



ZUSAMMENFASSUNG

1. EuGH verbietet „Safe Harbor“-Datenübermittlungen in die USA

- Unternehmen müssen prüfen und gegebenenfalls handeln.

2. Hohes Bußgeld für zu knappen Auftragsdatenverarbeitungsvertrag

- Aufsichtsbehörde verhängt fünfstelliges Bußgeld, weil Datensicherheitsmaßnahmen nicht exakt beschrieben waren.

3. Daten-Empfänger müssen korrekt identifiziert werden

- Personalausweiskopie ist ungeeignet.

4. Frage nach Telefon-Werbe-Zustimmung kann unzulässig sein

- Zulässige Anrufe werden durch Frage zu unzulässiger Telefonwerbung.

1. EuGH verbietet „Safe Harbor“-Datenübermittlungen in die USA

Der Gerichtshof der Europäischen Union hat die „Safe Harbor“-Regeln zur Datenübermittlung in die USA am 6. Oktober 2015 für ungültig erklärt. Unternehmen, die sich bisher auf „Safe Harbor“ verlassen haben, müssen nun reagieren.

Bisher waren Übermittlungen personenbezogener Daten in die USA zulässig, wenn sich das US-Unternehmen den „Safe Harbor“-Regeln unterworfen hat. So konnten Unternehmen auf relativ einfache Weise zum Beispiel Cloud-Services in den USA nutzen, Mitarbeiter- oder sonstige Daten in Konzerndatenbanken bei der US-Mutter verarbeiten oder im Rahmen komplexer Outsourcing-Projekte ihre IT in die USA verlagern.

Der EuGH hat „Safe Harbor“ jedoch ohne Übergangsfrist für ungültig erklärt. Aufsichtsbehörden haben bereits mitgeteilt, dass sie derzeit verschiedene Unternehmen im Hinblick auf „Safe Harbor“ prüfe und ein weiteres Vorgehen nur bis zum EuGH-Urteil zurückstelle.

Als alternative Erlaubnisnorm für Datenübermittlungen in „Drittstaaten“ wie die USA kommen nach einer Entscheidung der EU-Kommission die so genannten EU-Standardvertragsklauseln in Betracht. Diese können zwischen dem Auftraggeber in Europa und dem Auftragnehmer im Drittstaat vereinbart werden. Doch hat

der EuGH festgestellt, dass Regelungen, die Geheimdiensten einen faktisch unbeschränkten Zugriff auf elektronische Kommunikation ermöglichen, mit den europäischen Grundrechten nicht vereinbar sind. Damit besteht das Risiko, dass auch die EU-Standardvertragsklauseln eine Verletzung europäischer Datenschutzgrundsätze nicht ausräumen können, denn Verträge zwischen Unternehmen können naturgemäß nicht die Befugnisse von US-Behörden beschränken.

Bezüglich der Standardvertragsklauseln besteht allerdings in jedem Fall eine faktische Übergangsregelung: Der EuGH hat auch entschieden, dass nur er selbst eine Entscheidung der EU-Kommission für ungültig erklären kann. Bis also der EuGH eine entsprechende Entscheidung trifft, dürfte eine Berufung auf die Entscheidung der EU-Kommission weiter möglich bleiben.

Es gibt noch weitere Möglichkeiten, rechtmäßig Daten in die USA zu transferieren, etwa verbindliche Unternehmensregeln (Binding Corporate Rules, BCR), die etliche Konzerne vereinbart haben. Diese sind von der EuGH-Entscheidung zunächst nicht betroffen. Eine weitere Möglichkeit sind Einzelfallgenehmigungen durch die Aufsichtsbehörden, wobei nach dem EuGH-Urteil fraglich ist, wie oft diese künftig noch erteilt werden.

Von der aktuellen Entscheidung nicht betroffen sind Datenverarbeitungen in der EU oder dem Europäischen Wirtschaftsraum (EWR), und zwar auch dann nicht, wenn die Server von US-Unternehmen oder ihren Tochtergesellschaften betrieben werden. Ein europäisches Unternehmen kann daher auch nach dem EuGH-Urteil noch einen so genannten Auftragsdatenverarbeitungsvertrag mit einem US-Unternehmen schließen, wenn die Daten etwa in Irland verarbeitet werden. Hier haben die deutschen Aufsichtsbehörden zwar auch Bedenken angemeldet, aber uns ist kein Fall bekannt, in dem eine Behörde tatsächlich gegen einen solchen Vertrag vorgegangen wäre. Wichtig ist aber auch hier ein den gesetzlichen Anforderungen entsprechender Vertrag – sonst drohen Bußgelder von bis zu 50.000 Euro.

Da davon auszugehen ist, dass die Aufsichtsbehörden spätestens dann Datenübermittlungen in die USA genauer prüfen werden, wenn erste Gespräche über ein

abgestimmtes Vorgehen erfolgt sind, und Bußgelder im sechsstelligen Bereich drohen, sollten Unternehmen die verbleibende Zeit für eine Prüfung nutzen, ob und wenn ja auf welcher Rechtsgrundlage sie personenbezogene Daten an Dritte übermitteln. Dazu gehören auch Auftragsdatenverarbeitungen außerhalb des EU-/EWR-Gebietes – etwa die Nutzung von Cloud-Services in den USA oder gar nur eines E-Mail-Accounts bei einem US-Unternehmen. War die Rechtsgrundlage bisher „Safe Harbor“ oder fehlte sie gar ganz, besteht dringender Handlungsbedarf.

EU-Kommission und US-Regierung sind zwar bereits seit einiger Zeit in Verhandlungen über eine Art „Safe Harbor II“. Doch ist fraglich, wann diese Verhandlungen zu einem Erfolg kommen, hat der EuGH doch die Hürden hoch gesetzt: Staatliche Überwachungsbefugnisse, die sich nicht „auf ganz bestimmte, strikt beschränkte Zwecke“ beschränken, insbesondere „es den Behörden gestatten, generell auf den Inhalt elektronischer Kommunikation zuzugreifen“, widersprechen den EU-Grundrechten und verhindern auch die Datenübermittlung in ein Land, in dem solche Regeln gelten. Genau diese umfassenden Befugnisse der Geheimdienste sollen aber für die USA nicht verhandelbar sein.

Weiterführende Informationen:

EuGH, Urteil vom 6.10.2015, Rs. C-362/14

<https://www.boetticher.com/15100a>

2. Hohes Bußgeld für zu knappen Auftragsdatenverarbeitungsvertrag

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat kürzlich eine Geldbuße in fünfstelliger Höhe festgesetzt, weil das betroffene Unternehmen in einem Auftragsdatenverarbeitungsvertrag keine konkreten technisch-organisatorischen Maßnahmen zum Schutz der Daten festgelegt, sondern sich auf pauschale Aussagen und Wiederholungen des Gesetzestextes beschränkt hatte.

Wenn Unternehmen externe Dienstleister als so genannten Auftragsdatenverarbeiter mit der Verarbeitung

personenbezogener Daten beauftragen – und sei es nur, dass sie E-Mail-Accounts nicht mit eigenen Servern betreiben oder für die IT-Wartung auf Dienstleister zurückgreifen –, müssen sie mit diesen schriftliche Verträge abschließen. Zusätzlich zur Schriftform – also Papier mit Unterschrift beider Seiten – schreibt das Gesetz eine Reihe von Mindestinhalten vor.

Besonders wichtig sind dabei die so genannten technisch-organisatorischen Maßnahmen, also Datensicherheitsmaßnahmen. Viele Auftragsdatenverarbeitungsverträge wiederholen hierzu nur die Datensicherheits-Ziele aus dem Gesetz oder beinhalten ein paar allgemeine Floskeln. Genau so einen Vertrag hat die bayerische Behörde nun mit einem Bußgeld im fünfstelligen Bereich geahndet. Denn das Gesetz schreibt vor, dass jede einzelne Sicherheitsmaßnahme konkret im Vertrag aufgeführt werden muss. Denn nur so lässt sich überhaupt bewerten, ob das beim Auftragnehmer bestehende Datensicherheitsniveau ausreichend ist.

Unternehmen sollten die Pflicht zu ordnungsgemäßen Auftragsdatenverarbeitungsverträgen nicht auf die leichte Schulter nehmen. Denn auch wenn Kontrollen durch die Datenschutzbehörden selten sind – die Auftragsdatenverarbeitungsverträge werden eigentlich immer geprüft, weil diese Kontrolle keinen nennenswerten Aufwand erfordert. Fehlt der Vertrag vollständig oder ist er inhaltlich unzureichend, drohen Bußgelder von bis zu 50.000,- Euro. Außerdem liegt eine sichere und auf klarer vertraglicher Basis beruhende Datenverarbeitung auch im Eigeninteresse jedes Unternehmens: Der Auftraggeber bleibt einerseits juristisch voll für die Datenverarbeitung verantwortlich – und hat zudem die wirtschaftlichen Folgen einer bekannt werdenden Datenpanne zu tragen.

3. Datenempfänger müssen korrekt identifiziert werden

Ein vermeintlich besonders preisgünstiges Verfahren der Auskunft Infocore, Bonitätsauskünfte zu erteilen, hat zu einem Datenskandal geführt. Nach Presseberichten, dass praktisch jedermann via Internet Bonitätsauskünfte über beliebige Dritte einholen konnte, musste

Infocore sein Angebot zunächst vollständig einstellen und dann umstellen. Das Grundproblem, aus der Ferne jemanden ordnungsgemäß zu identifizieren, stellt sich jedoch nicht nur für Auskunfteien: Jedes Unternehmen, das personenbezogene Daten speichert, muss Betroffenen auf Antrag Auskunft über alle gespeicherten Daten erteilen – und dabei sicherstellen, dass die Daten nur an den Betroffenen gelangen. Wer dabei, wie Infocore früher, ohne korrekte Identifizierung des Betroffenen vorgeht, riskiert Bußgelder oder sogar Haftstrafen.

Um an eine vermeintliche „Selbstauskunft“ zu gelangen, genügte es, Namen, Anschrift und Geburtstag einer beliebigen Person bei Infocore online in ein Formular einzutragen, eine beliebige E-Mail-Adresse und eine beliebige Mobiltelefonnummer einzugeben und 19,95 Euro zu bezahlen. Die Bonitätsauskunft wurde sofort online erteilt – ohne zu prüfen, wer sie tatsächlich anfordert. Infocore hat das Verfahren mittlerweile umgestellt: Die Auskunft wird jetzt per Post geschickt, was in den meisten Fällen ausreicht, um die gesetzlichen Anforderungen zu erfüllen.

Als Alternative wurde unter anderem die Anforderung einer Personalausweiskopie vorgeschlagen. Vor einer solchen Lösung ist zu warnen, denn eine Ausweiskopie hat keinerlei Beweiswert. Wer einem Unberechtigten personenbezogene Daten wie etwa eine Selbstauskunft übermittelt, nur weil eine vermeintliche Ausweiskopie des Betroffenen vorlag, handelt mindestens leichtfertig und muss mit Bußgeldern von bis zu 300.000,- Euro rechnen. Denn wie das Verwaltungsgericht Wiesbaden in einem aktuellen Urteil ausgeführt hat: „Eine Kopie erweckt zwar den Anschein, Abbild des Originals zu sein, ihre inhaltliche Unverfälschtheit steht aber nicht fest. Kopien können manipuliert oder in anderer Form elektronisch erzeugt worden sein.“

Weiterführende Informationen:

Matthias Bergt, CR-online.de Blog vom 24.3.2015

<https://www.boetticher.com/15100b>

VG Wiesbaden, Urteil vom 20.1.2015, Az.
6 K 1567/14.WI

<https://www.boetticher.com/15100c>

4. Telefonische Frage nach Werbe-Zustimmung kann unzulässig sein

Ein eigentlich zulässiger Anruf bei einem Kunden wird zu einer unzulässigen Telefonwerbung und einem Datenschutzverstoß, wenn im Lauf des Gesprächs der Kunde gefragt wird, ob er mit Telefon-, E-Mail- oder SMS-Werbung einverstanden ist. Ein entsprechendes Verbot des Berliner Datenschutzbeauftragten hat jetzt das Oberverwaltungsgericht bestätigt. Zwar sei der Anruf ursprünglich als Zufriedenheitsbefragung zulässig gewesen; die Frage nach einer Werbeeinwilligung mache den Anruf jedoch zu einer unzulässigen Nutzung personenbezogener Daten zu Werbezwecken.

Die datenschutzrechtliche Einschätzung, der Anruf an sich sei zulässig gewesen, dürfte von den Wettbewerbsgerichten nicht geteilt werden. Diese gehen viel-

mehr davon aus, dass beispielsweise bei einer Störung nur nachgefragt werden darf, ob die Störung behoben ist. Bereits eine Frage nach der Kundenfreundlichkeit und Serviceausrichtung der Mitarbeiter ist danach unzulässige Telefonwerbung. Da der Grat zwischen zulässiger Rückfrage und unzulässiger Telefonwerbung äußerst schmal ist, ist eine genaue rechtliche Prüfung im Einzelfall geboten.

Weiterführende Informationen:

OVG Berlin-Brandenburg, Beschluss vom 31.7.2015, Az. 12 N 71.14

<https://www.boetticher.com/15100d>

OLG Köln, Urteil vom 19.4.2013, Az. 6 U 222/12

<https://www.boetticher.com/15100e>

Ansprechpartner:

Wenn Sie Fragen haben oder weitere Informationen zu einem der Themen wünschen, wenden Sie sich bitte an:

Matthias Bergt

E-Mail: mbergt@boetticher.com

Tel. +49 / 30 / 61 68 94 03

Dr. Anselm Brandi-Dohrn, maître en droit

E-Mail: abrandi-dohrn@boetticher.com

Tel. +49 / 30 / 61 68 94 03

oder Ihren üblichen Ansprechpartner bei VON BOETTICHER.

Dieses Update stellt lediglich eine Auswahl von aktuellen Entscheidungen und Entwicklungen zu den besprochenen Themen dar, dient der allgemeinen Information und ersetzt keinesfalls eine spezifische Beratung im Einzelfall. Wenn Sie Fragen zu den hier angesprochenen Rechtsproblemen – oder zu anderen Rechtsgebieten – haben, wenden Sie sich bitte an Ihren Ansprechpartner bei VON BOETTICHER oder an die oben unter „Ansprechpartner“ angegebene Person.

Wenn Sie keine weiteren Informationen von VON BOETTICHER über aktuelle Rechtsentwicklungen erhalten möchten, senden Sie bitte eine E-Mail an eine der oben als Ansprechpartner genannten Personen.

VON BOETTICHER Rechtsanwälte
Oranienstraße 164
10969 Berlin

VON BOETTICHER Rechtsanwälte
Widenmayerstraße 6
80538 München

© 2015 VON BOETTICHER Rechtsanwälte Partnerschaftsgesellschaft mbB. Alle Rechte vorbehalten.

VON BOETTICHER Rechtsanwälte Partnerschaftsgesellschaft mbB ist eine eingetragene Partnerschaftsgesellschaft mit beschränkter Berufshaftung (AG München PR 516).

Sitz: Widenmayerstr. 6, 80538 München. Impressum und weitere Informationen unter <https://www.boetticher.com/impressum>.