von **Dr. Sebastian Kraska**

# Datenschutz im Web 2.0: Wann gilt das deutsche Bundesdatenschutzgesetz?

Beinahe jede Neuerscheinung im Web 2.0 wird auch auf den datenschutzrechtlichen Prüfstand gestellt. Den Maßstab bildet in aller Regel das deutsche Bundesdatenschutzgesetz („BDSG“). Nicht immer zu Recht, wenn die Verantwortlichen im Ausland sitzen. Der folgende Beitrag stellt einige grundlegende Überlegungen zum internationalen Anwendungsbereich des Bundesdatenschutzgesetzes an.

## Kollisionsnorm

Keineswegs findet das BDSG auf alle Online-Aktivitäten deutscher Internet-Nutzer Anwendung. Vielmehr kommt es darauf an, wer den jeweiligen Datenverarbeitungsvorgang veranlasst. Ist die so genannte „verantwortliche Stelle“ im Ausland belegen, so gilt je nachdem, ob es sich um EU- oder Nicht-EU-Ausland handelt, § 1 Abs. 5 S. 1 oder S. 2 BDSG. § 1 Abs. 5 BDSG ist dabei eine so genannte „Kollisionsnorm“. Die Vorschrift regelt, welches nationale Recht auf einen grenzüberschreitenden Sachverhalt anzuwenden ist, wenn also mehrere Rechtsordnungen „kollidieren.“

## Anknüpfungspunkt Niederlassung

Existiert eine deutsche Niederlassung eines Unternehmens, dessen Hauptsitz sich innerhalb der EU befindet, und geht die Datenerhebung, -verarbeitung oder -nutzung von dieser Niederlassung aus, so findet das BDSG Anwendung. Im Übrigen jedoch nicht.
Den Inhalt des § 1 Abs. 5 BDSG gibt die EU-Datenschutzrichtlinie vor. In der Konsequenz heißt das, dass es im nationalen Datenschutzrecht eines jeden Mitgliedsstaates eine ähnlich lautende Kollisionsnorm geben muss. Denn die europäischen Richtlinien verpflichten die EU-Mitgliedsstaaten dazu, die enthaltenen Vorgaben im Rahmen der jeweiligen Richtlinie umzusetzen.

## Angeglichene Datenschutzstandards in der EU

Hinter § 1 Abs. 5 Satz 1 BDSG steht der Gedanke, dass es innerhalb des Geltungsbereichs der EU-Datenschutzrichtlinie keinen Unterschied machen dürfe, welches nationale Datenschutzrecht auf den Einzelfall Anwendung findet, weil dieses aufgrund der für alle EU-Mitgliedsstaaten verpflichtenden Wirkung der EU-Datenschutzrichtlinie ohnehin weitgehend harmonisiert ist und es nur gilt, Kollisionen verschiedener nationaler Datenschutzgesetze mit annähernd gleichem Schutzniveau zu vermeiden.

## Nicht-EU-Ausland

Anders verhält es sich, wenn die Hauptniederlassung außerhalb des Anwendungsbereichs der EU-Datenschutzrichtlinie liegt und deshalb nicht von einem harmonisierten Schutzniveau ausgegangen werden darf. Hier gibt das BDSG seine Schutzwirkung nicht so bereitwillig preis. Es gilt dann § 1 Abs. 5 Satz 2 BDSG. Dieser lautet:
„Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. (...)."

## Datenverarbeitung „im Inland"

Anknüpfungskriterium ist nach jetzigem Rechtsstand die Datenerhebung, -verarbeitung oder -nutzung „im Inland." Dafür verlangt die EU-Datenschutzrichtlinie in Artikel 4 Absatz 1 Buchstabe c, dass auf im Hoheitsgebiet des betreffenden Mitgliedsstaats belegene, automatisierte oder nicht automatisierte Mittel zurück gegriffen wird. Das kann etwa der Einwahlknoten eines Internetproviders, der Server eines Anbieters, der private PC des Nutzers eines Online-Dienstes oder der darauf installierte Browser sein. Ob und unter welchen Umständen nutzereigene Geräte und Programme als „Mittel" im Sinne des Artikel 4 Absatz Buchstabe c gelten dürfen, ist nicht abschließend geklärt. Bei einigen Internetdiensten ist aber gerade diese Einordnung wesentlich:

## Beispiel Datenverarbeitung „im Inland"?: Facebook-Like-Button

Der Facebook-Like-Button ist ein so genanntes „Social Plug-in" auf Webseiten privater und kommerzieller Betreiber. Die Einbindung des Facebook-Like-Buttons durch den Betreiber einer Webseite löst (bei gleichzeitiger Zuordnung zu einem Faebook-Account des aufrufenden PCs) eine direkte Verbindung und Datentransfer zwischen dessen Browser und den Facebook-Servern aus. Das dafür eingesetzte Mittel, der Browser des Internetnutzers, befindet sich zwar „im Inland", der die Datenverarbeitung steuernde Rechner vermutlich aber nicht.

## Beispiel Datenverarbeitung „im Inland"?: Facebook Gesichtserkennung

Hierbei werden die Fotos der Nutzer nach biometrischen Kriterien analysiert und entsprechend gespeichert. So kann, wenn die Person auf einem anderen Bild „erkannt" wird, ein entsprechender Markierungsvorschlag erfolgen. Es ist möglich, diese Vorschlagsfunktion abzuschalten, der Analyse der abgebildeten Gesichter und der Speicherung der dabei gesammelten biometrischen Daten kann allerdings derzeit nicht widersprochen werden.
Die von den Nutzern hochgeladenen Bilder befinden sich auf vermutlich global gestreuten Servern, so

dass nicht ohne Weiteres feststellbar ist, ob bei der biometrischen Analyse eine Datenverarbeitung „im Inland“ erfolgt. An die Server übermittelt werden die Daten aber vom Computer des Nutzers aus.
Die Anwendbarkeit des BDSG zu begründen dürfte den deutschen Datenschutzbehörden schwer fallen, solange Facebook keinen Einblick in die internen Abläufe gewährt. Diese Schwierigkeit suchen sie zu umgehen, indem sie den zweifellos im Inland belegenen PC oder Browser des Nutzers als „Mittel“ im Sinne des Artikel 4 Absatz 1 Buchstabe c der Datenschutzrichtlinie qualifizieren, wobei der Bundesdatenschutzbeauftragte Peter Schaar durchaus nicht leicht zu entkräftende Zweifel einräumt.

## Neuerungen durch die EU-Datenschutzverordnung

Der im Januar 2012 von der EU-Kommission offiziell vorgestellte Entwurf der geplanten EU-Datenschutzverordnung]enthält nun eine Abkehr vom Kriterium des im Inland belegenen Mittels. Er beansprucht nach Artikel 2 Absatz 2 Geltung für die Verarbeitung personenbezogener Daten von innerhalb der EU lebenden Personen, die sich an diese richten oder darauf abzielen, ihr Verhalten zu beobachten, wenn diese Verarbeitung durch eine außerhalb der EU belegene Niederlassung erfolgt. Diese Regelung bezieht sich erkennbar auf die oben dargestellten Dienste. Mit ihrer Verabschiedung würde die Verordnung in der gesamten EU unmittelbar „wie nationales Recht“ gelten. Die betreffenden Aktivitäten unterfielen dann dem in der Verordnung normierten Datenschutzrecht. Bis es allerdings so weit ist, gelten weiterhin die EU-Datenschutzrichtlinie und das BDSG.

## Verantwortlichkeitsprinzip

Konkretisierend enthält § 1 Abs. 5 BDSG als zweites Kriterium das der Verantwortlichkeit. Eine Stelle ist dann für einen Datenverarbeitungsvorgang verantwortlich, wenn sie die Entscheidungsgewalt darüber hat, also auf das Ob und Wie, über Mittel und Zweck der Datenverarbeitung Einfluss ausübt. Nach der Stellungnahme der Art. 29 Datenschutzgruppe soll in erster Linie die Entscheidungsgewalt hinsichtlich des Zwecks der Datenverarbeitung ausschlaggebend sein.

## Beispiel: Google Street View

Für diesen Dienst wurden Straßenzüge mit Häuserfassaden und allem/allen, was sich momentan im Fokus der Kamera befand, aufgenommen. Die Datenerhebung musste also notwendigerweise „im Inland“ erfolgen. Die Daten erhob die Google Germany GmbH, die deutsche Tochterfirma des in den USA ansässigen Mutterkonzerns, zum Zwecke der späteren Übermittlung in die USA. Verantwortliche Stelle war bis zur Übermittlung die Google Germany GmbH, denn sie konnte entscheiden, was mit den Daten geschieht. Solange das der Fall war, konnte auch das BDSG Geltung beanspruchen. Dementsprechend versuchte der Bundesrat mit seinem Gesetzesentwurf vom 9.7.2010, vor der Übertragung in die USA Zugriff zu nehmen.

## Niederlassung in der EU genügt allein nicht

Das Kriterium der Verantwortlichkeit schränkt das oben erläuterte Niederlassungsprinzip ein. So ist nicht allein deshalb zu schlussfolgern, dass Facebook irischem Datenschutzrecht mit europäischem Schutzstandard unterliegt, weil der Konzern dort eine Niederlassung unterhält. Umgekehrt darf aber auch nicht davon ausgegangen werden, dass die irische Niederlassung als bloße Abrechnungsstelle keinerlei Einfluss auf Datenverarbeitungsvorgänge nimmt. Nur wenn diese EU-Niederlassung die jeweilige datenschutzrelevante Aktivität in eigener Verantwortung vornimmt, gilt auch das Datenschutzrecht des Mitgliedsstaats, in dem sie sich befindet.

## Beispiele Verantwortlichkeitsprinzip: Facebook-Like-Button

Eine andere Frage ist die der datenschutzrechtlichen Verantwortlichkeit. Diese wird beim Einsatz des Facebook-Like-Buttons neben Facebook zum Beispiel durch das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein auch dem Webseitenbetreiber zugeschrieben, da er den Quellcode des Buttons in seine Webseite eingebunden hat. Mit dieser Argumentation forderte das ULD im Herbst 2011 die in Schleswig-Holstein ansässigen Webseitenbetreiber auf, den Button zu entfernen, da über § 3 Abs. 1 TMG auch deutsche Rechtsvorgaben zu beachten seien. Gegen die Verantwortlichkeit des Webseitenbetreibers wird unter anderem eingewandt, dass dieser keinerlei Einfluss darauf habe, wann und in welchem Umfang die Erhebung welcher Daten erfolge und diese Entscheidung letztlich bei Facebook liege. Eine verlässliche Entscheidung zu den streitigen Fragen existiert bislang nicht.

## Beispiel Verantwortlichkeitsprinzip: Google Analytics

Auch bei dem Webanalyse-Dienst Google Analytics fällt die grundsätzliche Entscheidung für die Erhebung der Daten zum Zweck der Übermittlung an Google durch den inländischen Betreiber der Webseite. Dass er über den genauen Zeitpunkt und Umfang nicht Bescheid weiß, ändert daran nichts. Im Unterschied zum Facebook-Like-Button ist für den Besucher hier überhaupt keine Verbindung zu Google zu erkennen. Er ist sich beim Besuch der Webseite zu keinem Zeitpunkt darüber im Klaren, dass sein Verhalten aufgezeichnet wird. Damit entscheidet der Webseitenbetreiber über den Zweck der Übermittlung an Google und ist daher nach der Definition der Artikel 29-Datenschutzgruppe insoweit als „verantwortliche Stelle“ anzusehen.

## Geteilte Verantwortung

Die Verantwortlichkeit des Webseitenbetreibers schließt diejenige von Facebook oder Google aber nicht aus. Ob allerdings im Falle von Facebook nach § 1 Abs. 5 S. 1 BDSG irisches oder nach § 1 Abs. 5 S. 2 BDSG deutsches Datenschutzrecht Anwendung findet, hängt davon ab, ob der US-amerikanische Mutterkonzern oder die irische Zweigniederlassung verantwortlich für die durch den Button ausgelösten Datenverarbeitungsvorgänge sind. Den deutschen Datenschutzbehörden ist es bislang nicht gelungen, sich hierüber Klarheit zu verschaffen.

## Differenzierte Betrachtung erforderlich

Eine pauschale Aussage zur Anwendbarkeit des BDSG auf Online-Dienste ist nach derzeitiger Rechtslage nicht möglich. Vielmehr muss diese Frage für jeden Einzelfall geklärt werden. Nach der geplanten EU-Datenschutzverordnung wird zumindest eine Untersuchung notwendig sein, ob Hinweise darauf bestehen, dass sich ein Angebot beispielsweise an deutsche Nutzer richtet. Dabei wird u.a. auf die Sprache, die Top Level Domain „.de“ oder Werbung für inländische Unternehmen abzustellen sein.

## Fazit

Der internationale Anwendungsbereich des BDSG hängt nach der momentanen Rechtslage stark vom Einzelfall ab und stößt in der Praxis insbesondere hinsichtlich der Durchsetzbarkeit schnell auf Grenzen. Die geplante EU-Datenschutzverordnung beabsichtigt insbesondere hinsichtlich der Durchsetzbarkeit eine Verschärfung auf europäischer Ebene, wenngleich offen ist, ob die Vorstellungen der europäischen Verwaltung in Anbetracht einer globalisierten Datenwelt und eines dynamischen Nutzerverhaltens einen praxisgerechten Weg vorgeben.

Autor:
**Dr. Sebastian Kraska**
Rechtsanwalt