Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14

Dieses Positionspapier richtet sich an nichtöffentliche und öffentliche Stellen in ihrer Funktion als verantwortliche Stellen für Datenverarbeitungen (§ 3 Abs. 7 BDSG/§ 2 Abs. 3 LDSG) und soll verdeutlichen, welche Folgen das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein aus dem „Safe-Harbor-Urteil" des Gerichtshofs der Europäischen Union (EuGH) vom 06.10.2015, C-362/14, zieht.

Zunächst wird dargestellt, welche Aussagen der EuGH in seinem Urteil getroffen bzw. nicht getroffen hat (1). Das Positionspapier nimmt danach Stellung zu der Frage, welche Handlungsoptionen nach dem Urteil für die EU-Kommission bestehen (2), auf Basis welcher Rechtsgrundlagen eine Übermittlung personenbezogener Daten in die USA noch in Betracht kommt bzw. nicht mehr zulässig ist (3) und wie mit den Standardvertragsklauseln umzugehen ist (4). Schließlich wird dargestellt, welche Auswirkungen die gerichtliche Entscheidung – soweit dies derzeit absehbar ist – auf die Prüftätigkeit des ULD hat (5).

1. Inhalt des Urteils

Der EuGH hat die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt. Während die darin geregelte Selbstzertifizierung US-amerikanischer Unternehmen bisher als Grundlage für Datenübermittlungen in die USA herangezogen wurde, ist dies mit Verkündung des Urteils nicht mehr zulässig.

Allem voran nimmt der EuGH Bezug auf Mitteilungen der Kommission an das Europäische Parlament und den Rat aus November 2013, in denen die Kommission diverse Schutzlücken ihrer Safe-Harbor-Entscheidung darstellt. Mit Blick auf diese Feststellungen der Kommission selbst macht der EuGH in seinem Urteil deutlich, dass die Safe-Harbor-Entscheidung ungültig ist, weil sie keine ausreichende Begrenzung der Zugriffe von staatlichen Behörden bewirke. Ebenso fehle es in der Safe-Harbor-Entscheidung an jeder Feststellung über ausreichende Rechtsschutzmöglichkeiten für europäische Bürgerinnen und Bürger. Ohne das Rechtssystem der USA konkret zu bewerten, stellt der EuGH abstrakt fest, dass nationale Regelungen, die es generell gestatten, auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzen.

Zudem schränke die Safe-Harbor-Entscheidung die Aufsichtsbefugnisse der europäischen Datenschutz-Aufsichtsbehörden zu sehr ein und halte sich nicht an die Vorgaben, auf Basis derer die Kommission über das Schutzniveau eines Drittstaates entscheiden könne. Statt wie es Art. 25 Abs. 6 der Richtlinie 95/46/EG verlangt, habe die Kommission keine Aussage über das Datenschutzniveau in den USA getroffen, sondern mit den Safe-Harbor-Grundsätzen eine untaugliche Hilfskonstruktion als Ersatz für das unangemessene Schutzniveau gewählt.

Der EuGH hat damit nicht abschließend über das in den USA geltende Schutzniveau geurteilt, sondern das Verfahren zur Klärung dieser konkreten Fragen an das irische Ausgangsgericht zurücküberwiesen.

2. Handlungsmöglichkeiten der EU-Kommission

a) Die Kommission könnte auf Basis von Art. 25 Abs. 6 der Richtlinie 95/46/EG eine neue Entscheidung erlassen, in der sie feststellt, dass die USA ein angemessenes Schutzniveau bieten. Hierzu wäre u.a. das Folgende zu beachten:

   Das datenschutzrechtliche Schutzniveau in den USA für die Freiheiten und Grundrechte der Betroffenen muss nach den Vorgaben des EuGH im Licht der Grundrechtecharta dem europäischen Schutzniveau gleichwertig sein. Nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben die Enthüllungen von Edward Snowden offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen und damit die Safe-Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden. Die USA können deshalb keine innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen vorweisen, die ein angemessenes Schutzniveau bieten.

   Nach den Vorgaben des EuGH erfordert die Annahme eines angemessenen Schutzniveaus einen wirksamen gerichtlichen Rechtsschutz für europäische Bürgerinnen und Bürger gegen Eingriffe in das Grundrecht auf Achtung der Privatsphäre. Es darf kein genereller Zugriff der staatlichen US-Behörden auf elektronische Kommunikation erfolgen, da dies gegen den Wesensgehalt von Art. 7 der Grundrechtecharta verstoßen würde. Haben EU-Bürgerinnen und -Bürger keine Möglichkeit, Zugang zu ihren personenbezogenen Daten zu erlangen bzw. gerichtlichen Rechtsschutz in Anspruch zu nehmen, läge ein Verstoß gegen Art. 47 der Grundrechtecharta vor.

   Bei der Prüfung des angemessenen Datenschutzniveaus müsste die Kommission auf bestehende sowie gesetzlich flankierte Schutzmechanismen und Regulierungsinstrumente in den USA abstellen und diese einer Adäquanzprüfung unterziehen. Ein von der Kommission selbst entwickeltes Regulierungsinstrument wie die Safe-Harbor-Grundsätze sind vor diesem Hintergrund nicht tragfähig und würden diesen Anforderungen nicht im Ansatz genügen.

b) Die Kommission könnte einen völkerrechtlichen Vertrag wie etwa ein Datenschutzabkommen mit den USA forcieren. Dieser völkerrechtliche Vertrag müsste insbesondere die Anforderungen der Art. 7, 8 Abs. 1 und 47 Abs. 1 der Grundrechtecharta erfüllen. Auch hierzu müssten die USA zunächst die inländische Datenverarbeitung gesetzlich regeln und dabei vor allem den generellen und zweckfreien Zugriff auf den Inhalt der elektronischen Kommunikation einstellen und einen wirksamen gerichtlichen Rechtsschutz für die EU-Bürgerinnen und Bürger vorsehen. Nach den Vorgaben des EuGH müssen ausreichende Garantien zum Schutz der Grundfreiheiten/Grundrechte der EU-Bürgerinnen und Bürger gerade im Hinblick auf die automatisierte Datenverarbeitung hin vorgesehen werden.

Ergebnis: Eine Entscheidung der Kommission zur Angemessenheit des Datenschutzniveaus in den USA erfordert ebenso wie der Abschluss eines völkerrechtlichen Datenschutzabkommens eine umfassende Änderung US-amerikanischen Rechts. Da entsprechende Änderungen derzeit nicht zu erwarten sind, scheiden beide Handlungsoptionen kurz- oder mittelfristig aus.

3. Rechtsgrundlagen für die Übermittlung personenbezogener Daten

Die Übermittlung personenbezogener Daten in Länder, in denen kein angemessenes Datenschutzniveau besteht, muss für nichtöffentliche Stellen anhand von § 4c Abs. 1 des Bundesdatenschutzgesetzes (BDSG), für öffentliche Stellen in Schleswig-Holstein nach § 16 Abs. 2 des Landesdatenschutzgesetzes (LDSG) beurteilt werden. Dabei ergeben sich für den Datentransfer in die USA folgende Leitlinien:

a) § 4c Abs. 1 Nr. 1 BDSG und § 16 Abs. 2 Satz 2 Nr. 1 LDSG legitimieren eine Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau auf Basis einer Einwilligung des Betroffenen. Die Einwilligung muss „ohne jeden Zweifel" gegeben werden, Art. 26 Abs. 1 Buschstabe a der Richtlinie 95/46/EG, Art. 29-Datenschutzgruppe, WP 187, S. 32. Eine wirksame Einwilligungserklärung erfordert nicht nur eine Aufklärung über die Zwecke, sondern auch über die Risiken der Datenverarbeitung bzw. den damit verbundenen Verzicht auf ein gleichwertiges bzw. angemessenes Schutzniveau. Der Betroffene müsste daher zunächst umfassend über das fehlende Schutzniveau, vor allem über US-staatliche Zugriffsbefugnisse, fehlende Rechtsschutzmöglichkeiten/Betroffenenrechte, Weiterverarbeitung der Daten ohne Zweckgebundenheit, die Nichtgeltung des Erforderlichkeitsgrundsatzes sowie über fehlende staatliche Kontrollmechanismen in den USA aufgeklärt werden.

   Für die Wirksamkeit einer Einwilligungserklärung muss insbesondere immer eine Aufklärung über die konkreten Zwecke der Verarbeitung erfolgen, § 4a Abs. 1 Satz 2 BDSG. Schließlich wäre für die Einwilligung erforderlich, dass eine Erklärung „für den konkreten Fall" bzw. für eine konkrete Datenverarbeitung abgegeben wird, Art. 29-Datenschutzgruppe, WP 187, S. 20 ff. Eine Generalerklärung für eine Vielzahl von nicht übersehbaren Datenverarbeitungen wird regelmäßig unzulässig sein. Speziell in Beschäftigungsverhältnissen würde den Beschäftigten hinsichtlich ihrer Erklärungen auch keine Wahlfreiheit verbleiben, soweit der Arbeitgeber eine Einwilligung für die Übermittlung ihrer personenbezogenen Daten in die USA verlangt. Es würde keine freie Entscheidung im Sinne von § 4a Abs. 1 BDSG, § 12 Abs. 2 LDSG vorliegen und damit keine wirksame Erklärung. Sehen US-amerikanische Vorschriften eine nicht zweckgebundene Datenverarbeitung durch staatliche Behörden vor, so scheitert bereits hieran die wirksame Einwilligung.

   Selbst bei ausreichender Information über die Risiken und auch in Fällen, in denen noch von einer Freiwilligkeit ausgegangen werden könnte, würde die Einwilligung grundsätzlichen Bedenken begegnen. Die anlasslose Massenüberwachung durch Geheimdienste greift nach Ansicht des EuGH in den Wesensgehalt des Grundrechts auf Achtung des Privatlebens ein. Derartige Eingriffe sind nach bundesverfassungsgerichtlicher Rechtsprechung jedoch der Disposition des Einzelnen, auch im Wege einer Einwilligung, entzogen. Dies kann sich auch auf die Einwilligung in die Datenübermittlung in einen Staat erstrecken, in dem der Wesensgehalt der Grundrechte der EU nicht gewahrt wird. Die Aufnahme einer solchen Einwilligung etwa in Allgemeine Geschäftsbedingungen wäre mit größter Wahrscheinlichkeit sittenwidrig im Sinne des § 138 BGB.

   Ergebnis: Die Einwilligung nach § 4a BDSG, § 12 LDSG scheidet nach den obigen Ausführungen als Rechtsgrundlage für die Zulässigkeit der Übermittlung trotz fehlenden angemessenen Datenschutzniveaus aus.

b) Im Bereich der Privatwirtschaft kommen als Rechtsgrundlagen im Wesentlichen nur § 4c Abs. 1 Nr. 2 und 3 BDSG in Betracht. Demnach ist die Datenübermittlung zulässig für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, soweit dies erforderlich ist, § 4c Abs. 1 Nr. 2 BDSG. Erfasst sind hiervon etwa Reise- und Flugbuchungen. Weiterhin wäre die Datenübermittlung zulässig, sofern diese zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll, § 4c Abs. 1 Nr. 3 BDSG. Beide Tatbestände bilden jedoch keine Übermittlungsgrundlagen für Beschäftigtendaten, welche in den USA z.B. zur Leistungs- oder Verhaltenskontrolle verarbeitet werden.

4. Umgang mit Standardvertragsklauseln durch nichtöffentliche Stellen

Exemplarisch wird auf Klausel 5 Buchstabe b des Beschlusses der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittstaaten vom 5. Februar 2010 (2010/87/EU) verwiesen. Demnach garantiert der Datenimporteur gegenüber dem europäischen Datenexporteur unter anderem, dass er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen. Genau diese vertragliche Pflicht können US-amerikanische Vertragspartner mit Blick auf das in den USA geltende Recht aber nicht einhalten. Der Datenexporteur ist in derartigen Fällen berechtigt, die Datenübermittlung auszusetzen oder den Standardvertrag zu kündigen. Gleiches gilt z.B. nach Klausel 5 Buchstabe b des Beschlusses der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittstaaten vom 27. Dezember 2001 (2002/16/EG) und nach Klausel 5 Buchstabe a des Beschlusses der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittstaaten vom 15. Juni 2001 (2001/497/EG).

Ergebnis: Nichtöffentliche Stellen, die für ihren Datentransfer in die USA Standardvertragsklauseln verwenden, müssen nun in Erwägung ziehen, den zugrunde liegenden Standardvertrag mit dem Datenimporteur in den USA zu kündigen oder die Datenübermittlungen auszusetzen. In konsequenter Anwendung der Vorgaben des EuGH in seinem Urteil ist eine Datenübermittlung auf Basis von Standardvertragsklauseln nicht mehr zulässig.

5. Prüftätigkeit des ULD gegenüber nichtöffentlichen Stellen

a) Im Bereich der Standardvertragsklauseln – exemplarisch Art. 4 Buchstabe a des Beschlusses der Kommission vom 5. Februar 2010 (2010/87/EU) – können die Aufsichtsbehörden Datenübermittlungen in die USA per verwaltungsrechtlicher Anordnung verbieten oder aussetzen. Die Anordnung ist möglich, wenn der Datenimporteur oder Unterauftragsverarbeiter nach den geltenden US-Vorschriften sich nicht an europäisches Datenschutzrecht/die Vorgaben der Standardvertragsklauseln halten können und die Anforderungen nach Art. 13 der Richtlinie 95/46/EG erfüllt sind. Die Datenexporteure aus Europa können dies nur abwenden, indem sie von ihrem vertraglich bestehenden Recht

Gebrauch machen, den Standardvertrag mit dem US-Datenimporteur aufzukündigen (exemplarisch Klausel 5 b des Beschlusses der Kommission vom 5. Februar 2010 – 2010/87/EU).

b) Die Übermittlung personenbezogener Daten in die USA ohne Rechtsgrundlage erfüllt den Bußgeldtatbestand nach § 43 Abs. 2 Nr. 1 BDSG und kann mit einem Bußgeld in Höhe von bis zu 300.000 € geahndet werden.

Ergebnis: Das ULD wird prüfen, ob Anordnungen gegenüber nichtöffentlichen Stellen getroffen werden müssen, auf deren Basis Datenübermittlungen in die USA ausgesetzt oder verboten werden müssen. Ferner ist zu prüfen, ob nichtöffentliche Stellen infolge der Datenübermittlung in ein Drittland mit fehlendem angemessenem Datenschutzniveau Ordnungswidrigkeiten verwirklicht haben.

Kontakt:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Tel: 0431 988-1200, Fax: -1223
E-Mail: mail@datenschutzzentrum.de