LfD Niedersachsen 17.12.15
LfD 4.2

Positionspapier der Landesbeauftragten für Datenschutz Niedersachsen zum Safe Harbor-Urteil des Europäischen Gerichtshofs vom 06.10.15

Für die Übermittlung personenbezogener Daten in ein Nicht-EU-Land ist eine Rechtsgrundlage erforderlich. Das Safe Harbor-Abkommen für die USA, die EU-Standardvertragsklauseln oder Binding Corporate Rules (BCR) konnten bisher als eine solche Rechtsgrundlage genutzt werden.
Mit Urteil vom 06.10.15 hat der EuGH das Safe Harbor-Abkommen jedoch für ungültig erklärt. Dies hat gravierende Auswirkungen auf die Zulässigkeit des Datentransfers in die USA.

1) Safe Harbor-Abkommen:

Das zwischen der EU und den USA vereinbarte Safe Harbor-Abkommen bot Unternehmen eine einfache und günstige Möglichkeit und Rechtsgrundlage für einen zulässigen transatlantischen Datentransfer.
Die EU-Kommission hat mit der Safe Harbor-Vereinbarung (Entscheidung 2000/520 vom 26.07.2000) festgestellt, dass in den USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Datenschutzniveau besteht. Verpflichtete sich ein US-Unternehmen zur Einhaltung der im Abkommen festgelegten Datenschutz-Grundsätze und ließ sich bei dem Handelsministerium der USA entsprechend registrieren, war nach dem Abkommen generell davon auszugehen, dass ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet ist (Art. 1 des Abkommens). Nur unter engen Voraussetzungen durften die Aufsichtsbehörden der Mitgliedstaaten dann nach Einzelfallprüfung den Datentransfer aussetzen (Art. 3 des Abkommens).
Durch die Snowden-Enthüllungen wurde aufgedeckt, dass US-Behörden massenhaft, ohne konkreten Anlass, auf bei Unternehmen gespeicherte personenbezogene Daten zugreifen. Die Safe Harbor-Zertifizierung bzw. –Verpflichtung bietet hiervor keinen Schutz. Dies haben die Datenschutzbeauftragten des Bundes und der Länder bereits in ihrer Konferenz am 18./19.03.15 kritisiert und Datenübermittlungen in die USA wurden insgesamt sehr kritisch gesehen.

2) EuGH-Urteil vom 06.10.15:

Der EuGH hat in seinem Urteil das Safe Harbor-Abkommen insgesamt für ungültig erklärt. Für die Feststellung eines angemessenen Schutzniveaus in einem Drittland muss gewährleistet sein, dass in dem Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder

internationaler Verpflichtungen tatsächlich ein Datenschutzniveau besteht, welches dem in der EU herrschenden gleichrangig ist. Die Kommission hat dieses Datenschutzniveau regelmäßig zu überprüfen. Angesichts der schon im Abkommen selbst enthaltenen generellen rechtlichen Möglichkeit der US-Behörden, die Safe Harbor-Grundsätze aus Gründen der nationalen Sicherheit oder des öffentlichen Interesses auszusetzen (s. Art. 4 von Anhang I), und der fehlenden Rechtsschutzmöglichkeiten für EU-Bürger nach US-Recht war das Safe Harbor-Abkommen von Anfang an nicht geeignet zur Garantie ausreichender Sicherheiten für die informationelle Selbstbestimmung der EU-Bürger. Die US-Behörden, insbesondere die Geheimdienste, haben quasi ungehinderten Zugang ohne konkreten Anlass zu den personenbezogenen Daten und ohne wirksamen Rechtsschutz für die Betroffenen. Insbesondere der ungehinderte und generelle Zugriff auf elektronische Kommunikationsdaten widerspricht jeglichen europäischen Datenschutzgrundsätzen. Das Fehlen von Rechtsschutzmöglichkeiten für EU-Bürger verletzt das Grundrecht auf wirksamen gerichtlichen Rechtsschutz.

In ihrem Positionspapier vom 26.10.15 haben sich die Datenschutzaufsichtsbehörden von Bund und Ländern zu den Auswirkungen des EuGH-Urteils geäußert.[1] Auch die Art. 29-Gruppe als Zusammenschluss der europäischen Datenschutzaufsichtsbehörden hat in einem Positionspapier Stellung genommen und insbesondere eine Frist bis Ende Januar für die Bewertung der rechtlichen Auswirkungen gesetzt. [2]

3) Folgerungen für den Datentransfer in die USA:

Das Safe Harbor-Abkommen kann nicht mehr als Rechtsgrundlage für den Datentransfer in die USA genutzt werden.

Darüber hinaus ergeben sich Folgerungen für die anderen Rechtsgrundlagen für den internationalen Datenverkehr. Insbesondere lassen die Feststellungen des Urteils die EU-Standardvertragsklauseln in einem problematischen Licht erscheinen. Mindestens ist hier nach den Vorgaben des EuGH zu überprüfen, ob personenbezogene Daten vor einem willkürlichen Zugriff durch Dritte ausreichend geschützt sind und ob Rechtsschutzmöglichkeiten für die betroffenen Personen bestehen.

Bei Verwendung von Binding Corporate Rules (BCR) oder eigenen Vertragslösungen müssen diese ebenfalls den Vorgaben des EuGH genügen; denkbar sind etwa zusätzliche Garantien bezüglich der Verschlüsselung der Daten oder größtmögliche Transparenz bei ungewollten Zugriffen durch Dritte. Hier ist eine Bewertung im Einzelfall herbeizuführen.

Die Einwilligung der betroffenen Person ist grundsätzlich als Ausnahmefall restriktiv zu verwenden und in massenhaften Routinefällen schon daher keine Lösung. Wegen der

[1] Das Positionspapier ist auf unserer Webseite www.lfd.niedersachsen.de abrufbar.
[2] Das Statement der Art. 29-Gruppe ist auf unserer Webseite www.lfd.niedersachsen.de abrufbar.

Möglichkeit des jederzeitigen Widerrufs durch die betroffene Person ist die Einwilligung auch aus praktischen Gründen wenig effektiv.
Die Datenschutzaufsichtsbehörden und weitere Gremien auf nationaler und auf europäischer Ebene prüfen derzeit verschiedene Gesichtspunkte und Folgerungen aus dem Urteil, um bis Ende Januar zu einer einheitlichen rechtlichen Position insbesondere hinsichtlich der oben genannten Rechtsinstrumente zu gelangen. Daneben verhandeln die EU-Kommission und Vertreter der US-Behörden über ein neues Safe Harbor-Abkommen unter Berücksichtigung der EuGH-Entscheidung.

4) Pflichten der datenexportierenden Stelle*:*
Die Verantwortung für einen datenschutzgerechten Umgang mit den exportierten personenbezogenen Daten liegt bei dem übermittelnden Unternehmen. Die Unternehmen sind daher verpflichtet, selbst eine rechtliche Bewertung ihres Datenexports in die USA unter den oben genannten Vorgaben durchzuführen und ggf. das eigene weitere Vorgehen zu prüfen.
Die datenexportierende Stelle sollte zunächst ihre Datenströme überprüfen und ggf. kategorisieren: welche Arten von personenbezogenen Daten werden übermittelt, zu welchem Zweck werden diese übermittelt und welche Rechtsgrundlage wird derzeit hierfür genutzt. Ein Datentransfer auf Grundlage des Safe Harbor-Abkommens ist sofort zu beenden, entsprechende Verträge mit Unternehmen in den USA sind zu kündigen, es ist eine Löschung der dort gespeicherten Daten zu verlangen. Um Rechtssicherheit zu erlangen und unabhängig von den weiteren rechtlichen und politischen Entwicklungen zu werden, ist eine Abkehr von einem Datentransfer in die USA allgemein in Betracht zu ziehen. Dies kann erreicht werden durch einen Wechsel zu europäischen Auftragsdatenverarbeitern bzw. anderen Dienstleistern oder je nach Organisationsstruktur des Unternehmens eine Speicherung der eigenen Daten ausschließlich auf Servern in Europa. Muss der Datentransfer in die USA weiter erfolgen, sind weitere technisch-organisatorische Maßnahmen ratsam wie verbesserte Verschlüsselung der Daten, Verwendung von Pseudonymen. Hierbei können die Orientierungshilfe Cloud Computing vom 09.10.14 der Datenschutzkonferenz und die Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ der Datenschutzkonferenz vom 27.03.14 herangezogen werden.[3] Diese Maßnahmen können im Einzelfall den Anforderungen an einen ausreichenden Datenschutz genügen.

5) Weiteres Vorgehen der Landesdatenschutzbeauftragten in Niedersachsen:
Zunächst wird die Landesdatenschutzbeauftragte Niedersachsen die Unternehmen und betroffenen Personen (weiterhin) über die veränderte Rechtslage und die weiteren Entwicklungen informieren und beraten. Im Rahmen der nationalen und europäischen

[3] Die Orientierungshilfe und die Entschließung sind auf unserer Webseite www.lfd.niedersachsen.de abrufbar.

Abstimmung werden derzeit unter Beteiligung der Landesdatenschutzbeauftragten Niedersachsen die Folgerungen des Urteils für die Rechtsinstrumente Standardvertragsklauseln, BCR etc. überprüft. Während dieser Überprüfung wird die Landesdatenschutzbeauftragte Niedersachsen grundsätzlich keine Beanstandungen oder Untersagungen von einzelnen Datentransfers in die USA aussprechen, es sei denn es handelt sich um einen schwerwiegenden Einzelfall. Umgekehrt werden keine neuen Genehmigungen für solche Datenübermittlungen erteilt. Grundlage des weiteren Handelns werden die Ergebnisse der Abstimmung auf nationaler und europäischer Ebene sein. Unter der Prämisse eines einheitlichen Vorgehens der Datenschutzaufsichtsbehörden wird die Landesdatenschutzbeauftragte Niedersachsen nach Ende der rechtlichen Abstimmung anlassunabhängige Überprüfungen der transatlantischen Datenströme durch niedersächsische Unternehmen durchführen.