



BerG im dortigen Verf für die Erfüllung des Kriteriums der Auffälligkeit nicht aus, wenn dem Werbe-text ein unauffälliges Sternchen zugeordnet ist und die Informationen als Auflösung des Sternchenverweises an entfernter Stelle erst am Ende der Website angeführt werden (OLG Wien 4 R 40/18h). Höchstgerichtlich ungeklärt ist, ob nach § 5 VKrG sämtliche Zahlenangaben im selben Schriftbild und optisch hervorgehoben sein müssen (idS *Heinrich in Schwimann/Kodek*⁴ § 5 VKrG Rz 10; *Schurr in Fenyves/Kerschner/Vonkilch*³ § 5 VKrG Rz 11) oder unter gewissen Voraussetzungen auch eine Angabe im Kleindruck ausreicht (*Pesek*, Verbrauchercreditver-

trag 26 f; *ders*, ZFR 2019/204; weitergehend *Zemann*, *ecolex* 2014, 932; *Zöchling-Jud in Wendehorst/Zöchling-Jud* § 5 VKrG Rz 5).

→ Für Darstellung im unmittelbaren Zusammenhang mit der erstmaligen Nennung der Leasingrate auch OLG Wien 4 R 142/19w (rk) VbR 2020/71 und 129 R 32/18a (rk) VbR 2018/125: Bei der Werbung im Internet sind sämtliche Pflichtangaben auf jener Einzel-seite anzuführen, auf der erstmals konkrete kostenbe-zogene Zahlen genannt werden; die Angabe auf einer über Anklicken oÄ gesondert aufzurufenden (Unter-) Seite („Layering“) reicht nicht aus (hL, statt aller *Heinrich in Schwimann/Kodek*⁴ § 5 VKrG Rz 11).

VbR 2020/118

Art 44 ff DSGVO

EuGH 16. 7. 2020,
C-311/18,
*Schrems und
Facebook Ireland*
(„*Schrems II*“)

Standard-
vertragsklauseln;

Safe Harbour;

Daten-
übermittlung;

Drittland

→ EU-US Privacy Shield: Kein angemessener Schutz

→ Der EU-US-Privacy-Shield-Beschluss 2016/1250 der EU-Kommission ist ungültig: Die Überwachungsprogramme der US-Behörden sind nicht auf das zwingend erforderliche Maß beschränkt, der vorge-sehene Ombudsmechanismus garantiert weder die Unabhängigkeit der Ombudsperson noch dass diese ermächtigt wäre, gegenüber den US-Nachrichtendiensten verbindliche Entscheidungen zu erlassen.

Die Entscheidung (Zusammenfassung):

Personenbezogene Daten dürfen grds nur dann in ein Drittland übermittelt werden, wenn dieses für die Daten ein angemessenes Schutzniveau gewährleistet. Stellt die EU-Kommission nach Art 45 DSGVO fest, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder seiner internationalen Verpflichtungen ein angemessenes Schutzniveau gewährleistet, bedarf die Datenübermittlung keiner besonderen Genehmigung. Liegt kein derartiger Beschluss vor, darf eine Datenübermittlung nur erfolgen, wenn der Exporteur der Daten geeignete Garantien vorsieht (die sich ua aus von der EU-Kommission erarbeiteten Standarddatenschutz-klauseln ergeben können) und wenn die betroffenen Per-sonen über durchsetzbare Rechte und wirksame Rechts-behelfe verfügen (Art 46 Abs 1 und 2 lit c DSGVO).

Datenübermittlung in Drittland

Die DSGVO ist auf eine Übermittlung personenbezogener Daten aus der EU in ein Drittland anwendbar, auch wenn die Daten bei ihrer Übermittlung oder im An-schluss daran von den Behörden des Drittlands für Zwe-cke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staats verarbeitet werden können.

Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden, müssen ein Schutzniveau genießen, das dem Niveau gleichwertig ist, das in der Union durch die DSGVO im Licht der GRC garantiert wird. Bei der Beurteilung dieses Schutzniveaus sind so-wohl die vertraglichen Regelungen zwischen Datenex-porteur und Empfänger zu berücksichtigen als auch die Rechtsordnung des Drittlands, was einen etwaigen Zu-griff der Behörden auf die übermittelten Daten betrifft.

Sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, sind die Aufsichtsbehörden insb

→ Der Beschluss 2010/87 über Standardvertrags-klauseln ist wirksam: Der Beschluss enthält wirk-same Mechanismen, die in der Praxis gewährleis-ten können, dass das unionsrechtliche Schutznive-au eingehalten wird und Datenübermittlungen ausgesetzt oder verboten werden, wenn gegen diese Klauseln verstoßen wird oder ihre Einhaltung unmöglich ist.

verpflichtet, eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn sie der Auffassung sind, dass die Standarddatenschutzklauseln in diesem Land nicht eingehalten wer-den (können) und der nach dem Unionsrecht erforder-liche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann.

Beschluss 2010/87: Standardvertragsklauseln

Der Beschluss 2010/87 ist gültig, auch wenn die ent-haltenen Standarddatenschutzklauseln aufgrund ihres Vertragscharakters die Behörden des Drittlands nicht binden: Gemäß dem Beschluss müssen der Datenex-porteur und der Empfänger der Übermittlung vorab prüfen, ob das erforderliche Schutzniveau im betref-fenden Drittland eingehalten wird. Ggf muss der Emp-fänger dem Datenexporteur mitteilen, dass er die Stan-dardschutzklauseln nicht einhalten kann, woraufhin der Exporteur die Datenübermittlung aussetzen und/oder vom Vertrag mit dem Empfänger zurücktreten muss.

Beschluss 2016/1250: Privacy Shield

Da die amerikanischen Überwachungsprogramme nicht auf das zwingend erforderliche Maß beschränkt sind, sind die im Beschluss 2016/1250 bewerteten Ein-schränkungen des Schutzes personenbezogener Daten durch den Zugriff amerikanischer Behörden nicht so geregelt, dass damit dem Unionsrecht gleichwertige Anforderungen erfüllt würden. Die Vorschriften hin-sichtlich bestimmter Überwachungsprogramme lassen in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung dieser Programme Einschränkungen bestehen; genauso wenig ist ersicht-lich, dass für die potenziell von diesen Programmen erfassten Personen Garantien existieren. Diese Vor-

schriften sehen zwar Anforderungen vor, die von den amerikanischen Behörden bei der Durchführung der Überwachungsprogramme einzuhalten sind, verleihen

den betroffenen Personen aber keine Rechte, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können.

Praxistipp:

→ Im Anlassfall werden die personenbezogenen Daten von Nutzern mit Wohnsitz in der EU von *Facebook Ireland* an Server der Facebook Inc in den USA übermittelt und dort verarbeitet. Aus dem Urteil folgt, dass Datenübermittlungen in die USA weder aufgrund des Privacy-Shield-Beschlusses (Art 45 DSGVO) noch auf Basis von Standarddatenschutzklauseln (Art 46 DSGVO) zulässig sind; diese können (faktisch) nur noch auf die (wenig praktikablen) Ausnahmen nach Art 49 DSGVO sowie bestehende Genehmigungen nach § 13 DSG 2000 gestützt werden. Verstöße können neben Geldbußen (Art 83 DSGVO) Schadenersatzansprüche betroffe-

ner Personen gegen Verantwortliche und Auftragsverarbeiter zur Folge haben (Art 82 DSGVO; § 29 DSG; zur Beweislast des Klägers für Schadenseintritt, -höhe und Kausalität 6 Ob 217/19h VbR 2020/42).

→ Offen ist, ob eine etwaige Verantwortlichkeit des Website-Betreibers nicht nur die automatisierte Datenübermittlung via Cookies oder Einbettung (vgl zum Facebook-Like-Button EuGH C-40/17, *Fashion ID*, VbR 2019/116) umfasst, sondern auch sog Double-Click-Lösungen oder externe Links, bei denen die Datenübermittlung nicht schon bei Aufruf der Website erfolgt, sondern erst durch Anklicken des Links durch den Nutzer.



Anmerkung:

Im Jahr 2015 hat der EuGH (C-362/14, *Schrems*, VbR 2015/120) das „Safe Harbor“-Abkommen, das die Übermittlung personenbezogener Daten aus der EU in die USA legitimierte, aufgehoben. Als Reaktion darauf haben die EU und die USA im Jahr 2016 das „EU-US Privacy Shield“ beschlossen, das personenbezogene Daten in den USA besser schützen und die Datenübermittlung wieder legitimieren sollte. In einer Auseinandersetzung zwischen (abermals) dem österr Datenschutzaktivisten *Maximilian Schrems* und der Social-Media-Plattform Facebook vor dem Data Protection Commissioner (irische Aufsichtsbehörde im Datenschutzrecht) wurden (indirekt) die Zulässigkeit des EU-US Privacy Shields sowie die Zulässigkeit der Übermittlung personenbezogener Daten aufgrund von Standardvertragsklauseln (in der Diktion der DSGVO nunmehr „Standarddatenschutzklauseln“ – SDK) in Frage gestellt.

Der EuGH folgte den Schlussanträgen des GA – der empfahl, eine Behandlung der Frage nach der Zulässigkeit des EU-US Privacy Shields abzulehnen (19. 12. 2019, C-311/18, *Saugmandsgaard Øe*, Rn 161, 166) – nicht, sondern **hob** das **EU-US Privacy Shield** mit sofortiger Wirkung ersatzlos **auf** (Rn 201, 203). Folglich ist die Übermittlung personenbezogener Daten aus der EU in die USA gestützt auf das EU-US Privacy Shield unzulässig. Gründe für die Aufhebung waren die weitreichenden geheimdienstlichen und sicherheitsbehördlichen Befugnisgesetze, die einen Zugriff auf personenbezogene Daten ohne richterlichen Beschluss zuließen, sowie der mangelhafte Rechtsschutz.

Der EuGH folgte den Schlussanträgen des GA (aaO Rn 343) jedoch dahingehend, dass die Übermittlung personenbezogener Daten aufgrund von **SDK** grundsätzlich **zulässig** ist (Rn 149). Bei SDK handelt es sich um von der Europäischen Kommission vorformulierte Vertragsklauseln. Während sich Unternehmen beim EU-US Privacy Shield jedoch auf die – von der Europäischen Kommission festgestellte – Angemessenheit des Schutzniveaus im Empfängerstaat verlassen durften, müssen sie diese bei der Nutzung von SDK selbst

beurteilen und den Rechtsrahmen im Empfängerstaat laufend evaluieren (vgl zB Punkt 4.b und 5.b der SDK im Beschluss [EU] 2010/87). Für die Übermittlung personenbezogener Daten in die USA hat der EuGH diese Prüfung mit seiner Entscheidung zum EU-US Privacy Shield bereits vorweggenommen: Ohne zusätzliche Maßnahmen, die eine Unterminierung des angemessenen Schutzniveaus durch US-Recht verhindern, ist das Datenschutzniveau in den USA nicht ausreichend und eine Übermittlung personenbezogener Daten in die USA daher auch auf Basis von SDK unzulässig.

Grds können Drittlandsübermittlungen auch durch **Binding Corporate Rules** gem Art 47 DSGVO sowie behördlich genehmigte **Ad-hoc-Vertragsklauseln** gem Art 46 Abs 3 DSGVO legitimiert werden. Für die Übermittlung in die USA gilt jedoch: Sofern nicht zusätzliche Maßnahmen, die eine Unterminierung des angemessenen Schutzniveaus verhindern, ergriffen werden, ist die Übermittlung unzulässig.

Weiterhin zulässig bleibt die Übermittlung personenbezogener Daten in die USA aufgrund von **behördlichen Genehmigungen** gem § 13 DSG 2000, die vor Inkrafttreten der DSGVO erteilt wurden; dies, solange die Datenübermittlung weiterhin vom Inhalt des Genehmigungsbescheids gedeckt ist. Diese Genehmigungen bleiben bis zu einer allfälligen Aufhebung, inhaltlichen Abänderung oder Ersetzung durch die Datenschutzbehörde aufrecht.

Abgesehen davon kann die Drittlandsübermittlung in die USA auf die (eingeschränkt praktikablen) „**Ausnahmen für bestimmte Fälle**“ gem Art 49 DSGVO gestützt werden, die nach Ansicht des Europäischen Datenschutzausschusses jedoch einschränkend auszulegen sind (vgl *EDSA*, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679). Näher zur eingeschränkten Zulässigkeit der Übermittlung personenbezogener Daten in die USA *Gabauer/Höller*, Dako 2020/45; zum Prüfungsschema einer Drittlandsübermittlung *Zavadil/Knyrim*, Dako 2020/43.

Alexander Höller,
Rechtsanwalt in Wien

