Zertifizierung besitzt.

[1] Der Begriff „Kundendaten“ ist im Sinne von natürlichen Personen als „Endkunden“ gemeint (z.B. Endkunden eines Unternehmens).

2 Übermittlung personenbezogener Daten in sonstige Drittländer

2.1 Bitte geben Sie an, ob Ihr Unternehmen personenbezogene Daten in andere Drittstaaten (also solche außer den USA) übermittelt.

2.2 Sofern die Antwort zu 2.1 „ja“ lautet, geben Sie bitte alle betreffenden Drittstaaten an. Sofern die Daten zunächst an einen Auftragsdatenverarbeiter in einem bestimmten Drittstaat und von dort anschließend in weitere Drittstaaten (z.B. an Subunternehmer / Unterauftragnehmer) zugeleitet werden (z.B. indem Unterauftragnehmer per Fernzugriff auf die Daten zugreifen können), sind daher alle Drittstaaten zu nennen, in die die Daten auf diese Weise zugeleitet werden.

2.3 Bitte geben Sie an, ob es sich bei den übermittelten Daten um solche von Mitarbeitern, von (End-) Kunden und/oder ggf. von anderen Betroffenen (z.B. Ansprechpartner von Geschäftspartnern, Lieferanten, Abnehmern etc.) handelt.

2.4 Bitte geben Sie an, auf welcher Grundlage Ihr Unternehmen gegenwärtig personenbezogene Daten in sonstige Drittstaaten (also Drittstaaten außer USA) übermittelt. Bitte betrachten Sie dabei alle Fälle, in denen Ihr Unternehmen personenbezogene Daten in sonstige Drittsaaten übermittelt; sofern mehrere Antworten zutreffend sind, kreuzen Sie bitte alle zutreffenden Antworten an.

3 Arten von Übermittlungen

3.1 Im Hinblick auf den Umfang der datenschutzrechtlichen Verantwortung ist zwischen verantwortlichen Stellen und Auftragsdatenverarbeitern zu unterscheiden. „Verantwortliche Stellen“ sind Stellen, die personenbezogene Daten für eigene Geschäftszwecke verarbeiten, während „Auftragsdatenverarbeiter“ die Daten im Auftrag einer verantwortlichen Stelle (Auftraggeber) und nach dessen Weisungen verarbeiten. Bitte geben Sie unter Nr. 3.1 an, ob Sie Übermittlungen in Drittstaaten an „verantwortliche Stellen“, an „Auftragsdatenverarbeiter“ oder ggf. an beide Arten von Empfängern übermitteln. Sofern Sie keine personenbezogene Daten in Drittstaat übermitteln, kreuzen Sie bitte „weder noch“ an.

3.2 - 3.13: Wie oben unter Nr. 3 „Ziel der Prüfung“ dargestellt, gibt es sehr unterschiedliche Geschäftsprozesse, im Rahmen derer u.U. personenbezogene Daten in Drittstaaten übermittelt werden. Um Unternehmen die Auffindung der Übermittlungen personenbezogener Daten in Drittstaaten zu erleichtern, wird unter 3.2 bis 3.13 nach Verarbeitungsvorgängen gefragt, in deren Rahmen es erfahrungsgemäß häufig zu Übermittlungen personenbezogener Daten in Drittstaaten kommt.

3.2 Hier geht es um Übermittlungen, die innerhalb eines Konzerns stattfinden; solche Übermittlungen sind in der Praxis bei grenzüberschreitend tätigen Konzernen sehr häufig, gerade mit Blick auf Mitarbeiterdaten. Ein häufiges Einsatzfeld ist z.B. die Lohnabrechnung. Darüber hinaus gibt es auch häufig mehr oder weniger zentralisierte Personaldatenbanken in Konzernen oder zumindest Zugriffsmög-

lichkeiten von konzernangehörigen Unternehmen aus Drittstaaten auf Mitarbeiterdaten im Inland. Auch solche Zugriffe stellen Übermittlungen in einen Drittstaat dar (§ 3 Abs. 4 Satz 2 Nr. 3 b BDSG). Geben Sie unter Nr. 3.2 insgesamt an, ob Sie personenbezogene Daten an Unternehmen, die demselben Konzern angehören, mit Sitz in Drittstaaten übermitteln.

3.3 bis 3.13: Hier werden einige typische Dienstleistungen externer Anbieter (insbesondere Cloud-Lösungen) aufgezählt, bei denen es vielfach zu einer Übermittlung personenbezogener Daten in Drittstaaten kommt. Die Anbieter solcher Dienste sind häufig US-amerikanische Unternehmen, die entsprechenden Datenverarbeitungen finden hierbei oft in Drittstaaten statt. Selbst in Fällen, in denen die eigentliche Datenspeicherung in der EU stattfindet, gibt es häufig eine „Spiegelspeicherung“ z.B. in den USA. Daneben gibt es zahlreiche Datenzugriffe auf (in der EU gespeicherte) Daten im Rahmen des Supports oder der Fernwartung auch aus den USA und/oder aus anderen Drittstaaten. Auch ein Fernzugriff aus einem Drittstaat auf in der EU gespeicherte Daten ist datenschutzrechtlich als „Übermittlung in einen Drittstaat“ zu qualifizieren, so dass auch bei einem solchen Fernzugriff eine Grundlage für die Übermittlung in Drittstaaten notwendig ist. Geben Sie zunächst durch Ankreuzen an, ob Sie entsprechende Dienstleistungen, bei denen personenbezogene Daten in Drittstaaten übermittelt werden, in Ihrem Unternehmen überhaupt in Anspruch nehmen. Wenn Sie dies mit „ja“ beantworten, zählen Sie bitte anschließend konkret den jeweiligen Anbieter und das betreffende Produkt bzw. den betreffenden Dienst auf (bspw. Microsoft Office 365, Salesforce Sales Cloud, Google Apps for Works, …).

3.5 Viele Unternehmen lassen Geschäftsreisen von Mitarbeitern durch Schwesterunternehmen (d.h. durch ein anderes konzernangehöriges Unternehmen) bearbeiten; sofern das bearbeitende Unternehmen seinen Sitz in einem Drittstaat hat, kommt es dabei zur Übermittlung personenbezogener Daten in einen Drittstaat. Daneben gibt es aber auch spezialisierte Reisemanagement-Dienstleister, die derartige Leistungen anbieten (z.B. den US-Anbieter Carlson Wagonlit Travel) oder Software-as-a-Service-Produkte wie etwa Sabre.

3.6 Auch CRM-Systeme und Marketing-Systeme gehören inzwischen zu den wohl am häufigsten verbreiteten Cloud-Produkten. Zu nennen sind hier etwa CRM-Systeme von Anbietern wie Salesforce, Microsoft (etwa Microsoft Dynamics CRM), Zoho oder Marketing-Systeme wie etwa Oracle Eloqua.

3.7 Cloud-Produkte (meist als sog. Software as a Service) werden auch im Bereich der Personalgewinnung (Bewerbermanagement, Recruiting) eingesetzt. Ein Beispiel wäre etwa der US-Anbieter Jobvite. Sofern Sie solche Produkte einsetzen, und beim Einsatz personenbezogene Daten (auch) in Drittstaaten übermittelt werden, kreuzen Sie bitte „ja“ an.

3.8 Gemeint ist die Inanspruchnahme von Speicherplatz bei externen Anbietern, etwa im Rahmen von Google Drive, SAP Hana, Box.com, Amazon Cloud, Microsoft OneDrive etc.

3.9 Bitte geben Sie hier an, ob Sie externe E-Mail-Provider für die geschäftliche Kommunikation von Mitarbeitern einsetzen (z.B. Microsoft Exchange Online). Des Weiteren geben Sie bitte auch etwaige ex-

terne Dienstleister für die Versendung von Newslettern an natürliche Personen (insb. Endkunden) an, z.B. Anbieter wie Mailchimp.

3.10 Hier sind Cloud-Pakete mit Office-Anwendungen gemeint, z. B. Microsoft Office 365 oder Google Apps for Works, die aus verschiedenen Modulen bestehen. Bitte antworten Sie auch dann mit „ja“, wenn Sie nur einzelne Module aus solchen Paketen nutzen.

3.11 An dieser Stelle sind Plattformen externer Anbieter anzugeben, die für die Zusammenarbeit von Mitarbeitern aus unterschiedlichen Unternehmens-/Konzerneinheiten genutzt werden, z.B. für die gemeinsame Dokumentbearbeitung, Videokonferenzen, Chat- oder Messaging-Systeme. Bitte kreuzen Sie auch dann „ja“ an, wenn solche Produkte ggf. Teil von Paketen sind, die auch unter Nr. 3.10 fallen.

3.12 Cloud-Lösungen gibt es auch im Bereich der sog. Ticketbearbeitung, d.h. bei der Bearbeitung von (z.B. Support-)Anfragen eigener Kunden. Beispiele wären etwa Zendesk oder ServiceNow.

3.13 Die hier erwähnten Bereiche „Qualitätsmanagement“, „Risikomanagement“ und „Compliance“ werden in der Praxis gelegentlich unter dem Oberbegriff Compliance zusammengefasst. Bitte geben Sie im Zweifel alle derartigen Produkte bzw. Dienste an, die Sie im weiteren Sinne unter dem Begriff Compliance zuordnen würden, sofern dabei personenbezogene Daten in Drittstaaten übermittelt werden könnten.

3.14 Um eine vollständigen Überblick darüber zu bekommen, in welchen Bereichen die Übermittlung personenbezogener Daten in Drittstaaten erfolgt, werden hier als Auffangfrage die sonstigen - nicht schon bei den Fragen 3.3 bis 3-13 angesprochenen - Bereiche abgefragt, etwa Leistungen im Bereich dessen, was herkömmlich als „Consulting“ bezeichnet wird. Ein Beispiel wäre der Anbieter MARSH, der umfassend Beratung zu Personal-, aber auch zu Versicherungsfragen sowie die Abwicklung von Schadensersatzansprüchen anbietet.

4 Betrieblicher Datenschutzbeauftragter

Verantwortliche Stellen haben unter den in § 4f BDSG genannten Fällen einen betrieblichen Datenschutzbeauftragten zu bestellen. Betriebliche Datenschutzbeauftragte sollen in den jeweiligen Unternehmen auf die Einhaltung datenschutzrechtlicher Vorschriften hinwirken. Sie sind deshalb über den Einsatz von Datenverarbeitungsprogrammen, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu unterrichten. Ferner ist ihnen eine Übersicht über die entsprechenden Verfahren zur Verfügung zu stellen. Die Fragen dieses Abschnitts zielen darauf ab, festzustellen, ob die gesetzliche Verpflichtung, bei Vorliegen der Voraussetzungen einen Datenschutzbeauftragten bestellt zu haben erfüllt ist und dieser seine Aufgabe – bezogen auf den Fokus dieser Prüfung – ordnungsgemäß erfüllen kann.