

Stellungnahme zum
Entwurf eines Gesetzes zur weiteren Digitalisierung der Justiz
BT-Drucks. 20/10943

– Datenschutzrecht als Ermöglichungsrecht –

Die Bundesregierung hat am 8.4.2024 den Entwurf eines Gesetzes zur weiteren Digitalisierung der Justiz vorgelegt. Der Entwurf knüpft an zahlreiche Modernisierungs- und Digitalisierungsvorhaben der Regierung an und setzt sie fort. In diesem Zusammenhang stellt sich regelmäßig die Frage nach dem Datenschutz, der oftmals als Hemmnis statt als Treiber gesehen wird. Digitalisierung und Datenschutz stehen in einem Spannungsverhältnis, aber nicht notwendig in einem Widerspruch, vielmehr ermöglicht der Datenschutz die Digitalisierung – wenn er richtig angewendet und umgesetzt wird. Dabei steht insbesondere der Gesetzgeber im Fokus, denn es liegt auch an ihm, die Verarbeitung personenbezogener Daten rechtssicher zu gestalten.

I. Das Ziel ist würdig und recht

Digitalisierung ist in aller Munde. Nicht selten ist von einem Digitalisierungstau die Rede. Das hat auch die Ampelkoalition erkannt, die die Digitalisierung des Staates als eines ihrer Kernanliegen in ihrem Koalitionsvertrag nennt.¹ Zu Recht, denn es geht dabei nicht lediglich um verbesserte Effizienz oder Produktivität, sondern auch um gesamtgesellschaftliche Fragen und um einen wichtigen Faktor für den Wirtschafts- und Industriestandort Deutschland. Nach dem zuletzt beschlossenen Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens² sowie der geplanten Änderung des Onlinezugangsgesetzes zur Digitalisierung der Verwaltung³ nimmt sich der Gesetzgeber nun auch der Digitalisierung der Justiz an – das tut er nicht zum ersten Mal. Schließlich handelt es sich bei dem vorgelegten Gesetzesentwurf der Bundesregierung um den Entwurf eines Gesetzes zur *weiteren* Digitalisierung der Justiz.⁴ Das ist richtig und wichtig, denn Digitalisierung ist ein fortlaufender Prozess,

¹ Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP), S. 5.

² BGBl. 2024 I, Nr. 101.

³ S. zum aktuellen Stand im Gesetzgebungsverfahren, <https://dip.bundestag.de/vorgang/gesetz-zur-änderung-des-onlinezugangsgesetzes-sowie-weiterer-vorschriften-zur-digitalisierung/300144> (abgerufen am 13.5.2024).

⁴ BT-Drs. 20/10943.

der ständiger Anpassung bedarf. Der Entwurf der Bundesregierung knüpft an zahlreiche Modernisierungs- und Digitalisierungsvorhaben der Vorgängerregierung im Bereich der Justiz an⁵ und umfasst insgesamt 44 Artikel, die Änderungen in sämtlichen Verfahrensordnungen vorsehen. Die geplanten Änderungen reichen von der Möglichkeit der Stellung eines Strafantrags per E-Mail über die Ausweitung von Videoverhandlungen bis hin zu Hybridakten sowie der verpflichtenden elektronischen Aktenführung.

II. Datenschutz und Digitalisierung stehen in einem Spannungsverhältnis, sind aber kein Widerspruch

Bei der Digitalisierung stellt sich zurecht immer wieder die Frage nach dem Datenschutz. Dabei wird er oftmals als Hemmnis statt als Treiber empfunden. Das ist nicht immer falsch, aber eben auch nicht zwingend. Ziel der für den Datenschutz maßgeblichen Datenschutz-Grundverordnung (DSGVO) ist ausweislich ihres Erwägungsgrundes 10 S. 1 einerseits die Gewährleistung eines gleichmäßigen und hohen Datenschutzniveaus für natürliche Personen und andererseits die Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten in der Union.⁶ Datenschutzrecht ist somit in seiner Grundidee ein Ermöglichungsrecht und kein Verhinderungsrecht.⁷ Dies gerät in der Interpretation des Rechts allzu oft in Vergessenheit – mit dann sehr sperrigen Ergebnissen. Das europäische Datenschutzgrundrecht aus Art. 8 GRCh genießt aber eben keinen absoluten Schutz, vielmehr können personenbezogene Daten in dem von der DSGVO vorgegeben Rahmen verarbeitet werden.⁸ Für den Gesetzgeber geht es darum die mitgliedstaatlichen Spielräume auszuschöpfen (1.) – so wie die Bundesregierung das etwa am Beispiel des § 130a Abs. 2 S. 2 ZPO-E i.V.m. § 13a ERVV-E tut (2.).

1. Datenschutzrechtliche Rahmenbedingungen für die Justiz und mitgliedstaatliche Spielräume

Zunächst gilt es den datenschutzrechtlichen Rahmen für die Verarbeitung personenbezogener Daten durch die Justiz abzustecken. In Erwägungsgrund 20 S. 1 DSGVO heißt es: „Diese Verordnung gilt zwar unter anderem für die Tätigkeiten der Gerichte und anderer Justizbehörden, doch könnte im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt werden, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden im Einzelnen auszusehen haben.“ Somit muss sich auch die Justiz an den Datenschutz

⁵ S. etwa das Gesetz zur Modernisierung des Strafverfahrens v. 10.12.2019, BGBl. I S. 2121; Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften v. 25.6.2021, BGBl. I S. 2099; Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer Vorschriften v. 5.10.2021, BGBl. I S. 4607.

⁶ S. auch Art. 1 Abs. 1 DSGVO.

⁷ OLG Hamm, Urt. v. 26.4.2023 – 8 U 94/22, NZG 2024, 120 Rn. 60.

⁸ *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 144 ff.

halten,⁹ mit der Folge, dass sie wie jede andere verantwortliche Stelle auch, eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten benötigt. Diese folgen für die Justiz vor allem aus Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO. Danach ist eine Datenverarbeitung rechtmäßig, wenn sie „zur Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der Verantwortliche unterliegt“ (lit. c) oder wenn sie „für die Wahrnehmung einer Aufgabe erforderlich [ist], die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“ (lit. e). Mitgliedstaaten können den Verantwortlichen die rechtlichen Verpflichtungen oder öffentlichen Aufgaben gemäß Art. 6 Abs. 2 und 3 DSGVO auferlegen bzw. übertragen.¹⁰ Das geschieht in der Praxis für Datenverarbeitungen in der Justiz durch die einschlägigen Vorschriften der jeweiligen Verfahrensordnungen.¹¹ Halten die Mitgliedstaaten die Vorgaben des Art. 6 Abs. 2 und 3 DSGVO ein,¹² wie z.B. die Zweckfestlegung oder die Verfolgung eines im öffentlichen Interesse liegendes Ziel, sind ihnen grundsätzlich keine Grenzen gesetzt. Darüber hinaus können Mitgliedstaaten nicht nur in eigener Regie datenschutzrechtliche Rechtsgrundlagen schaffen, sondern gemäß Art. 4 Nr. 7 Hs. 2 DSGVO auch Verantwortliche bzw. die Kriterien ihrer Benennung vorsehen. Die DSGVO bietet den Mitgliedstaaten – nicht nur für den Bereich der Justiz – sehr weite Spielräume, die sie durch eigene Rechtssetzung ausfüllen und gestalten können.

2. Schaffung von datenschutzrechtlichen Rechtsgrundlagen am Beispiel des § 130a Abs. 2 S. 2 ZPO-E i.V.m. § 13a ERVV-E

Der Entwurf eines Gesetzes zur weiteren Digitalisierung der Justiz sieht unter anderem eine Änderung des § 130a ZPO-E („Elektronisches Dokument; Verordnungsermächtigung“) vor, der Regelungen zum elektronischen Dokument im Zivilprozess trifft. Konkret geht es um eine Ergänzung des § 130a Abs. 2 S. 2 ZPO a.E., der im Ergebnis wie folgt aussehen soll:¹³

(2) ¹Das elektronische Dokument muss für die Bearbeitung durch das Gericht geeignet sein. ²Die Bundesregierung bestimmt durch Rechtsverordnung mit Zustimmung des Bundesrates technische Rahmenbedingungen für die Übermittlung und die Eignung zur Bearbeitung durch das Gericht sowie das Nähere zur Verarbeitung von Daten der Postfachinhaber nach Absatz 4 Satz 1 Nummer 4 und 5 in einem sicheren elektronischen Verzeichnis.

⁹ Vgl. auch EuGH, Urt. v. 2.3.2023 – C-268/21, BeckRS 2023, 2998 Rn. 28; s. hierzu *Schemmer/Lange*, ZGI 2024, 56, 56 f.

¹⁰ Taeger/Gabel/Taeger, 4. Aufl. 2022, Art. 6 DS-GVO Rn. 153.

¹¹ S. etwa das SG Mannheim, Datenverarbeitung in der Justiz, <https://sozialgericht-mannheim.justiz-bw.de/pb/Lde/Startseite/Service/Datenverarbeitung+in+der+Justiz> (abgerufen am 13.5.2024).

¹² Das Verhältnis der von Abs. 2 zu Abs. 3 ist indes umstritten; s. hierzu Kühling/Buchner/*Buchner/Petri*, 4. Aufl. 2024, Art. 6 DS-GVO Rn. 195 f.

¹³ BT-Drs. 20/10943, Art. 13.

Diese Vorschrift verweist bezüglich der technischen Rahmenbedingungen für die Übermittlung von elektronischen Dokumenten und der Eignung zur Bearbeitung durch das Gericht auf die ERVV.¹⁴ Die geplante (oben unterstrichene) Ergänzung ist auch für die Verfahrensordnungen der StPO, des ArbGG, SGG sowie der VwGO und FGO vorgesehen.¹⁵ Konkret verweist die Ergänzung auf den neu geplanten § 13a ERVV-E verwiesen, der in seinem Abs. 1 regelt, „welche Daten von Inhabern von eBOs¹⁶ und Inhabern von Postfächern eines OZG-Nutzerkontos¹⁷ beim Betrieb solcher Postfächer zur Auffindbarkeit und Adressierung im sicheren Verzeichnis verpflichtend gespeichert und abgerufen werden dürfen.“¹⁸ In Abs. 2 werden Kriterien für die Bestimmung des datenschutzrechtlich Verantwortlichen festlegt.

Das Augenmerk soll an dieser Stelle weniger auf den konkreten Inhalt, sondern auf die Regelungstechnik gerichtet werden, also den Verweis auf eine Rechtsverordnung, die die nähere Ausgestaltung der Datenverarbeitung regelt. Eine solche Vorgehensweise ist mit den Vorgaben der DSGVO vereinbar. Zwar handelt es sich bei einer Rechtsverordnung um kein formelles Parlamentsgesetz, jedoch fallen auch Gesetze im materiellen Sinne unter das Recht der Mitgliedstaaten, sodass auch im Rahmen von Rechtsverordnungen rechtliche Verpflichtungen oder öffentliche Aufgaben auferlegt bzw. übertragen werden können.¹⁹ Darüber hinaus zählen auch z.B. kommunale Satzungen zum Recht des Mitgliedstaats.²⁰ Denn in Erwägungsgrund 41 S. 1 DSGVO heißt es: „Wenn in dieser Verordnung auf eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt; davon unberührt bleiben Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats.“ Selbstverständlich muss die Rechtsverordnung selbst den Anforderungen des Grundgesetzes (vgl. Art. 80 GG) entsprechen.²¹ Wenn das der Fall ist, kann ohne Weiteres auch eine Vorschrift aus einer Rechtsverordnung als Rechtsgrundlage herangezogen werden.

III. Konsequenzen (nicht nur für den Entwurf eines Gesetzes zur weiteren Digitalisierung der Justiz) und zugleich eine kurze Summa

Was folgt aus dem o.g. Beispiel zu § 130a Abs. 2 S. 2 ZPO-E i.V.m. § 13a ERVV-E für die Digitalisierung? Das gewählte Beispiel ist sicherlich keiner der großen Streitpunkte des

¹⁴ Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV); s. auch Musielak/Voit/Stadler, 21. Aufl. 2024, § 130a ZPO Rn. 3.

¹⁵ BT-Drs. 20/10943, Art. 1, 22, 25, 28, 31.

¹⁶ Besonderes elektronisches Bürger- und Organisationenpostfach, vgl. § 130a Abs. 4 S. 1 Nr. 4 ZPO.

¹⁷ Nutzerkonto nach § 2 Abs. 5 OZG, vgl. § 130a Abs. 4 S. 1 Nr. 5 ZPO.

¹⁸ BT-Drs. 20/10943, S. 70.

¹⁹ Ehmann/Selmayr/Heberlein, 3. Aufl. 2024, Art. 6 DS-GVO Rn. 60; Kühling/Buchner/Buchner/Petri, 4. Aufl. 2024, Art. 6 DS-GVO Rn. 84.

²⁰ VGH München, Beschl. v. 20.08.2019 – 12 ZB 19.333, BeckRS 2019, 18701 Rn. 74.

²¹ Kühling/Buchner/Buchner/Petri, 4. Aufl. 2024, Art. 6 DS-GVO Rn. 84.

Gesetzesentwurfs, jedoch kann es dazu dienen, aufzuzeigen, dass der Datenschutz richtig interpretiert kein Hemmnis für die Digitalisierung ist. Die DSGVO bietet den Mitgliedstaaten etwa über Art. 6 Abs. 2 und 3 DSGVO genügend Spielraum, um selbst rechtssetzend tätig zu werden und Datenverarbeitungen zu ermöglichen und zu gestalten. Der nationale Gesetzgeber hält alle Karten in der Hand. Er muss von seinen Möglichkeiten nur Gebrauch machen. Hierzu kann er sich neben formellen Gesetzen auch materiellen Gesetzen bedienen. Letztere bieten den Vorteil, dass datenschutzrechtliche Rechtsgrundlagen geschaffen werden können, ohne dass das Gesetzgebungsverfahren für formelle Parlamentsgesetze durchlaufen werden muss. Selbstverständlich müssen die materiellen Gesetze ihrerseits den Anforderungen des GG entsprechen. Der Gesetzgeber muss den Datenschutz nur von Anfang an berücksichtigen, damit er die Spielräume der DSGVO ausschöpfen und etwaige Datenverarbeitungen rechtssicher ermöglichen und gestalten kann. Anderenfalls können sich Lücken ergeben, die zu erheblicher Rechtsunsicherheit führen.

Der scheidende Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) traf es mit folgender Aussage ganz gut: „Digitalisierung ohne Datenschutz ist wie die Entwicklung eines Medikamentes ohne Prüfung auf Nebenwirkung“.²² Der Datenschutz steht der Digitalisierung nicht entgegen. Er muss nur von Anfang an Beachtung finden. Das gilt nicht nur die Digitalisierung der Justiz, sondern auch für alle anderen Bereiche der Gesellschaft. Daher: Mehr Mut zur Digitalisierung!

* * *

²² BfDI, Pressemitteilung vom 31.12.2018, https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2018/11_DigitalisierungUndDatenschutz.html (abgerufen am 13.5.2024).