

DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz

Schriftleitung: Prof. Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer

Editorial

Tilman Herbrich

Das Wettbewerbsrecht als Booster für den Datenschutz?

Seite 253

Stichwort des Monats

Stephan Hansen-Oest

„Chilling Effects“ durch die Rechtsprechung des EuGH zu Art. 9 DSGVO?

Seite 254

Datenschutz im Fokus

Carolin Steiger

**Auskunft zum Drittlandtransfer gem. Art. 15 Abs. 2 DSGVO:
Alles oder nichts beauskunften?!**

Seite 259

Dr. Giuliana Schreck und Dr. Nina Herbort

Wer ist hier der Bürokrat? Wie die Institution des Datenschutzbeauftragten Aufwand gerade abbaut

Seite 263

Aktuelles aus den Aufsichtsbehörden

Philipp M. Kühn und Angeliki Sembritzki

Neue Konkretisierungen und Praxishinweise der Datenschutzkonferenz zu Asset Deals

Seite 267

Rechtsprechung

Dr. Jens Ambrock

EuGH zum Ermessen der Datenschutzbehörden

Seite 272

Dr. Alexander Theusner

Über die Grenzen der zielgerichteten Werbung

Seite 275

Matthias Horn

EuGH zu Gesundheitsdaten und wettbewerbsrechtliche Unterlassungsansprüche

Seite 278

Dr. Dominik Sorber und Christina Knoepffler

**Weiterleitung betrieblicher E-Mails an privaten E-Mail Account =
Fristlose Kündigung – auch für Vorstände**

Seite 281

▪ Nachrichten Seite 257

Stephan Hansen-Oest

„Chilling Effects“ durch die Rechtsprechung des EuGH zu Art. 9 DSGVO?

Die Rechtsprechung des EuGH zur Verarbeitung besonderer Kategorien personenbezogener Daten ist zu Recht nicht unumstritten. Die Folgen können für die Informations- und Meinungsfreiheit gravierend sein. Und auch Anbietende von Onlinediensten mit „user generated content“ sind erheblich betroffen. Schwebt das Damoklesschwert der fehlenden Rechtsgrundlage über dem Geschäftsmodell und auch Recht auf freie Meinungsäußerung?

„Chilling Effects“ am Anfang

Am 24. Mai 2016 trat die DSGVO in Kraft. Bevor sie dann am 25. Mai 2018 in die Anwendung kam, gab es in kritischen datenschutzrechtlichen Kreisen eine interessante Diskussion.

Eine Befürchtung stand im Raum. Wird die DSGVO als großes Regelungsinstrument dazu führen, dass andere Grundrechte – insbesondere die Freiheit der Meinungsäußerung und Informationsfreiheit (Art. 11 GRCh) negativ beeinträchtigt werden können?

Könnte der negative Einfluss vielleicht sogar so groß sein, dass Menschen ihr Verhalten einschränken und ihre Freiheitsrechte nicht mehr oder nicht mehr im gewohnten Umfang ausüben? Wir sprechen in diesen Fällen von sog. „Chilling Effects“ einer staatlichen Regulierung. Bürgerinnen und Bürger üben ihre Grundrechte dann aus Angst vor negativen Folgen nicht mehr aus, obwohl sie ihnen zustehen.

Diese Befürchtungen vor negativen Folgen und die Änderung des menschlichen Verhaltens aufgrund datenschutzrechtlicher Vorgaben der DSGVO gab es dann ab Juni 2018 auch. Einige werden sich noch an „Dingdong, Datenschutz“ erinnern – die Diskussion hinsichtlich der Zulässigkeit des Anbringens von Namen auf Klingelschildern. Oder auch die Verunsicherung bei der Anfertigung, Verwendung und Veröffentlichung von Fotos in Schulen und Kindertagesstätten.

Die meisten dieser „Chilling Effects“ haben sich mittlerweile entweder durch eine juristische Aufarbeitung aufgelöst oder die Verunsicherung ist über die Jahre weniger geworden.

Rechtsprechung des EuGH als Grundlage neuer „Chilling Effects“

Was viele noch nicht bemerkt zu haben scheinen: Die Rechtsprechung des EuGH zu Art. 9 DSGVO kann jetzt in einer ganz anderen Dimension zu „Chilling Effects“ führen. Und man kann nur staunen, dass dieses Problem bislang nicht bzw. nur am Rande in Fachkreisen diskutiert wird.

Denn die Schlagkraft lässt sich an einem einfachen Anwendungsfall darstellen.

Bevor dies an einem Beispielfall aufgezeigt wird, müssen wir kurz auf die insoweit folgenschwere Auslegung des Art. 9 DSGVO durch den EuGH zu sprechen kommen.

In seiner „Meta Platforms“-Entscheidung hat der EuGH (Urt. v. 4.7.2023 – C-252/21) zunächst festgestellt, dass eine Verarbeitung von besonderen Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO auch dann vorliegt, wenn die Daten dem Verantwortlichen aufgedrängt werden, er diese also gar nicht verarbeiten möchte. Dies hat der EuGH noch einigermaßen nachvollziehbar damit begründet, dass nur so der durch Art. 9 DSGVO gebotene hohe Schutzmaßstab für diese Datenarten eingehalten werden könne.

Weiter hat der EuGH dann noch ausgeführt, dass eine Verarbeitung von besonderen Kategorien personenbezogener Daten auch dann vorliege, wenn diese Daten nicht korrekt sind. Wenn also jemand eine Krebserkrankung vorspiegelt, handelt es sich also dennoch um ein Gesundheitsdatum.

Der EuGH hätte jetzt in der „Lindenapotheken“-Entscheidung (Urt. v. 4.10.2024 – C-21/23; siehe auch S. 278 ff.) die Chance gehabt, seine Rechtsprechung zu Art. 9 DSGVO zurechtzurücken oder zumindest so zu konkretisieren, dass man zu praktisch brauchbaren Ergebnissen kommt.

Der Generalanwalt hat in seinen Schlussanträgen in diesem Verfahren versucht, der weitgehenden Auslegung von Art. 9 DSGVO durch den EuGH dadurch Einhalt zu gebieten, dass der Begriff der Gesundheitsdaten eingeschränkt wird. Eine Verarbeitung von Gesundheitsdaten i. S. d. Art. 9 DSGVO hätte nach Ansicht des Generalanwalts nur dann vorgelegen, wenn die Angaben zum Gesundheitszustand nicht bloß vermutet werden, sondern wenn ein Mindestmaß an Gewissheit dafür vorliegt.

Der EuGH hat sich diesem Ansatz nicht angeschlossen. Leider. Er hat vielmehr seine ausufernde Auslegung zum Vorliegen von Gesundheitsdaten weiter ausgedehnt.

Das konkrete Problem am Beispiel einer „Website“

Stellen wir uns einen Anbieter eines Onlinedienstes auf einer Internetseite vor. Der Anbieter hat eine Internetseite. Über diese werden Online-Gitarrenkurse angeboten. In einem Diskussionsforum auf der Internetseite können sich die Kursteilnehmenden untereinander austauschen. Das Forum wird vom Anbieter moderiert. Beim Forenbetrieb fallen notwendigerweise personenbezogene Daten der Nutzenden an. Dazu gehören neben den Bestandsdaten (E-Mail-Adresse, Username und ggf. weitere Daten wie z. B. Profilbilder) auch Nutzungsdaten und Inhaltsdaten („Inhalte der Beiträge“) an.

In rechtlicher Hinsicht ist der Anbieter der Internetseite Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO. Man kann darüber streiten, ob das Verbot mit Erlaubnisvorbehalt im europäischen Datenschutzrecht schon in Art. 8 GRCh angelegt ist. Wegen der in der DSGVO verankerten Vorgabe, dass jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage bedarf, benötigt der Anbieter der Internetseite eine Rechtsgrundlage zur Verarbeitung der Daten des Betriebs des Diskussionsforums.

Nach der Rechtsprechung des EuGH sind die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten abschließend in Art. 6 DSGVO geregelt. Sofern das Diskussionsforum Bestandteil der Leistungen für die Kursteilnehmenden ist, wird der Anbieter sich insoweit im Wesentlichen schon auf die Rechtsgrundlage des Art. 6 Abs. 1 lit. b DSGVO stützen können. Soweit personenbezogene Daten verarbeitet werden, die nicht zum Kern der vertraglichen Leistungen gehören, kommt ergänzend noch Art. 6 Abs. 1 lit. f DSGVO in Betracht. So weit, so gut.

Eskalationsstufe 1 – Gesundheitsdaten

Nehmen wir im genannten Szenario einmal an, dass eine Kursteilnehmerin im Diskussionsforum darüber berichtet, dass sie wegen eines Unfalls im Kindesalter eine Teillähmung am rechten Zeigefinger hat und daher eine bestimmte Technik beim Musizieren nutzt.

Nach der Rechtsprechung des EuGH handelt es sich bei dieser Information um Gesundheitsdaten. Da die Verarbeitung von Gesundheitsdaten wegen Art. 9 Abs. 1 DSGVO grundsätzlich untersagt ist, benötigt der Anbieter der Internetseite jetzt nicht nur eine Rechtsgrundlage aus Art. 6 DSGVO. Er benötigt auch noch eine Ausnahmeregelung aus Art. 9 Abs. 2 DSGVO für die Verarbeitung der Inhaltsdaten des Beitrags.

Selbst wenn der Anbieter in seinen Nutzungsbedingungen in wirksamer Weise mit den Kursteilnehmenden vereinbart hätte, dass diese keine besonderen Kategorien personenbezogener Daten in Forenbeiträgen „posten“ dürfen,

würde diese vertragliche Regelung nicht verhindern können, dass nach der Rechtsprechung des EuGH dennoch Gesundheitsdaten verarbeitet werden. Und dies wäre jedenfalls für den Zeitraum bis zur Löschung des Beitrags ohne eine Rechtsgrundlage erfolgt.

Einwilligung oder offensichtliche Veröffentlichung als Rechtsgrundlage?

Die Lösung für diese Fälle könnte auf den ersten Blick die Einwilligung der Kursteilnehmerin sein. So ist eine Verarbeitung von Gesundheitsdaten nach Art. 6 Abs. 1 lit. a DSGVO i. V. m. Art. 9 Abs. 2 lit. a DSGVO zulässig, wenn die betroffene Person eine wirksame Einwilligung in die Verarbeitung ihrer Gesundheitsdaten erteilt hat.

Nur: Was macht der Anbieter, wenn die betroffene Person dann ihre Einwilligung widerruft? Die Rechtsgrundlage für die Datenverarbeitung würde dann entfallen. Die Gesundheitsdaten des Beitrags müssten bzw. der Beitrag selbst müsste dann gelöscht werden. Dies kann wiederum im Einzelfall Diskussionsstränge nicht mehr nachvollziehbar machen. Die Einwilligung ist für Anbieter entsprechender Onlinedienste mit Diskussionsfunktion in der Regel keine sonderlich attraktive Rechtsgrundlage.

Eine bessere Lösung kommt im konkreten Fall mit Art. 9 Abs. 2 lit. e DSGVO als Ausnahmeregelung in Betracht. Danach ist eine Verarbeitung von Gesundheitsdaten zulässig, wenn die betroffene Person die Gesundheitsdaten offensichtlich öffentlich gemacht hat.

Das dürfte im vorliegenden Fall grundsätzlich passen. Aber ganz sicher ist es wiederum auch nicht. Denn ob die betroffene Person im konkreten Fall wirklich – wie die Rechtsprechung des EuGH verlangt – „explizit seine Entscheidung zum Ausdruck gebracht hat, die ihn betreffenden Daten einer unbegrenzten Zahl von Personen öffentlich zugänglich zu machen.“ (vgl. EuGH, Urt. v. 4.7.2023 – C-252/21 Rn. 85).

Auch hier verbleibt also ein gewisses Restrisiko für den Anbieter des Onlinedienstes.

Das Medienprivileg als Rettung?

Nach Art. 85 DSGVO sind die Mitgliedsstaaten der EU aufgerufen, Regelungen zu treffen, die das Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken mit dem Schutz personenbezogener Daten in Einklang bringen sollen.

An einer einschlägigen spezifischen Regelung, auf die sich der Anbieter des Onlinedienstes berufen könnte, fehlt es jedoch im Recht der Bundesrepublik Deutschland.

Insbesondere die Regelungen des Mediendienstestaatsvertrags (MStV) sind für den Anbieter unserer Online-Gitarrenkurse nicht anwendbar. Der Anbieter fällt schon nicht in den Anwendungsbereich von § 23 MStV.

Es lässt sich zudem schon generell daran zweifeln, dass aufgrund des geschlossenen Charakters des Diskussionsforums die erforderliche Auswirkung auf die öffentliche Meinungsbildung angenommen werden kann.

Als Zwischenergebnis kann festgestellt werden, dass eine belastbare Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten in der „Eskalationsstufe 1“ schon kaum vorhanden ist.

Eskalationsstufe 2 – Gesundheitsdaten Dritter

Mutige Geschäftsführende werden bei Eskalationsstufe 1 ggf. noch das Risiko einer „wackeligen“ Rechtsgrundlage für vertretbar erscheinen lassen und vielleicht auch die Flucht in die Einwilligung als passable Lösung wählen.

Wie sieht es aber aus, wenn nun im Forum des Anbieters des Onlinedienstes Kursteilnehmende über die Krankheiten von anderen Kursteilnehmenden oder anderen Dritten Beiträge veröffentlichen? Auch in diesem Szenario liegt nach der Rechtsprechung des EuGH eine Verarbeitung von Gesundheitsdaten vor.

Nur hilft in diesem Fall nicht die Einwilligung. Denn die betroffene Person, um deren Gesundheitsdaten es geht, wird schwerlich eine wirksame Einwilligung in die Verarbeitung ihrer Gesundheitsdaten erteilt haben. Im Zweifel hat diese noch nicht einmal Kenntnis von diesem Forum.

Spätestens an dieser Stelle brechen also Geschäftsmodelle in Ermangelung einer Rechtsgrundlage zusammen.

Ich denke, dass jeder und jedem klar sein sollte, dass dieses nicht das „richtige“ Ergebnis sein kann. Wenn wir also die Rechtsprechung des EuGH zu Art. 9 DSGVO anwenden, führt dies dazu, dass Bürgerinnen und Bürger ihre Freiheit der Meinungsäußerung und Informationsfreiheit i. S. d. Art. 11 GRCh verlieren. Es ist auch nicht nur ein Teilverlust. Der Kernbereich dieses Rechts wird eingeschränkt.

Mögliche Lösungen

Alle denkbaren Lösungen für dieses Dilemma sind nicht kurzfristig umzusetzen bzw. müssen auch gewollt werden. Wenn es jetzt nicht um besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO gehen würde, dann würde man unter Zugrundelegung der Rechtsprechung des BGH zur Interessenabwägung die Hoffnung haben können, dass der BGH die Lösung sein könnte. Denn der BGH führt bei Datenverarbeitungen auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO eine Prüfung der widerstreitenden

Grundrechte und Grundfreiheiten durch und könnte aufgrund einer Verletzung des Kernbereichs von Art. 11 GRCh das Recht auf den Schutz personenbezogener Daten i. S. d. Art. 8 GRCh zurücktreten lassen.

Dieser Weg ist jedoch bei besonderen Kategorien personenbezogener Daten verbaut, weil es an einer passenden Ausnahmeregelung in Art. 9 Abs. 2 DSGVO fehlt.

Eine Lösung wäre, dass der EuGH endlich beginnt, die DSGVO primärrechtskonform auszulegen. Und hier könnte schon bei der Beantwortung von Vorlagefragen insoweit mitgedacht werden, ob bestimmte Feststellungen nicht dazu führen könnten, dass in der Konsequenz ein Missverhältnis zwischen Art. 8 GRCh und anderen Grundrechten und Grundfreiheiten der Charta entsteht, das nach Art. 52 GRCh in ein Gleichgewicht zu bringen sind.

Schließlich bliebe noch die Option, dass der deutsche Gesetzgeber seinen Gestaltungsauftrag i. S. d. Art. 85 DSGVO endlich erfüllt und spezifische Regelungen trifft, um das Recht auf den Schutz personenbezogener Daten mit der Informations- und Meinungsfreiheit in Ausgleich zu bringen.

Es bleibt ein Dilemma

Keiner der aufgezeigten Lösungswege ist derzeit praktisch hilfreich. Wenn wir dann noch bedenken, dass Anwältinnen und Anwälte haftungsrechtlich den „sichersten Weg“ zu beraten haben, fürchte ich, dass einige Mandantinnen und Mandanten demnächst von ihren Kanzleien erfahren werden, dass es das „Sicherste“ wäre, wenn sie ihren Onlinedienst in der bisherigen Form einfach einstellen – jedenfalls soweit „user generated content“ vorgesehen ist. Eine wahrlich „chillige“ Konsequenz, die mich fröstelnd hinterlässt.

Autor: Stephan Hansen-Oest ist Rechtsanwalt und Fachanwalt für IT-Recht in Flensburg.

