BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 53/2021
September 2021
Registernummer: 25412265365-88

Digitale Grundprinzipien der Europäischen Union

Mitglieder des AS Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Simone Eckert
RA Prof. Dr. Armin Herb, (Vorsitzender)
RA Dr. Wulf Kamlah
RAin Simone Kolb
RA Jörg Martin Mathis
RA Dr. Hendrik Schöttle
RA Prof. Dr. Ralph Wagner, LL.M.

RA André Haug, Vizepräsident BRAK
RA Sebastian Aurich, LL.M., BRAK Berlin

Mitglieder des AS Europa
RAuN a.D. Kay-Thomas Pohl (Vorsitzender)
RA Dr. Hans-Joachim Fritz
RAin Dr. Margarete Gräfin von Galen
RA Marc André Gimmy
RA Andreas Max Haak
RA Dr. Frank J. Hospach
RA Guido Imfeld
RAin Dr. Kerstin Niethammer-Jürgens
RA Dr. Christian Lemke
RA Maximilian Müller
RA Jan K. Schäfer, LL.M.
RAin Stefanie Schott
Prof. Dr. Gerson Trüg

RA Dr. Hans-Michael Pott
RA Andreas von Máriássy
RA Dr. Thomas Westphal

RAuN Dr. Thomas Remmers, Vizepräsident, Bundesrechtsanwaltskammer
RAin Dr. Heike Lörcher, Bundesrechtsanwaltskammer, Brüssel
RAin Astrid Gamisch, LL.M., Bundesrechtsanwaltskammer, Brüssel
Referent Rafael Javier Weiske, Bundesrechtsanwaltskammer, Brüssel

Verteiler: Europäische Kommission

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

Die Bundesrechtsanwaltskammer bedankt sich für die Möglichkeit einer Beteiligung im Rahmen der Konsultation zur Erklärung zu den digitalen Grundprinzipien der Europäischen Union und nimmt diese gerne wahr.

I. Forderung: Das Mandatsgeheimnis auch als digitales Grundprinzip

Zu den digitalen Grundprinzipien der Europäischen Union sollte ein den rechtsstaatlichen Grundsätzen genügender Schutz des Mandatsgeheimnisses gehören. Es muss verhindert werden, dass die *praktischen* Möglichkeiten, die die Digitalisierung eröffnet, zu einer Aushöhlung des *normativen* und rechtsstaatlichen Grundsatzes der Vertraulichkeit der Mandatskommunikation führen. Dahingehende Tendenzen sind erkennbar. Diesen gilt es entgegenzutreten.

Die digitalen Grundprinzipien der Europäischen Union sollten daher den folgenden Grundsatz enthalten:

> *Die Vertraulichkeit der Kommunikation zwischen Rechtsanwältinnen und Rechtsanwälten, Ärztinnen und Ärzten u. a. zur Geheimhaltung verpflichteten Berufsträgern mit Ihren Mandanten, Patienten ist zu schützen. Die Vertraulichkeit der Mandatskommunikation zwischen Rechtsanwältinnen und Rechtsanwälten einerseits und deren Auftraggebern andererseits wird auch im digitalen Bereich gewährleistet. Die Inanspruchnahme vertraulicher Rechtsberatung muss jedermann über die von ihm gewählten Kommunikationsnetze bzw. Plattformen frei von staatlicher oder nicht staatlicher Einsichtnahme oder Kontrolle möglich sein. Es darf auch nicht erfasst werden, wer einen Anwalt bzw. eine Anwältin konsultiert hat.*

II. Begründung

1. Das Mandatsgeheimnis als Grundvoraussetzung rechtsstaatlicher und grundrechtlicher Garantien

Die anwaltliche Verschwiegenheit ist eine Voraussetzung für die Inanspruchnahme rechtsanwaltlicher Beratung und damit ein Grundpfeiler eines jeden Rechtsstaats. Sie unterfällt dem Schutz der europäischen wie nationalen Rechtsstaatsgarantien aus Art. 47 Abs. 1 Satz 2 GRCh, Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK sowie Art. 20 Abs. 2 GG, Art. 103 Abs. 1 GG. Zugleich ist sie im Kontext anwaltlicher Beratung Voraussetzung für die Verwirklichung europäischer wie nationaler Grundrechte aus Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK, Art. 47 Abs. 1, 2 Satz 2 GRCh, Art. 20 Abs. 3, Art. 103 Abs. 1 GG, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK, Art. 7 GRCh, Art. 12 Abs. 1 GG. Sie dient in erster Linie dem Schutz des Mandanten und seines Zugangs zum Recht. Es schützt Opfer, Täter und sonstige Rechtsuchende gleichermaßen. Wird der Schutz des Mandatsgeheimnisses nicht gewährleistet und können Mandanten daher keinen Rechtsrat in Anspruch nehmen, wird dadurch zugleich die Anwaltschaft in ihrer Berufsausübungsfreiheit beeinträchtigt.

2. Das Mandatsgeheimnis im digitalen Bereich

Der Schutz des Mandatsgeheimnisses erweist sich angesichts der fortschreitenden Digitalisierung und Vernetzung und der damit einhergehenden gewandelten Nutzungsgewohnheiten als Herausforderung. Dies gilt zum einen in technischer Hinsicht, da massenhaftes, ortsungebundenes Datenauslesen für einen immer größeren potenziellen Täterkreis möglich wird und die hiergegen zu richtenden Schutzmaßnahmen oft deutlich komplexer – und damit fehleranfälliger sind – als in der analogen Welt.

Dem wird durch die Einrichtung vertraulicher Kommunikationssysteme – wie etwa des besonderen elektronischen Anwaltspostachs (beA) – teilweise bereits sehr erfolgreich begegnet. So kann teilweise sogar ein höheres Maß an Vertraulichkeit und Integrität erzielt werden, als dies im analogen Zeitalter der Fall war. Auch angesichts der logistischen und vieler weiterer Vorteile nimmt die digitale Kommunikation auch im anwaltlichen Bereich zu – sowohl im Umgang mit Behörden und Gerichten als auch mit Mandanten und Anwälten untereinander.

Digitalisierung und Vernetzung erleichtern in weiten Teilen die Kontaktaufnahme zu Rechtsanwälten und können insoweit zu einer Verbesserung des Zugangs zum Recht beitragen. Dies funktioniert aber nur, wenn dabei die Vertraulichkeit gewahrt ist. Ist dies nicht der Fall und werden, wie es bereits weitgehend geschehen ist, die analogen Kommunikationsformen durch digitale ersetzt, droht der Zugang zum Recht beeinträchtigt zu werden.

Während bei der Korrespondenz mit öffentlichen Stellen und anderen Anwälten zunehmend auf sehr sichere Kommunikationswege wie das beA zurückgegriffen werden kann, ist dies bei der Kommunikation mit Mandanten häufig nicht der Fall. Dies gilt insbesondere für die Rechtsberatung gegenüber natürlichen Personen und kleineren Betrieben und Einrichtungen. Gerade wenn, wie in rechtlichen Auseinandersetzungen häufig, Fristen zu beachten sind oder sich Mandanten in einer Notlage befinden und auf den ihnen bekannten Kommunikationswegen schnell und unkompliziert Kontakt zu einem Anwalt aufnehmen möchten, lässt sich ein dem beA vergleichbar sicherer Kommunikationsweg zum Mandanten schwerlich einrichten. Insbesondere viele Privatpersonen sind nicht mit den technischen Begebenheiten und Erforderlichkeiten besonders gesicherter Kommunikationswege vertraut. Sie suchen Rechtsrat in der Regel auf den von Ihnen gewohnten, weit verbreiteten Kommunikationswegen und möchten ihn auch dort in Anspruch nehmen. Besonders gesicherte Kommunikationswege stehen ihnen – insbesondere bei der ersten Kontaktaufnahme – in der Regel nicht zur Verfügung. In einem Rechtsstaat ist es unabdinglich, dass in all diesen Situationen gleichermaßen vertraulich Rechtsrat in Anspruch genommen werden kann. Muss ein Mandant befürchten, dass Dritte und namentlich staatliche Stellen von Mandatsinhalten oder auch nur der Inanspruchnahme des Rechtsrats erfahren, wird er diesen möglicherweise nicht in Anspruch nehmen und in seinem Zugang zum Recht beschränkt sein. Daher gilt es bereits jedem Anschein entgegenzutreten, dass Dritten Einblicke in die Mandatskommunikation gewährt werden könnten.

3. Bedrohungen des Mandatsgeheimnisses durch öffentliche Stellen und Private

Zu den technischen Herausforderungen bei der Gewährleistung vertraulicher Mandatskommunikation treten zunehmend Bestrebungen staatlicher Stellen – namentlich von Sicherheits- und Gefahrenabwehrbehörden – sowie Privater – etwa Plattformbetreibern, Interessenverbänden und Krimineller –, Einblicke auch in eine vertrauliche Online-Kommunikation zu erhalten.

Eine Aussonderung der Mandatskommunikation, die auch in Fällen, in denen staatlichen oder privaten Stellen eine Zugriffsmöglichkeit eingeräumt wird, die Vertraulichkeit der Mandatskommunikation gewährleisten würde, ist in der Regel nicht möglich. Beispielhaft sei an dieser Stelle die im Juli vom Euro-

päischen Parlament angenommene Übergangsverordnung zur Bekämpfung sexuellen Kindesmissbrauchs im Internet genannt. In deren Erwägungsgrund 27 wird nun zwar ein Schutz des Mandatsgeheimnisses postuliert. Die Aufnahme dieses Erwägungsgrundes war aber bis zuletzt so umstritten, dass keinesfalls darauf vertraut werden kann, dass künftige Gesetzgebungsvorhaben entsprechende Klauseln enthalten werden. Schließlich hatten sich Sicherheitspolitiker und Interessensverbände mit erheblichem Einsatz gegen einen entsprechenden Schutz des Mandatsgeheimnisses ausgesprochen und sich damit zunächst durchgesetzt. Dies steht auch künftig zu befürchten. Zudem bleibt fraglich, wie der Schutz des Mandatsgeheimnisses in der Praxis gewährt werden kann, wenn, wie im Falle des Anwendungsbereichs der Übergangsverordnung, eine Aussonderung der Mandatskommunikation praktisch nicht möglich ist, ohne vom Mandatsinhalt Kenntnis zu nehmen.

4. Schlussfolgerung

Angesichts der mannigfaltigen Bedrohungen für das Mandatsgeheimnis im digitalen Raum, unbeantworteter technischen Fragen beim staatlich regulierten Zugriff auf Kommunikationsdienste (Aussonderung von Mandatskommunikation praktisch nicht möglich) sowie der nicht bei allen Entscheidern und Interessenträgern hinreichend ausgeprägten rechtsstaatlichen Sensibilität und Standfestigkeit, ist ein klares Bekenntnis der Europäischen Union zum Schutz des Mandatsgeheimnisses auch im digitalen Bereich dringend geboten. Dabei sollte die Formulierung so gewählt werden, dass die Bedeutung und der Anwendungsbereich des Mandatsgeheimnisses auch für damit nicht vertraute Entscheidungsträger ersichtlich wird.

5. Beantwortung von Einzelfragen

Auf die gesonderte Beantwortung der Fragen unter 1.1., 1.3. und 1.9. in Abschnitt I des Konsultationsfragebogens wird hingewiesen.

* * *

Antworten Konsultationsfragebogen Digitale Grundprinzipien der EU

Auf den Fragebogen der Konsultation der Kommission, antwortet die Bundesrechtsanwaltskammer auf Grundlage der Erfahrungen ihrer Expertinnen und Experten wie folgt:

Zu Abschnitt I:

Zu 1.1.:

Im Kommentarfeld:

> Bei der Bereitstellung universeller Internetzugänge müssen auch die weiteren Nutzungsbedingungen mit in den Blick genommen werden. Hinsichtlich internetgestützter Kommunikation in besonderen Vertrauensbeziehungen – etwa zwischen Mandanten und ihren Anwälten – reicht es nicht aus, allein den Zugang zu Internetdiensten zu garantieren. Damit Mandanten solche für die Inanspruchnahme einer rechtsstaatlichen Grundsätzen genügenden anwaltliche Beratung nutzen können, ist vielmehr zusätzlich erforderlich, dass eine vertrauliche Korrespondenz über diese Dienste möglich ist. Hierzu bedarf es zusätzlicher Garantien. Sofern solche bestehen, kann durch einen Ausbau von Internetzugängen auch der Zugang zum Recht im Interesse der Bürgerinnen und Bürger und des Rechtsstaats insgesamt verbessert werden. Mit Blick auf die Vertrauensbeziehung zwischen Mandanten und Anwälten kann dies etwa durch die von der Bundesrechtsanwaltskammer in Abschnitt II vorgeschlagene Aufnahme eines zusätzlichen Prinzips zum Schutz des Mandatsgeheimnisses im digitalen Bereich gewährleistet werden.

Zu 1.3.

Ankreuzoptionen:

Zum Prinzip: “Every person should submit their data or information only once when they are digitally interacting with public administrations across the European Union.”

Ankreuzempfehlung: Neutral, No Opinion oder keine Auswahl

Zum Prinzip “Digital technologies and solutions should contribute to better levels of public security and safety.”:

Ankreuzempfehlung: Neutral, No Opinion oder keine Auswahl

Im Kommentarfeld:

I. Zu: “Every person should submit their data or information only once when they are digitally interacting with public administrations across the European Union.”

Ein Prinzip, wonach jede Person ihre Daten nur einmal übermitteln sollte, wäre mit erheblichen Risiken für die informationelle Selbstbestimmung der betroffenen Personen verbunden. Die uneingeschränkte Verwirklichung eines solchen Prinzips könnte zumindest fak-

tisch einen uneingeschränkten Datenzugriff sämtlicher Behörden und staatlicher Institutionen in der Europäischen Union ermöglichen oder würde einen solchen zumindest stark vereinfachen. Dies wäre auch rechtsstaatlich bedenklich. Es bestünde erhebliches Missbrauchspotenzial. Insbesondere angesichts der Bedenken der Europäischen Union bezüglich der Einhaltung rechtsstaatlicher Grundsätze in einigen Mitgliedsstaatendarf darf nicht blind darauf vertraut werden, dass sämtliche Behörden in sämtlichen Mitgliedstaaten Daten nur abrufen werden, wenn und soweit dies rechtsstaatlich und datenschutzrechtlich zulässig ist.

Um derartigen Risiken entgegenzutreten, wurde der datenschutzrechtliche Grundsatz der Direkterhebung entwickelt. Dieser sollte an dieser Stelle Anwendung finden.

Sollte gleichwohl ein entsprechendes Prinzip etabliert werden, sollte dies zumindest mit effektiven Sicherungsmaßnahmen flankiert werden. Ein entsprechendes Erfordernis sollte bereits in der Formulierung des Prinzips zum Ausdruck kommen. Dabei sollte die Schaffung von Datenpools ebenso vermieden werden wie uneingeschränkte Zugriffsmöglichkeiten. Sollten Daten doch zentral gehalten werden, wären umso höhere Sicherungsanforderungen zu stellen.

Aus anwaltspraktischer Sicht ist darauf hinzuweisen, dass die Auskunfts-bzw. „Datenlieferungs-“ Pflicht der bzw. des Einzelnen hoch strittig sein und einer Klärung im behördlichen oder gerichtlichen Verfahren bedürfen kann. Dies gilt insbesondere angesichts der vorbeschriebenen Risiken.

Auch um derartige Streitigkeiten zu vermeiden, sollten ein behördlicher Datenabruf bei einer anderen Behörde oder aus einem Datenpool nur mit Zustimmung der betroffenen Person ermöglicht werden; gleiches gilt für die Datennutzung in anderen als dem Ursprungsverfahren.

II. Zu: „Digital technologies and solutions should contribute to better levels of public security and safety“.

Bei allen Verbesserungen, die im Bereich der öffentlichen Sicherheit und Gefahrenabwehr durch den Einsatz digitaler Technologien möglicherweise zu erreichen sind, dürfen die damit einhergehenden Risiken nicht außer Acht gelassen werden. Auch dürfen bestehende rechtsstaatliche und grundrechtliche Garantien durch den Einsatz digitaler Technologien nicht beeinträchtigt werden. Die europäischen Grundwerte gelten im digitalen und analogen Bereich gleichermaßen.

Wenn aber etwa, wie im Zuge des Kampfes gegen sexuellen Kindesmissbrauch, erwogen wird, Kommunikationsinhalte auf den großen und gängigen Online-Kommunikationsplattformen und Messenger-Diensten anlasslos, massenhaft und ohne Rücksicht auf die auf ein möglicherweise bestehendes besonderes Vertrauensverhältnis digital zu durchleuchten, wird in diesem Bereich die Geltung von vertraulichkeitsbasierten Grundrechten und Rechtsstaatsgarantien insgesamt infrage gestellt. Dies gilt in besonderem Maß für das Mandatsgeheimnis und den Zugang zum Recht. Ein solches Ergebnis wäre inakzeptabel.

Mit Blick auf Verkehrsüberwachungssysteme muss sichergestellt sein, dass die Erstellung von Bewegungsprofilen verhindert wird. Der Schutz des Mandatsgeheimnisses gebietet es,

die Möglichkeit zu erhalten, Rechtsanwälte aufzusuchen, ohne dass dies erfasst und bekannt wird. Auch andere digitale Gefahrenabwehrtechnologien, wie etwa der Einsatz von Erkennungssoftware, dürfen die Möglichkeit, einen Anwalt unerkannt aufzusuchen, nicht beschränken.

Angesichts der mit dem Einsatz digitaler Technologien zum Schutz der öffentlichen Sicherheit und Gefahrenabwehr einhergehenden Risiken darf ein solcher Einsatz nicht uneingeschränkt selbst zum Prinzip erklärt und keinesfalls Selbstzweck werden. Vielmehr muss er seinerseits den Werten und Prinzipien der Union gerecht werden bzw. diesen dienen. Zu einer normativen Verschiebung darf es nicht kommen. Sollte ein entsprechendes Prinzip in die Charta aufgenommen werden, sollte dies um die Formulierung ergänzt werden „…soweit dies dem Recht und den Grundwerten der Europäischen Union entspricht".

Zu 1.9.

Zum Prinzip: "No one should be limited or purposefully misguided by algorithmic systems against their autonomy and free will."

Ankreuzempfehlung: Very important

Im Kommentarfeld:

Begrüßenswert und auch für den justiziellen bzw. anwaltlichen Bereich bedeutsam ist die angedachte Einführung des Prinzips *„No one should be limited or purposefully misguided by algorithmic systems against their autonomy and free will."* Dieser Grundsatz sollte indes nicht zu eng gefasst werden. Die Formulierung *„purposefully"* könnte hier zu einer nachteiligen und sicher nicht beabsichtigten Einschränkung führen. Denn es sollten auch unbeabsichtigte Irreführungen vermieden werden. Solche stehen etwa im justiziellen bzw. rechtsberatenden Bereich zu befürchten, wenn eine künstliche Intelligenz unzutreffende oder unvollständige Empfehlungen ausspricht, weil sie etwa mit unzureichenden Daten trainiert wurde oder nicht in der Lage ist, notwendige Schlüsse zu ziehen, die sich nicht aus der Datenlage ergeben. Das Wort *purposefully* sollte daher gestrichen werden.

Zu Abschnitt II:

Antwortoptionen: yes

Es bedarf der Aufnahme des folgenden zusätzlichen digitalen Prinzips zum Schutz einer rechtsstaatlichen Grundsätzen genügenden anwaltlichen Beratung und anwaltlichen Arbeit im digitalen Raum:

Die Vertraulichkeit der Mandatskommunikation wird auch im digitalen Bereich gewährleistet. Die Inanspruchnahme vertraulicher Rechtsberatung muss für jedermann über die von ihm gewählten Kommunikationsnetze bzw. Plattformen frei von staatlicher oder nicht staatlicher Einsichtnahme oder Kontrolle möglich sein. Es darf auch nicht erfasst werden, wer einen Anwalt bzw. eine Anwältin konsultiert hat. Siehe hierzu im Einzelnen die im freien Teil der Konsultation abgegebene Stellungnahme der Bundesrechtsanwaltskammer.

Zur Erläuterung sei auf die beigefügte Stellungnahme der Bundesrechtsanwaltskammer verwiesen.