§ 41 eGovernment und eJustice

Schrifttum: Anders/Gehle/Anders, 80. Aufl. 2022, ZPO § 130a; Jörg Berkemann, Freies Recht für freie Bürger! in: JurPC Web-Dok. 188/1999, Abs. 1–79; Bernhardt, Deutschland nicht „eIDAS-ready?, NJW-aktuell H. 20/2016, 17; Bernhardt, E-Government in Deutschland und Europa, Keynote auf dem 25. Drei-Länder-Treffen der Deutschen Gesellschaft für Recht und Informatik e. V. (DGRI) am 21. Juni 2018 in St. Gallen, DGRI Jahrbuch 2018, 213–234; Bernhardt, Editorial „Wie können wir die Rechtstreue des Staates sichern?", Verwaltung & Management 2021, 202; Bernhardt, Europa und die Herausforderung der Digitalisierung, in: Henning Lühr, Brauchen wir eine neue Staatskunst? Herausforderungen für das Staats- und Verwaltungshandeln durch die digitale Entwicklung – Ergebnisse des Kolloquiums im Bremer Rathaus, 2019, 132 ff.; Bernhardt, E-Justice überwindet die Grenzen innerhalb Europas, JurPC Web-Dok. 75/2007, Abs. 1–43; Bernhardt, in: Chibanguza/Kuß/Steege (Hrsg.), Künstliche Intelligenz, Recht und Praxis automatisierter und autonomer Systeme, 2021; Bernhardt, Die deutsche Justiz im digitalen Zeitalter. Entwicklung und Entwicklungsperspektiven von E-Justice, NJW 2015, 2775 ff.; Bernhardt, Quo vadis Digitalisierung der Justiz? jM 2018, 310 ff.; Bernhardt, Quo vadis Ampel? Digitalisierung der Justiz, jM 2022, S. 90 ff.; Bernhardt, The Use of Artificial Intelligence in the Field of Justice, in: Szostek/Załucki (Hrsg.) Internet and New Technologies Law, S. 173 ff.; Bernhardt, Structuring Judicial Communication, in: Bergener/Räckers/Stein (Hrsg.), The Art of Structuring, 2019, S. 241 ff.; Bernhardt, Verfassungsprinzipien. Verfassungsgerichtsfunktionen- Verfassungsprozessrecht im EWG-Vertrag, 1987; Bernhardt/Leeb in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl., Kap. 6 (Stand: 23.1. 2024); Bernhardt/Leeb in: Kramer/Kuhn/Putzke, Was muss Juristenausbildung heute leisten? 84 ff.; Bertrams, DRiZ 2010, S. 248 ff.; Bertrams, Zentralisierung der Informationstechnik in der Landesverwaltung Nordrhein-Westfalen unter Einbeziehung der Dritten Gewalt?, NWVBl. 2007, 205; Bertrams, Eingriff in die Unabhängigkeit der Dritten Gewalt durch Zentralisierung der IT-Organisation unter dem Dach der Exekutive, NWVBl. 2010, 209); Biallaß, Der Umgang mit dem elektronischen Empfangsbekenntnis, NJW 2019, 3495 ff.; Biallaß, in: Ory/Weth, jurisPK-ERV Band 1, 2. Aufl., Kapitel 8 (Stand: 23.11.2022); Bomhard/Merkle, Der Entwurf eines EU Data Acts, RDi 2022, 168; Brandhorst, https://www.dbb.de/mediathek/magazine/europathemen/artikel/das-engagement-der-eu-fuer-den-digitalen-staat.html; abgerufen am 15.4.2022; Brosch/Lummel/Sandkühler/Freiheit, Elektronischer Rechtsverkehr mit dem beA, 2017; Büttner, JurPC Web-Dok. 117/2016; Effer-Uhe, Möglichkeiten des elektronischen Zivilprozesses, MDR 2019, 69; Gaier, Der moderne liberale Zivilprozess, NJW 2013, 2871; Goodenough, Legal Technology 3.0, HuffPost v. 2.4.2015, https://www.huffpost.com/entry/legal-technology-30_b_6603658; Graef/Husovec/van den Boom, Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes, EuCML 2020, 3; Greger, Der Zivilprozess auf dem Weg in die digita-le Sackgasse, NJW 2019, 3429 ff; Hähnchen, Was ist „Elektronischer Rechtsverkehr"?, JurPC Web-Dok. 151/2007, Abs. 1–22; Hähnchen/Schrader/Weiler/Wischmeyer, Legal Tech, JuS 2020, 625; Heckmann in: Wirtz, E-Government, 2020, S. 93 ff.; Heinze/Prado Ojea, Der Beweis mit privaten elektronischen Dokumen-ten nach ZPO und elDAS-VO, CR 2018, CR 2018, 37; Herberger, Ejustice-Kompetenz – Plädoyer für ein Ausbildungskonzept, in: Gottwald (Hrsg.) e-Justice in Österreich. Erfahrungsberichte und europäischer Kontext, Festschrift für Martin Schneider, 2013, S. 391–402; Hoffmann/Luch/Schul/Borchers, Die digitale Dimension der Grundrechte Baden-Baden, 2015; Hoffmann/Köhnlein, in: BeckOK GVG, 6. Ed. 2020, § 23 EGGVG; Jansen in: Ory/Weth, jurisPK-ERV Band 1, 2. Aufl., Kapitel 5.3 (Stand: 6.12.2023); Kipker, EAID: EU-Datenstrategie: Welche Auswirkungen ergeben sich für den Datenschutz?, ZD-Aktuell 2022, 04465; Klasen in: Ory/Weth, jurisPK-ERV Band 2, 2. Aufl., § 128a ZPO (Stand: 6.2.2024)); Köbler, Die Videoverhandlung im Zivilprozess – Vorschlag einer Neuregelung, NJW 2021, 1072; Köbler, Und es geht doch: Strukturierter Parteivortrag – ein Werkstattbericht, AnwBl Online 2018, 399; Köbler, Neue Formen der Prozessführung, in: Ory/Weth, jurisPK-ERV Band 1, 2. Aufl., Kapitel 7 1. Überarbeitung (Stand: 16.1.2024); Köbler/Herberger, Und es geht doch: Strukturierter Parteivortrag – Werkstattbericht Nr. 2, AnwBl 2019, 351; Leeb, Digitalisie-rung, Legal Technology and Innovation, Berlin 2019; Marly, Keine Verletzung der richterlichen Unabhängig-keit durch Nichtvorlage von Ausdrucken zum elektronischen Handelsregister, LMK 2011, 313258; Meissner/Schenk, in: Schoch/Schneider Bier, VwGO, 37. EL 2019, § 55 VwGO; Möller, Der digitale Postausgang, NJW 2021, 2179; Müller, Der elektronische Rechtsverkehr im arbeitsgerichtlichen Verfahren, NZA 2019, 11 ff.; Müller, E-Justice reloaded- Der Gesetzgeber justiert den elektronischen Rechtsverkehr nach, RDi 2021, 486 ff.; Müller, Die neuen Formvorschriften im elektronischen Rechtsverkehr ab dem 1.1.2018, NZS 2018, 207; Müller in: jurisPK-ERV Band 2, § 130a ZPO; Müller/Gomm, jM 2021, 222; Oltmanns/Fuhlrott, Die Nutzungspflicht des elektronischen Rechtsverkehrs: Unverhältnismäßige Einschränkung des Justizgewährungsanspruchs? NZA 2020, 897; Paschke, Digitale Gerichtsöffentlichkeit – Informationstechnische Maßnahmen,

rechtliche Grenzen und gesellschaftliche Aspekte der Öffentlichkeitsgewähr in der Justiz, 2018; Peuker, Die Digitalisierung der Kommunalverwaltung, DÖV 2022, 275; Posser/Wolff, BeckOK VwGO, 60. Edition, § 55a VWGO; Radke, EJustice – Aufbruch in die digitale Epoche, JurPC Web-Dok. 46/2006, Abs. 1–28; Richter, 2022: Ankunft im Post-Open-Data-Zeitalter, ZD 2022, 3; Rolfs/Giesen/Meßling/Udsching, BeckOK Arbeitsrecht, 63. Edition, Stand: 1.3.2022; Roßnagel, Beweiswirkungen elektronischer Vertrauensdienste, MMR 2016, 647; Sander, BeckOK BNotO, 5. Ed. 31.7.2021; Schildbach, Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes, ZD 2022, 148, 152; Schmitz, BeckOK VwGO/ 60. Ed. 1.1.2022, VwGO § 55a; Schnelle/Bender, Der elektronisch gestützte Zivilprozess – Das „Neue Stuttgarter Modell", DRiZ 1993, 97–109; Schürger/Kersting in: Viefhues, Elektronischer Rechtsverkehr, Ausgabe 2/2016; Schulz, Kooperationsmodelle zur Umsetzung des Einheitlichen Ansprechpartners als unzulässige Mischverwaltung?, DÖV 2008, 1028; Siegel, Der Europäische Portalverbund – Frischer Digitalisierungswind durch das einheitliche digitale Zugangstor („Single Digital Gateway"), NVwZ 2019, 905, 909; Ulrich/Schmieder, Die elektronische Einreichung in der Praxis, NJW 2019, 113; Viefhues in: Ory/Weth, jurisPK-ERV Band 1, 1. Aufl., Kapitel 1, (Stand: 4.1.2022); Völzmann, Effektiver Rechtsschutz durch Legal Tech? , DÖV 2021, S. 474; Vorwerk, Strukturiertes Verfahren im Zivilprozess; NJW 2017, 2326, 2326;Vorwerk/Wolf, BeckOK § 130d ZPO, 44. Edition, Stand: 1.3.2022; Wahedi, Verfassungsrechtliche Anforderungen an die Automatisierung der Justiz, 2021; Windoffer, Die Implementierung einheitlicher Ansprechpartner nach der EU-Dienstleistungsrichtlinie – Problemfelder und Anpassungsbedarf im nationalen Recht, NVwZ 2007, 495; Zwickel, Die digitale Strukturierung und inhaltliche Erschließung zivilprozessualer Schriftsätze im Spannungsfeld zwischen Parteiherrschaft und Richtermacht, in: Buschmann/Gläß/Gonska et al., Digitalisierung der gerichtlichen Verfahren und das Prozessrecht – 3. Tagung junger Prozessrechtswissenschaftler und -wissenschaftlerinnen am 29./30.9.2017 in Leipzig, 2018, S. 179 ff.

I. Europäisches E-Government

1. Allgemein

1 **a) Rolle der Kommission.** E-Government auf europäischer Ebene ist bestimmt vor allem durch die Koordinierung der mitgliedstaatlichen Aktivitäten auf diesem Gebiet, denn der größte Teil der Verantwortung für die Digitalisierung der öffentlichen Verwaltung liegt bei den EU-Mitgliedstaaten. Die Verantwortung für die Koordinierung nimmt seit zwei Jahrzehnten vor allem die **EU-Kommission** wahr. Innerhalb der Kommission sind verschiedene Generaldirektionen zuständig: Die GD CNET (Generaldirektion für Kommunikationsnetze, Inhalte und Technologien), die GD DIGIT (Generaldirektion für Datenverarbeitung) und die GD GROW (Generaldirektion für Binnenmarkt, Industrie, Unternehmertum und KMU). Inhaltlich wurde die Kommission tätig insbesondere durch E-Government-Programme,[1] etwa durch die Government-Aktionsplan2016-2020,[2] durch gemeinsame Projekte mit den Mitgliedstaaten,[3] aber vor allem durch Gesetzgebungsinitiativen –Vorschläge für Verordnungen und Richtlinien. Bei diesen Initiativen beruft sich die EU-Kommission vor allem auf

[1] Etwa die Programme eEurope 2002 – Eine Informationsgesellschaft für alle- Entwurf eines Aktionsplans der Europäischen Kommission vom 24.5.2000 zur Vorlage auf der Tagung des Europäischen Rates am 19./20.6.2000 in Feira (KOM (2000) 330 endgültig); Strategie i2010 – Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung, als Mitteilung der Kommission vom 1.6.2005 an den Rat, das Europäische Parlament, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen(KOM 2005, 229 endgültig); die Digitale Agenda 2020 als Teil der im Juni 2010 vom Europäischen Rat verabschiedeten Strategie Europa 2020 (Mitteilung der Kommission vom 19.5.2010 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine Digitale Agenda für Europa", KOM(2010) 245 endgültig, nicht im Amtsblatt veröffentlicht).

[2] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und an den Ausschuss der Regionen: EU-eGovernment-Aktionsplan 2016–2020 – Beschleunigung der Digitalisierung der öffentlichen Verwaltung, COM(2016) 179 final.

[3] Etwa das SCOOP4C-Projekt, das von der Europäischen Kommission im November 2016 ins Leben gerufen finanziert wurde. Fünf Organisationen aus vier verschiedenen Mitgliedsstaaten erforschten, wie das Once-Only-Prinzip für Bürger/innen auf europäischer Ebene umgesetzt werden kann. Ferner ist beispielhaft das Projekt TOOP zu erwähnen (The Once-Only Principle Project), das im Januar 2017 (bis zum 31.3.2021) von rund 50 Organisationen aus 20 EU-Mitgliedstaaten und assoziierten Ländern mit dem Ziel initiiert wurde, das Once-Only Prinzips im grenzüberschreitenden, gesamteuropäischen Maßstab zu erforschen, wobei der Schwerpunkt auf der Verringerung des Verwaltungsaufwands für Unternehmen lag, https://toop.eu/, abgerufen am 29.2.2024.

die EU-Binnenmarktkompetenz gemäß Art. 114 AEUV,[4] denn auch für die Wahrnehmung der EU-Freiheiten ist die Verwaltungsdigitalisierung ein entscheidender Erfolgsfaktor. Darüber hinaus sichert die Möglichkeit, grenzüberschreitend digitale Verwaltungsleistungen wahrnehmen zu können, auch die wirtschaftliche Wettbewerbsfähigkeit der EU.[5]

b) Rolle des Rats der Europäischen Union. Ferner trug der **Rat der Europäischen Union** für europäisches E-Government Verantwortung,[6] heute vor allem in den Ratsformationen „TTE-Rat" (Transport, Telekommunikation und Energie) und bei Wettbewerbsthemen der „COMPET-Rat". Unterstützt werden die Aktivitäten durch Formationen von Sachverständigen, vor allem durch die „Strategiegruppe Digitaler Binnenmarkt", mit hochrangigen Vertretern der Mitgliedstaaten zur Gestaltung der digitalen Zukunft Europas. 2

c) Rolle des Europäischen Parlaments. Das **Europäische Parlament** ist ebenfalls in die E-Government- Aktivitäten eingebunden, vor allem durch den ITRE-Ausschuss (Ausschuss für Industrie, Forschung und Energie), den LIBE-Ausschuss (Ausschuss für bürgerliche Freiheiten, Justiz und Inneres) und den IMCO-Ausschuss (Ausschuss für Binnenmarkt und Konsumentenschutz). 3

2. EU-Verordnungen[7]

EU- Verordnungen müssen nicht in einzelstaatliches Recht umgesetzt werden. Sie sind in allen ihren Teilen verbindlich und gelten unmittelbar in allen Mitgliedsländern, was zur Folge hat, dass entgegenstehendes nationales Recht mit dem Inkrafttreten der Verordnung unanwendbar wird. Dabei setzt gerade eine EU-Verordnung erfahrungsgemäß wichtige Impulse für die nationalen E-Government-Entwicklungen;[8] so hätte Deutschland seine EU-Verpflichtungen aus der SDG-Verordnung ohne die Forcierung der OZG-Gesetzgebung in noch geringerem Maße erfüllen können. 4

a) Verordnung des Europäischen Parlaments und des Rates vom 21.11.2018 über die Einrichtung eines zentralen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/201 („Single Digital Gateway"- SDG-Verordnung). aa) Allgemein. Die Verordnung stellt die zentrale Norm für das E-Government in Europa im engeren Sinne dar. Sie ist seit November 2018 in Kraft. Ziel der Verordnung ist es, Informationen, Verfahren und Unterstützungsdienste der öffentlichen Verwaltungen grenzüberschreitend nutzbar zu und die Interaktionen zwischen Bürgern und Unternehmen einerseits und den zuständigen Behörden anderseits grenzüberschreitend zu erleichtern und Diskriminierungen infolge nationaler Zugangsbarrieren zu verhindern, letztlich damit den Zugang zum Binnenmarkt zu erleichtern. Aus der unmittel- 5

[4] Art. 114 AEUV verweist wiederum auf Art. 26 AEUV, der in den ersten beiden Absätzen folgende Aussagen trifft: „(1) Die Union erlässt die erforderlichen Maßnahmen, um nach Maßgabe der einschlägigen Bestimmungen der Verträge den Binnenmarkt zu verwirklichen beziehungsweise dessen Funktionieren zu gewährleisten. (2) Der Binnenmarkt umfasst einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gemäß den Bestimmungen der Verträge gewährleistet ist."

[5] Brandhorst, https://www.dbb.de/mediathek/magazine/europathemen/artikel/das-engagement-der-eu-fuerden-digitalen-staat.html, abgerufen am 29.2.2024.

[6] Ein Meilenstein war die Malmöer Erklärung vom 18.11.2009 der Minister für eGovernment der EU-Mitgliedstaaten, der Beitritts- und Kandidatenländern sowie der Länder der Europäischen Freihandelszone. Sie sah vor, dass bis 2015 Bürgerinnen und Bürger sowie Unternehmen nutzerzentrierte E-Government- Services erhalten sollten, die die Transparenz staatlichen Handelns erhöhen sowie den Zugang zu öffentlichen Informationen und die Partizipation am staatlichen Handeln erleichtern sollten. Ferner sollte die Mobilität im Binnenmarkt erhöht, grenzüberschreitend Unternehmensgründungen und -niederlassungen sowie das Studieren, Arbeiten und die Wahl des Alterswohnsitzes vereinfacht werden. Ähnlich bedeutsam die Tallinn-Erklärung von 2017, in der die Prinzipien europäischen E-Governments benannt wurden: Digital by default, Inklusivität und Barrierefreiheit, Once Only, Vertrauenswürdigkeit und Sicherheit, Offenheit und Transparenz, Interoperabilität by default, https://www.bmi.bund.de/Webs/PA/DE/verwaltung/eIDAS-verordnung-der-EU/tallinn-erklaerung-zu-e-government/tallinn-erklaerung-zu-e-government-node.html;jsessionid=7B1F86FD99CB3CC60328BA19177E307C.2_cid295#doc14626862bodyText1, abgerufen am 29.2.2024.

[7] Zu den Rechtsakten allgemein: von Mangoldt/Klein/Starck GG Art. 91c Rn. 9, 10.

[8] Henning Lühr/Bernhardt S. 132 ff.

bar anwendbaren Verordnung ergeben sich auch Vorgaben für nationale Vorschriften und Verfahren, mit denen Binnenmarktrechte (wie Freizügigkeit) ausgeübt werden. Instrument ist die Schaffung eines einheitlichen digitalen europäischen Zugangstors von Kommission und Mitgliedstaaten mit einer gemeinsamen Nutzerschnittstelle, die die in das Portal „Ihr Europa" zu integrieren ist. Über dieses Zugangstor soll der Zugang zu den einschlägigen Websites von Union und Mitgliedstaaten geboten werden (Art. 2 Abs. 1, Art. 18 SDG-VO).

6 **bb) Verpflichtungen** aus der SDG-Verordnung:

(1) **Zugang zu bestimmten Informationen in Deutsch und Englisch über allgemeingültige Rechte und Pflichten** gemäß Anhang I der SDG-VO und ihrer Spezifika in Deutschland. Dies betrifft die Bereiche

(a) **Reisen innerhalb der Union** (etwa Dokumente wie Personalausweis, Visum, Pass); Rechte und Pflichten von Flug-, Zug-, Schiffs- und Busreisenden in und aus der Union und von Personen, die Pauschalreisen oder verbundene Reiseleistungen in Anspruch nehmen; Hilfestellung bei eingeschränkter Mobilität bei Reisen, Mitnahme von Tieren, Pflanzen, Alkohol, Tabak, Zigaretten ua, Anrufe und Versand und Empfang von elektronischen Nachrichten und elektronischen Daten innerhalb der Union Arbeit und Ruhestand innerhalb der Union;

(b) **Arbeit und Ruhestand innerhalb der Union** (wie Arbeitssuche, Aufnahme einer Beschäftigung, Anerkennung von Qualifikationen zum Zwecke der Beschäftigung jeweils in einem anderen Mitgliedstaat, Besteuerungsfragen, Beschäftigungsbedingungen, Gleichbehandlungsvorschriften, Gesundheits- und Sicherheitsvorschriften, Rechte und Pflichten im Bereich der sozialen Sicherheit);

(c) **Fahrzeuge in der Union** (ua vorübergehende oder dauerhafte Mitnahme eines Kraftfahrzeugs in einen anderen Mitgliedstaat, Führerscheinfragen, An- und Verkauf von Fahrzeugen, nationalen Verkehrsvorschriften);

(d) **Wohnsitz in einem anderen Mitgliedstaat** (ua vorübergehender oder dauerhafter Umzug in einen anderen Mitgliedstaat, Teilnahme an Kommunalwahlen);

(e) **Bildung und Praktikum** (ua Schulbesuch, Hochschulbesuch und Praktika in einem anderen Mitgliedstaat, Forschungstätigkeit);

(f) **medizinische Versorgung** (ua medizinische Behandlung in einem anderen Mitgliedsstaat), Arzneimittelkauf, Präventionsmaßnahmen, Rechte und Voraussetzungen für den Einzug in stationäre Pflegeeinrichtungen);

(g) **Bürger- und Familienrechte** (zB grenzüberschreitende Familienrechte und -pflichten, erbrechtliche Regelungen);

(h) **Verbraucherrechte** (Kauf von Waren und Dienstleistungen aus einem anderen Mitgliedstaat sowie Finanzdienstleistungen – online oder offline- , Besitz von Bankkonten in einem anderen Mitgliedstaate, Inanspruchnahme von öffentlichen Dienstleistungen, zB Gas-, Strom-, Wasserversorgung, Telekommunikationsdienstleistungen und Internet);

(i) **Datenschutzregelungen;**

(j) **Gründung, Führung und Schließung eines Unternehmens** (zB Registereintragungen Arbeitsnehmerrechte);

(k) **Steuern, Waren, Dienstleistungen, Finanzierung eines Unternehmens, Öffentliche Aufträge, Gesundheit und Sicherheit am Arbeitsplatz.**

7 (2) **Leistungsbeschreibungen zu On- und Offline-Verfahren** und Links zu **Online-Verfahren** auf nationaler Ebene, um die Bürger in die Lage zu versetzen, ihre Rechte wahrzunehmen und die entsprechenden Pflichten und Vorschriften einzuhalten.

8 (3) **Informationen über Hilfs- und Problemlösungsdienste (Unterstützungsdienste)** als solche sowie **deren Verfahren** (über den Einheitlichen Ansprechpartner, die Produktinfostellen, die Informationsstellen für Bauprodukte, nationale Beratungsstellen für berufliche Qualifikationen, nationale Beratungsstellen für berufliche Qualifikationen und die Online-Streitbeilegung); Art. 7 schreibt vor, dass die Mitgliedstaaten und die Kommission sicherzustellen haben, dass die (auch grenzüberschreitenden) Nutzer online über

verschiedene Kanäle auf die Hilfs- und Problemlösungsdiensten leicht zugreifen können.

(4) **Fristen** für **Informationsbereitstellung.** Bis Dezember 2020 waren die Informationen über allgemeine Rechte und Vorschriften, On- und Offline-Verfahren sowie über die Unterstützungsdienste von den Mitgliedstaaten zur Verfügung zu stellen. Kommunalbehörden waren bis spätestens zum 12.12.2022 verpflichtet, die Informationen zur Verfügung zu stellen. Die SDG-Regelungen gelten allerdings nicht für Informationen, die bereits im E-Justice-Portal hinterlegt sind. Mit dieser Ausnahmeklausel soll verhindert werden, dass die Justiz verpflichtet ist, für eine doppelte Informationsbereitstellung zu sorgen. Allerdings gelten die SDG-Regelungen immer dann, wenn Gerichte als Verwaltung agieren (Justizregister). 9

(5) **Online-Zugang zu bestimmten Verfahren** nach Art. 2 Abs. 2 lit. b SDG-VO. Die Mitgliedstaaten haben gemäß Art. 6 bestimmte, in Anhang II aufgeführte Verfahren diskriminierungsfrei online anzubieten. Das betrifft etwa den Nachweis über die Eintragung in das Geburtenregister oder die Geburtsurkunde, die Entscheidung über den Antrag auf Studienfinanzierung, die Entscheidung über den Antrag auf Anerkennung von akademischen Diplomen, Prüfungszeugnissen oder sonstigen Nachweisen über Studien oder Kurse, die Entscheidung über die Europäische Krankenversicherungskarte, die Bestätigung der Abmeldung von der früheren Adresse und der Anmeldung an der neuen Adresse, den Kfz-Zulassungsnachweis, die Bestätigung des Eingangs des Antrags oder des Beschlusses über den Antrag auf Ruhestands- oder Vorruhestandsleistungen. Von dem reinen Online-Verfahren kann abgewichen werden, wenn der angestrebte Zweck in begründeten Ausnahmefällen aus übergeordneten Gründen des öffentlichen Interesses in den Bereichen öffentliche Sicherheit, öffentliche Gesundheit oder Bekämpfung missbräuchlichen Verhaltens nicht vollständig online erreicht werden kann. Dann können die Mitgliedstaaten verlangen, dass der Nutzer für einzelne Verfahrensschritte persönlich bei der zuständigen Behörde vorstellig wird., Art 6 Abs. 3 SDG-VO. 10

(6) **Nichtdiskriminierung.** Die Mitgliedstaaten müssen sicherstellen, dass die Websites ihrer öffentlichen Stellen gemäß den Grundsätzen der Wahrnehmbarkeit, Bedienbarkeit, Verständlichkeit und Robustheit zugänglich sind und den in der Richtlinie EU 2016/2102[9] festgelegten Anforderungen genügen. Die dargestellten Online-Verfahren müssen auch für grenzüberschreitende Nutzerinnen und Nutzer auf nichtdiskriminierende Art mit Hilfe derselben oder einer alternativen technischen Lösung online zugänglich sein und von diesen online abgewickelt werden können (Art. 13 Abs. 1). Nutzerinnen und Nutzer müssen sich gemäß der eIDAS-Verordnung elektronisch ausweisen und authentifizieren, Unterlagen unterzeichnen oder mit einem Siegel versehen können (Art. 13 Abs. 2 Buchst. b). Die Beibringung von Nachweisen in elektronischem Format ist grenzüberschreitenden wie inländischen Nutzern zu ermöglichen (Art. 13 Abs. 2 Buchst. d). Ist zur Abwicklung eines Verfahrens eine Zahlung erforderlich ist, sollen die Nutzer grenzüberschreitende Zahlungsdienste ohne Diskriminierung aufgrund des Niederlassungsorts des Zahlungsdienstleisters, des Ausstellungsorts des Zahlungsinstruments oder des Standorts des Zahlungskontos in der Union nutzen können (Art. 13 Abs. 2 Buchst. e). 11

(7) **Once Only.** Die Online-Verfahren sind an das von der Kommission in Kooperation mit den Mitgliedstaaten bereitgestellte europaweite Once-Only-Technical-System (OOTS) anzuschließen. Mit Hilfe des OOTS soll der Austausch von Nachweisen europaweit grenzüberschreitend und automatisiert zwischen Behörden erfolgen. Für Bürgerinnen, Bürger und Unternehmen erübrigt sich damit das mehrfache Bereitstellen von Nachweisen, sofern sie einer Übermittlung des jeweiligen Nachweises zustimmen (Art. 14). 12

(8) **Qualitätsanforderungen.** Art. 9 bis 11 regeln Qualitätsanforderungen im Zusammenhang mit Informationen über Rechte, Pflichten und Vorschriften und über Hilfs- und Problemlösungsdienste. Art. 12 betrifft die Übersetzungsfragen und Art. 17 das System 13

[9] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L2102.

der Qualitätsüberwachung. Art. 24 regelt statistische Erhebungen, Art. 25 sieht ein Feedback-System vor, das den Nutzerinnen und Nutzern die Möglichkeit gibt, unmittelbar nach der Nutzung der mit dem Your Europe-Portal verlinkten Informationen, Verfahren und Unterstützungsdienste anonym zu deren Qualität und Verfügbarkeit Stellung zu nehmen.

14 **(9) Fristen für die Bereitstellung von Online-Diensten.** Bis zum 12.12.2023 waren die genannten Online-Verfahren sowie die Leistungen aus der Richtlinie 2005/36/EG vom 7.9.2005 über die Anerkennung von Berufsqualifikationen, der Dienstleistungsrichtlinie 2006/123/EG, der Richtlinie über Auftragsvergabe 2014/24/EU und der Richtlinie über die Vergabe von Aufträgen durch Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste 2014/25/EU in allen Mitgliedstaaten vollständig digital und mehrsprachig grenzüberschreitend bereitzustellen, Art. 39.

15 **(10) Sanktionen.** Wesentlich für die Bedeutung der SDG-Verordnung ist die Frage, welche Sanktionsmöglichkeiten für den Fall bestehen, dass die Verordnung von EU-Mitgliedstaaten nicht rechtzeitig umgesetzt wird. Neben der europarechtlichen Sanktion eines Vertragsverletzungsverfahrens gemäß Art. 258 AEUV kommt auch die Durchsetzung eines subjektiv-öffentlichen Rechts der Unionsbürgerinnen und Unionsbürger in Betracht. Wenn Art. 6 Abs. 1 SDG-VO jeden Mitgliedstaat (bis Ende 2023) dazu verpflichtet, den Nutzern und Nutzerinnen einen vollständigen Online-Zugang zu allen in Anhang II aufgeführten binnenmarktrelevanten Verfahren zu erstellen und eine Online-Abwicklungsmöglichkeit zu verschaffen, sofern das jeweilige Verfahren in dem betreffenden Mitgliedstaat eingerichtet worden ist, dann spricht dies im Hinblick auf die Binnenmarktrechte und Freizügigkeitsrechte[10] dafür, dass ein unionsrechtlich begründetes und ggfls. gerichtlich durchsetzbares subjektiv-öffentliches Recht[11] auf die elektronische Bereitstellung der in der SDG-VO genannten binnenmarktrelevanten Verwaltungsleistungen verliehen werden soll.[12]

16 **(11) Europäische Datenschutzgrundverordnung[13] und Verordnung 2018/1725.**[14] Eine digitale, effizient arbeitende und nutzerzentrierte öffentliche Verwaltung muss mit einer Fülle von personenbezogenen Daten umgehen, muss sie speichern und behördenübergreifend verarbeiten, etwa um das „Once only"-Prinzip zu realisieren. Die Datenschutz-Grundverordnung (DSGVO) trifft umfangreiche Regelungen für die Verarbeitung dieser Daten. Insbesondere gibt sie vor, dass die Verwaltung die personenbezogenen Daten nur verarbeiten darf, wenn der Bürger/die Bürgerin darin eingewilligt hat bzw. im Einzelfall eine spezielle gesetzliche Ermächtigung vorliegt. Die DSGVO enthält viele Öffnungs- und Konkretisierungsklauseln in den Art. 6 Abs. 2 und Abs. 3 DSGVO sowie Art. 9 Abs. 2 lit. b, h und Abs. 4 DSGVO, die durch die Datenschutzvorschriften des Bundes und der Länder ausgefüllt werden. So kann Deutschland gemäß Art. 6 Abs. 2 spezifischere Bestimmungen treffen, sofern die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt[15] oder wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.[16] Ferner können nationale Regelungen getroffen werden, um Art. 9 Abs. 2 lit. b zu konkretisieren im Hinblick auf die

[10] Erwägr. 4 und 6 sowie in Art. 1 Abs. 1 lit. a SDG-VO.

[11] Zur Bedeutung der subjektiv-öffentlichen Rechte zur Durchsetzung von staatlichen Pflichten siehe Bernhardt Verwaltung & Management 2021, 202.

[12] Peuker DÖV 2022, 275, ebenso Siegel NVwZ 2019, 905, 909.

[13] EU-Verordnung vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1 vom 4.5.2016.

[14] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23.10.2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (Text von Bedeutung für den EWR). ABl-L295/39 vom 21.11.2018.

[15] Solche rechtlichen Verpflichtungen ergeben sich aus unterschiedlichen Gesetzen, etwa § 312i Abs. 1 S. 1 Nr. 3 BGB, § 57a StVZO oder § 257 HGB, § 63a Abs. 3 StVG,

[16] Siehe dazu § 3 BDSG.

Zulässigkeit von Verarbeitungen, die erforderlich sind, damit der Verantwortliche oder Betroffene seine Rechte bzw. Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes ausüben bzw. wahrnehmen kann.[17] Die rechtlichen Regelungen sind im Einzelnen in § 34 des Handbuchs darlegt.

Für die Verarbeitung personenbezogener Daten durch das Handeln der Organe, Einrichtungen und sonstigen Stellen der Europäische Union sieht die Verordnung (EU) 2018/1725 spezifische Regelungen vor, die inhaltlich mit der Datenschutzgrundverordnung und der Richtlinie über den Datenschutz bei der Strafverfolgung korrespondieren. Sie trat am 11.12.2018 in Kraft. **17**

In der praktischen Anwendung hat diese Verordnung Relevanz, wie die Entscheidung des Europäischen Datenschutzbeauftragten (EDSB) vom 11.3.2024 verdeutlicht. So hat der EDSB festgestellt, dass die Kommission gegen mehrere Bestimmungen der Verordnung (EU) 2018/1725 verstoßen hat, insbesondere gegen die Regelungen, die die Übermittlung personenbezogener Daten außerhalb der EU/des Europäischen Wirtschaftsraums (EWR) betreffen. So habe die Kommission nicht in ausreichender Weise sichergestellt, dass die Länder außerhalb der EU/des EWR, an die die personenbezogenen Daten übermittelt werden, über ein im Wesentlichen gleichwertiges Schutzniveau wie in der EU/im EWR verfügen. Darüber hinaus habe die Kommission in ihrem Vertrag mit Microsoft nicht ausreichend die Arten der zu erhebenden Daten und die Zwecke der Nutzung von Microsoft 365 festgelegt. Der EDSB hat daher die Kommission mit Wirkung vom 9. Dezember 2024 aufgefordert, alle Datenströme, die sich aus der Nutzung von Microsoft 365 an Microsoft und an seine verbundenen Unternehmen und Unterauftragsverarbeiter in Ländern außerhalb der EU/des EWR ergeben, die nicht unter einen Angemessenheitsbeschluss fallen, auszusetzen und die Verarbeitungsvorgänge, die sich aus der Verwendung von Microsoft 365 ergeben, mit der Verordnung (EU) 2018/1725 in Einklang zu bringen.[18] **18**

c) Elektronische-Transaktionen-Verordnung (eIDAS-Verordnung).[19] Die eIDAS-Verordnung trat in allen 28 (nun 27) EU-Mitgliedstaaten sowie im Europäischen Wirtschaftsraum am 17.9.2014 in Kraft und ist überwiegend seit dem 1.7.2016 (Art. 52 der Verordnung) unmittelbar anwendbar. Die eIDAS-Verordnung trifft europaweit verbindliche Regelungen für die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel. Folgende Vertrauensdienste sind geregelt: Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, die Zustellung elektronischer Einschreiben, die Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung sowie die Bewahrung der diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten. Die Verordnung führte zur Unanwendbarkeit widersprechenden nationalen Rechts, also auch zur partiellen Unanwendbarkeit von Teilen des deutschen SigG und der SigV. Dies führte teilweise zu erheblichen Rechtsunsicherheiten.[20] So wurde der vor Inkrafttreten der eIDAS-Verordnung vorgeschriebene Einsatz einer Smartcard zur Erzeugung einer qualifizierten elektronischen Signatur in Deutschland unter bestimmten Bedingungen überflüssig, weil auch eine Fernsignatur den Status einer qualifizierten elektronischen Signatur erlangen kann. Gemäß Art. 3 Nr. 11 und 12 iVm Art. 26 eIDAS-Verordnung ist erforderlich, dass sie eindeutig dem Unterzeichner zugeordnet ist, die Identifizierung des Unterzeichners ermöglicht, unter Verwendung elektronischer Signaturerstellungsdaten erstellt wird, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann und die Signatur so mit den auf diese Weise unterzeichneten Daten verbunden ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Die Verantwortung für die optimale Sicherheit wird also auf „Anbieter von **19**

[17] Siehe dazu aus dem deutschen Recht § 67a Abs. 1 S. 2 SGB und § 22 Abs. 1 Nr. 1 lit. a BDSG.

[18] https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en?etrans=de.

[19] Verordnung (EU) Nr. 910/2014 vom 23.7.2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, L 257/73 vom 28.8.2014.

[20] Bernhardt NJW-aktuell H. 20/2016, 17.

qualifizierten Vertrauensdiensten“ übertragen. Alle EU-Mitgliedstaaten sind verpflichtet, die Gültigkeit einer qualifizierten elektronischen Signatur anzuerkennen, sofern sie mit einem qualifizierten Zertifikat aus einem anderen Mitgliedstaat erstellt wurde. Im deutschen Recht führte die eIDAS-Verordnung als neuen Dienst das elektronische Siegel ein. Zwar sind die elektronischen Siegel technisch mit den elektronischen Signaturen vergleichbar, allerdings sind sie nicht einer natürlichen, sondern einer juristischen Person zugeordnet. Auch werden mit der Verwendung des Siegels keine Willenserklärungen abgegeben. Das Siegel dient vielmehr einer Institution als Herkunftsnachweis, vergleichbar mit dem Behördenstempel in der analogen Welt. Ziel der eIDAS-Verordnung ist insbesondere, den Rechtsverkehr auch grenzüberschreitend durch gegenseitige Anerkennung der nationalen Siegel zu erleichtern. Das eIDAS-Durchführungsgesetz[21] regelt u.a die Aufsichtsstellenfunktion der Bundesnetzagentur für die Erstellung, Überprüfung und Validierung elektronischer Signaturen, elektronischer Siegel oder elektronischer Zeitstempel und Dienste für die Zustellung elektronischer Einschreiben und die Bewahrung der elektro-nischen Signaturen, Siegel oder Zertifikate. § 9 legt die Zuständigkeit der Bundesnetzagentur für die Aufstellung, Führung und Veröffentlichung von Vertrauenslisten nach Art. 22 eIDAS-VO fest. § 12 ermöglicht Attribute eines qualifizierten Zertifikats für elektronische Signaturen (zB amts- und berufsbezogene Angaben für Notare oder Rechtsanwälte).

20 **d) EU-Verordnung zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität[22] („eIDAS 2.0“).** Die bisher geltende eIDAS- Verordnung[23] wird den neuen Marktanforderungen nicht gerecht, weil sie ausschließlich auf den öffentlichen Sektor beschränkt ist, die Verknüpfung privater Online-Anbieter mit dem System kompliziert ist und die Möglichkeiten hierfür begrenzt sind. Ferner sind notifizierte eID-Lösungen weiterhin nicht in allen Mitgliedstaaten ausreichend verfügbar und sie sind auch nicht ausreichend flexibel, um eine Vielzahl von Anwendungsfällen abzudecken.[24] Andererseits sind Identitätslösungen, die von Betreibern sozialer Medien und von Finanzinstituten angeboten werden und nicht in den Anwendungsbereich der eIDAS-Verordnung fallen, im Hinblick auf den Schutz der Privatsphäre und Datenschutz bedenklich.

21 Über die neue Verordnung wurde am 8.11.2023 in den Trilogverhandlungen zwischen EU-Kommission, Rat der EU und EU-Parlament eine Einigung erzielt; dabei gibt es allerdings weiterhin datenschutzrechtliche Bedenken, auch wenn es aus dieser Sicht gegenüber dem ursprünglichen Entwurf der EU-Kommission einige Verbesserungen gibt.[25] Die finalen Abstimmungen im Europäischen Parlament und im Rat der Europäischen Union waren für Februar 2024 vorgesehen, somit die Veröffentlichung im Amtsblatt für Ende März. Bei einem Inkrafttreten der Verordnung im April 2024 hätten die Mitgliedstaaten bis Oktober 2026 Zeit, die Wallet bereitzustellen.

22 Die vor dem Abschluss stehende Verordnung[26] sieht vor, dass die Mitgliedstaaten den Bürgerinnen, Bürgern und Unternehmen digitale „Wallets“ („Brieftaschen“) zur Verfügung stellen, in denen sie ihre nationale digitale Identität mit den Nachweisen anderer persönlicher Attribute (zB Führerschein, Abschlusszeugnisse, Geburtsurkunde, Heiratsurkunde, Bankkonto usw.) verknüpfen können. Diese „Brieftaschen“ können von Behörden oder pri-

[21] Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23.7.2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz) vom 18.7.2017, BGBl. I, 2745.

[22] Der endgültige Text der Verordnung ist noch nicht offiziell veröffentlicht worden; das Europäische Parlament hat am 29.2.2024 darüber entschieden. (Stand 29.2.2024).

[23] In der Fassung der Berichtigung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23.7.2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, ABl. L 155 vom 14.6.2016, S. 44–44).

[24] Siehe Begründung zum Vorschlag der Kommission COM(2021) 281 final.

[25] https://netzpolitik.org/2023/eidas-reform-digitale-brieftasche-mit-ausspaehgarantie/.

[26] Siehe zum Inhalt https://www.bundesdruckerei.de/de/innovation-hub/eidas/eidas-2-0, abgerufen am 27.2.2024.

vaten Einrichtungen bereitgestellt werden, sofern sie von einem Mitgliedstaat anerkannt sind. Dank der neuen EUID-Wallet werden Unionsbürgerinnen und Bürger sowie Unternehmen online auf öffentliche und private Dienste zugreifen können, ohne private Identifizierungsmethoden nutzen oder unnötig personenbezogene Daten weitergeben zu müssen. Nach einer einmaligen Identifizierung werden die Daten mit dem Einverständnis der Nutzerin/des Nutzers für die weitere Verwendung etwa bei digitalen Behördengängen wie Adressänderungen oder Steuererklärungen bis hin zur Nutzung von Gesundheitsservices gespeichert.

23 Der Entwurf (Art. 6a Abs. 2 eIDAS-VO neu) sah drei Möglichkeiten für die Ausstellung der EUID-Brieftaschen in den EU-Mitgliedstaaten vor: a) eine mitgliedstaatliche Lösung für Bürgerinnen/Bürger und Unternehmen des Mitgliedstaates, b) die Beauftragung eines privaten Unternehmens zur Entwicklung und Verfügbarmachung durch den Mitgliedstaat oder c) die unabhängige Entwicklung durch Privatunternehmen, aber mithilfe eines staatlich anerkannten Zertifizierungsprogramms. Gemäß Art. 6a Abs. 3 eIDAS- VO- neu müssen EUID-Brieftaschen dem Nutzer ermöglichen: „a) das sichere, für den Nutzer transparente und nachvollziehbare Anfordern und Erhalten, Speichern, Auswählen, Kombinieren und Weitergeben der erforderlichen gesetzlichen Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen, um sich online und offline zur Nutzung öffentlicher und privater Online-Dienste zu authentifizieren; b) das Unterzeichnen mit qualifizierten elektronischen Signaturen. „EUID-Brieftaschen" werden im Rahmen eines notifizierten elektronischen Identifizierungssystems mit dem Sicherheitsniveau „hoch" ausgestellt. Die Verwendung der EUID-Brieftaschen soll für natürliche Personen kostenlos sein. Art. 6a Abs. 7 eIDAS-VO (neu) regelt, dass die Nutzer/Nutzerinnen die uneingeschränkte Kontrolle über die EUID-Brieftasche haben sollen und es dem Aussteller untersagt ist, Informationen über weitergehende (über die eigentliche Funktion hinausgehende) Verwendungen der Brieftasche zu sammeln oder die Personenidentifizierungsdaten mit anderen personenbezogenen Daten zu kombinieren, es sei denn, die Nutzer/Nutzerinnen haben dies ausdrücklich verlangt.

24 **e) EU-Verordnung vom 17.4.2019 über die ENISA.**[27] Die Verordnung beschreibt in Art 1 den Zweck der Verordnung, nämlich das ordnungsgemäße Funktionieren des Binnenmarkts zu gewährleisten und gleichzeitig in der Union ein hohes Niveau in der Cybersicherheit, bei der Fähigkeit zur Abwehr gegen Cyberangriffe und beim Vertrauen in die Cybersicherheit zu erreichen. Dazu legt die Verordnung die Ziele, Aufgaben und organisatorischen Aspekte der ENISA (Agentur der Europäischen Union für Cybersicherheit) fest und setzt einen Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung mit dem Ziel, für IKT- Produkte, -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten und eine Fragmentierung des Binnenmarkts bei Zertifizierungsschemata in der Union zu verhindern. Dabei sollen die Zuständigkeiten der Mitgliedstaaten für die Tätigkeiten für die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich unberührt bleiben.

25 **f) Data Governance Act (DGA).**[28] Die Verordnung, die am 23.6.2022 in Kraft getreten und seit dem 24.9.2023 anwendbar ist, soll den Datenaustausch über verschiedene Branchen sowie über Ländergrenzen hinweg auf der Basis einer sicheren Infrastruktur fördern und mit dem Abbau technischer Hindernisse eine bessere Entwicklung von Künstlicher Intelligenz, Medizin oder Mobilität ermöglichen. Die Verordnung will ein Datenaustauschmodell als Instrument für einen sicheren und souveränen Datenaustausch zwischen Unternehmen, Privatpersonen und der öffentlichen Hand festlegen. Ferner sollen Datenspenden von Bürgern erleichtert und ein besserer Zugang zu Daten der öffentlichen Hand geschaffen

[27] Verordnung(EU) 2019/881 vom 17.4.2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. 2019, L 151/15 vom 7.6.2019.

[28] Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724, ABl. L 152, 3.6.2022, S. 1–44.

werden. Der DGA selbst verweist auf die Datenschutz-Grundverordnung (DSGVO):[29] Insoweit regelt der DGA, dass die Vorschriften der DSGVO unberührt bleiben und Vorrang genießen."[30] Der DGA sieht verschiedene Arten von Datenmittlern vor, die sowohl personenbezogene als auch nicht personenbezogene Daten verarbeiten. Als Datenschutzmaßnahmen nennt Erwägungsgrund 7 „Techniken, die datenschutzfreundliche Analysen ermöglichen, zB Anonymisierung, Pseudonymisierung, differentielle Privatsphäre, Generalisierung oder Datenunterdrückung und Randomisierung "Mit diesen Techniken und mit umfassenden Datenschutzkonzepten soll eine Weiterverwendung personenbezogener Daten und vertraulicher Geschäftsdaten für Forschung, Innovation und statistische Zwecke gewährleistet werden. „Mittler für die gemeinsame Nutzung personenbezogener Daten", sollen Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Datenschutz-Grundverordnung (DSGVO) unterstützen."

26 Datenvermittlungsdienste müssen in einem Register aufgeführt werden müssen, um den Kunden eine Überprüfungmöglichkeit zu geben, ob die Dienstleister vertrauenswürdig sind. Damit neutrale Marktplätze entstehen, sollen Dienstleister, die für den Datenaustausch verantwortlich sind, nicht selbst Daten für eigene Zwecke auswerten dürfen. Insbesondere soll verhindert werden, dass Datenaustauschdienste ihre Dienstleistung mit weiteren Angeboten so verknüpfen, dass daraus unerwünschte Lock-in-Effekte entstehen.[31]

27 **g) Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung)- Data Act.**[32] Mit der am 11.1.2024 in Kraft getretenen und ab 12.9.2025 anzuwendenden Datenverordnung werden die rechtlichen Rahmenbedingungen für den Datenzugang und die Datennutzung festgelegt. Ziel ist es, eine gerechte Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft zu gewährleisten und den Datenzugang und die Datennutzung zu fördern. Sowohl die Privatwirtschaft als auch der öffentliche Sektor erhalten Zugangsrechte zu Daten. Zugleich werden Dateninhabern, Produktherstellern und Cloud-Anbietern erhebliche Pflichten auferlegt. Folgende Kerninhalte sieht die Verordnung vor:

28 aa) Eine Erleichterung des Datenzugangs und der Datennutzung für Verbraucher und Unternehmen, gleichzeitig aber die Sicherung von Anreizen für Investitionen in die Wertschöpfung und die Gewährleistung von Fairness bei Verträgen über gemeinsame Datennutzung;

29 bb) in Fällen außerhalb der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung und außerhalb der Zoll- oder Steuerverwaltung: Das Recht von öffentlichen Stellen, der Kommission, der Europäischen Zentralbank und von EU-Einrichtungen auf Zugang zu Daten des privaten Sektors und zur Nutzung der Daten für spezifische Zwecke von öffentlichem Interesse, wenn dies unter außergewöhnlichen Umständen erforderlich ist. Das betrifft insbesondere öffentlichen Notfälle wie etwa Überschwemmungen und Waldbränden oder gilt zur Erfüllung einer Aufgabe im öffentlichen Interesse. Wann ein öffentlicher Notfall vorliegt, soll von den Mitgliedstaaten oder internationalen Organisationen „nach dem jeweiligen Verfahren" festgestellt werden (Erwgr. 57). Die Situation, in der solche Datennutzungsverlangen gestellt werden können, ist in Art. 15 geregelt. So muss das außergewöhnliche Erfordernis der Nutzung bestimmter Daten befristet und im Umfang begrenzt sein und gilt dann, wenn die verlangten Daten zur Bewältigung eines öffentlichen Notstands (etwa Naturkatastrophen, Pandemien, Terroranschläge) erforderlich sind und öffentlichen Stellen und Einrichtungen diese Daten unter gleichwertigen Be-

[29] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4.5.2016.

[30] Erwägr. 4.

[31] https://www.zeit.de/digital/2021-12/daten-governance-gesetz-eu-einigung, abgerufen am 10.4.2022.

[32] ABl. L, 2023/2854 vom, 22.12.2023.

dingungen auf andere Weise nicht rechtzeitig und wirksam beschaffen können (Art. 15 Abs. 1 Buchst. a). In solchen Fällen haben auch Kleinst- und Kleinunternehmen ihre Daten bereitzustellen und erhalten dafür eine Gegenleistung, während ansonsten die Datenbereitstellung im Wesentlichen unentgeltlich zu erfolgen hat.

■Ein solches Verlangen kann ferner gestellt werden, wenn die öffentliche Stelle oder Einrichtung auf der Grundlage des Unionsrechts oder des nationalen Rechts tätig wird und spezifische Daten ermittelt hat, deren Fehlen sie daran hindert, eine bestimmte im öffentlichen Interesse ausgeübte Aufgabe zu erfüllen. Die Aufgabe muss rechtlich ausdrücklich vorgesehen sein. Als Beispiele nennt die Verordnung die Fälle, dass amtliche Statistiken zu erstellen oder ein öffentlicher Notstand einzudämmen oder zu überwinden sind. Vorher müssen aber alle anderen zur Verfügung stehenden Möglichkeiten ausgeschöpft werden, um solche Daten zu erlangen. Auszuschöpfen ist (sofern es nicht um Statistiken geht) demnach die Möglichkeit eines Erwerbs auf dem Markt zu Markttarifen von nicht-personenbezogenen Daten oder die Inanspruchnahme bestehender Verpflichtungen zur Bereitstellung von Daten oder der Erlass neuer Rechtsvorschriften, die die rechtzeitige Verfügbarkeit der Daten gewährleisten könnten (Art. 15 Abs. 1 Buchst. b). Zur Datenbereitstellung in den letztgenannten Fällen sind Kleinstunterneh-men und Kleinunternehmen nicht verpflichtet (Art. 15 Abs. 2). 30

Art. 17 trifft verschiedene formale Anforderungen an das konkrete Datenbereitstellungsverlangen und sieht eine Beschwerdemöglichkeit vor, wenn der Dateninhaber der Ansicht ist, dass seine Rechte durch die Übermittlung oder Bereitstellung von Daten verletzt wurden. 31

Weitere Regelungen zur Erfüllung der Datenverlangen und die Pflichten der öffentlichen Einrichtung bei der bei der Nutzung der bereitgestellten Daten finden sich in den Art. 18 und 19. In engen Grenzen sieht die Verordnung auch eine Weitergabemöglichkeit der erlangten Daten an Forschungseinrichtungen oder statistische Ämter vor (Art. 21). 32

cc) die Erleichterung des Wechsels von Datenverarbeitungsdiensten (insb. Cloud- und Edge-Anbieter, Art. 23 bis 31). 33

Kunden können beanspruchen, grundsätzlich kostenlos zwischen verschiedenen Datenverarbeitungsdiensten zu wechseln und alle ihre exportierbaren Daten auf einen neuen Dienst zu übertragen (Art. 23 ff.). Dabei sind die Anbieter von Datenverarbeitungsdiensten zur Erleichterung des Wechsels verpflichtet, im Vertrag alle Kategorien von Daten und digitalen Vermögenswerten zu benennen, die im Rahmen eines Wechsels zu einem neuen Anbieter übertragen werden können (Art. 25). Darüber hinaus bestehen Informationspflichten hinsichtlich Wechsel- und Übertragungsmethoden, -formaten und technischen Beschränkungen sowie eines Online-Registers mit Angaben zu den exportierbaren Daten (Art. 26). Es gilt eine maximale Kündigungsfrist für die Einleitung des Wechsels, die zwei Monate nicht überschreiten darf. Der Anbieter von Datenverarbeitungsdiensten hat den Kund beim Wechsel oder der Löschung aller exportierbaren Daten zu unterstützen. Nach einer mindestens 30tägigen weiteren Abrufzeit muss der Anbieter alle exportierbaren Daten des Kunden löschen. Seit dem 11.1.2024 dürfen nur noch ermäßigte Wechselentgelte gefordert werden, ab dem 12.1.2027 wird dann der Wechsel grundsätzlich kostenlos sein.

dd) die Einführung von Schutzvorkehrungen gegen den Zugriff auf Clouddaten durch Regierungen, die nicht zur EU oder zum Europäischen Wirtschaftsraum (EWR) gehören. 34

Mit der Datenverordnung sollen die Möglichkeiten von Cloud-Anbietern eingeschränkt werden, auf Anweisung ausländischer Gerichte oder Behörden Zugang zu den in der EU gespeicherten nicht-personenbezogenen Daten im Besitz von Produktherstellern und produktbezogenen Dienstleistern zu gewähren. Die Cloud-Anbieter sollen zur Vermeidung eines Konflikts mit dem Unionsrecht oder dem nationalen Recht des entsprechenden Mitgliedstaates verpflichtet werden, angemessene technische, rechtliche und organisatorische Maßnahmen zu ergreifen, um die Übermittlung nicht-personenbezogener Daten in das EU-Ausland zu verhindern, sofern der Schutz nicht-personenbezogener Daten nicht dem Schutz gemäß dem EU-Recht entspricht (Art. 32 Abs. 1). Entscheidun-

gen von Verwaltungsbehörden bzw. Urteile eines Gerichts eines Drittlands mit der Aufforderung an Anbieter von Datenverarbeitungsdiensten, nicht-personenbezogene Daten zu übermitteln oder Zugang zu diesen Daten zu gewähren, können nur anerkannt werden bzw. sind nur vollstreckbar, wenn sie auf einer rechtskräftigen internationalen Übereinkunft, etwa auf einem Rechtshilfeabkommen zwischen dem anfragenden Drittland und der Union oder einer solcher Übereinkunft zwischen dem anfragenden Drittland und einem Mitgliedstaat, beruhen (Art. 32 Abs. 2).

35 Wenn kein solches internationale Abkommen besteht und die Befolgung der ausländischen Entscheidung durch den Cloud-Anbieter die Gefahr birgt, dass er gegen EU-Recht oder gegen das nationale Recht der Mitgliedstaaten verstößt, dann können Cloud-Anbieter ausländischen Anordnungen über den Zugang zu in der EU gespeicherten nicht-personenbezogenen Daten nur unter engen Voraussetzungen nachkommen, nämlich

- wenn das Rechtssystem des Drittlands vorschreibt, dass die Entscheidung oder das Urteil zu begründen ist und verhältnismäßig sein muss, und vorsieht, dass die Entscheidung oder das Urteil hinreichend bestimmt ist, etwa im Hinblick auf eine bestimmte verdächtige Person oder Rechtsverletzungen,
- wenn der begründete Einwand des Adressaten von einem zuständigen Gericht des Drittlands überprüft wird und
- wenn das zuständige Gericht des Drittlands in seiner Entscheidung die einschlägigen rechtlichen Interessen des Bereitstellers der durch das Unionsrecht oder das nationale Recht des betreffenden Mitgliedstaats geschützten Daten gebührend berücksichtigen kann.

36 Cloud-Anbieter können die zuständigen EU- Behörden um ihre Meinung dazu bitten, ob die Bedingungen für die Beantwortung eines ausländischen Datenzugangsantrags erfüllt sind. Dies gilt vor allem dann, wenn der Cloud-Anbieter der Ansicht ist, dass die Entscheidung möglicherweise Geschäftsgeheimnisse und andere sensible Geschäftsdaten sowie Inhalte betrifft, die durch Rechte des geistigen Eigentums geschützt sind, oder die Übermittlung eine Re-Identifikation ermöglichen könnte. Sofern der Cloud-Anbieter meint, dass die Entscheidung oder das Urteil die nationale Sicherheit oder die Verteidigungsinteressen der Union oder ihrer Mitgliedstaaten beeinträchtigen könnte, erfragt er eine Stellungnahme der einschlägigen nationalen Stellen oder Behörden dazu, ob die verlangten Daten die nationale Sicherheit oder die Verteidigungsinteressen der Union oder ihrer Mitgliedstaaten betreffen. Hat der Cloudanbieter von den Adressaten der Frage binnen eines Monats keine Antwort erhalten oder gelangt eine solche Stelle oder Behörde in ihrer Stellungnahme zu dem Schluss, dass die in Unterabsatz 1 festgelegten Bedingungen nicht erfüllt sind, so kann der Cloud-Anbieter die Aufforderung zur Übermittlung der Daten oder den Zugang zu den Daten ablehnen. Aber auch wenn es eine Rechtsgrundlage für die Übermittlung der Daten bzw. die Einräumung des Zugangs zu den Daten gibt, dann soll der Cloudanbieter nur ein Mindestmaß an Daten bereitstellen, das auf der Grundlage einer angemessenen Auslegung dieses Verlangens durch den Anbieter oder die einschlägige nationale Stelle oder Behörde als Reaktion auf das Verlangen zulässig ist (§ 32 Abs. 4).

37 Der Cloud-Anbieter ist ferner verpflichtet, den Dateninhaber über die Anfrage zu informieren, bevor er dem Verlangen nachkommt. Ausgenommen von der Mitteilungspflicht sind nur die Fälle, bei denen das Verlangen Strafverfolgungszwecken dient und solange dies zur Wahrung der Wirksamkeit der Strafverfolgungsmaßnahmen erforderlich ist (§ 32 Abs. 5).

38 ee) die Entwicklung von Interoperabilitätsstandards für Daten, die von anderen Sektoren weiterverwendet werden sollen.

Die Datenverordnung regelt auch das Thema Interoperabilität, um Lock-Im-Effekte zu reduzieren. Gemäß Art. 2 Nr. 40 Datenverordnung handelt es sich bei der „Interoperabilität“ um „die Fähigkeit von zwei oder mehr Datenräumen oder Kommunikationsnetzen, Systemen, vernetzten Produkten, Anwendungen, Datenverarbeitungsdiensten oder Komponenten, Daten auszutauschen und zu nutzen, um ihre Funktionen auszuführen.“ Die Pflicht zur Herstellung einer verbesserten Interoperabilität soll dem „Binnenmarkt der Daten“ dienen, also dem erleichterten Austausch und der Nutzung der Daten dienen. Teilnehmer von Datenräumen, bei denen es sich um zweck- oder sektorspezifische oder

sektorübergreifende interoperable Rahmen für gemeinsame Normen und Verfahren für die Weitergabe oder die gemeinsame Verarbeitung von Daten – unter anderem für die Entwicklung neuer Produkte und Dienste, wissenschaftliche Forschung oder Initiativen der Zivilgesellschaft – handelt, müssen grundlegend Anforderungen erfüllen. Dies dient der Erleichterung der Interoperabilität von Daten, von Mechanismen und Diensten für die Datenweitergabe. So sind Datensatzinhalte, Nutzungsbeschränkungen, Lizenzen, Datenerhebungsmethoden, Datenqualität und Unsicherheiten gegebenenfalls in maschinenlesbarem Format – hinreichend zu beschreiben, um dem Empfänger das Auffinden der Daten, den Datenzugang und die Datennutzung zu ermöglichen. Ferner ist vorgesehen, die Datenstrukturen, Datenformate, Vokabulare, Klassifizierungssysteme, Taxonomien und verfügbare Codelisten in einer öffentlich verfügbaren und einheitlichen Weise zu beschreiben und die die technischen Mittel für den Datenzugang (zB Anwendungsprogrammierschnittstellen und die Nutzungsbedingungen) ausreichend zu beschreiben, um automatischen Datenzugang und die automatische Datenübermittlung zu ermöglichen, sofern dies technisch machbar ist und die Funktionsfähigkeit des Produkts nicht beeinträchtigt. Die Kommission soll die Anforderungen durch delegierte Rechtsakte ergänzen und präzisieren dürfen (Art. 33 Abs. 2). Ferner sollen die europäischen Normungsinstitute mit der Ausarbeitung von Normen beauftragt werden (Art. 32 Abs. 4).

Sofern Daten oder Datendienste für andere Teilnehmer an Datenräumen angeboten wer- **39**
den, die ganz oder teilweise den in den Durchführungsrechtsakten festgelegten Spezifikationen entsprechen, gilt eine Konformitätsvermutung mit den wesentlichen Anforderungen (Art. 33 Abs. 8).

Schließlich beschreibt Art. 35 Datenverordnung die Anforderungen an offene Spezifika- **40**
tionen. Bei den „offene Interoperabilitätsspezifikationen" handelt es sich um „eine technische Spezifikation im Bereich der Informations- und Kommunikationstechnologie, die leistungsbezogen darauf ausgerichtet sind, die Interoperabilität zwischen Datenverarbeitungsdiensten herzustellen" (Art. 2 Nr. 41). Auch insoweit wird die Kommission ermächtigt, die europäischen Normungsinstitute mit der Ausarbeitung von Normen für bestimmte Arten von Datenverarbeitungsdiensten zu beauftragen (Art. 35 Abs. 4). Zudem wird die Kommission ermächtigt, in delegierten Rechtsakten gemeinsame Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen festzulegen (Art. 35 Abs 5).

h) Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Ge- 41
setz über Künstliche Intelligenz- KI-Gesetz). aa) Allgemein: Die auch für die Verwaltung bedeutsame Verordnung wurde am 13.3.2024 vom Europäischen Parlament beschlossen.[33] An die zu erwartende endgültige Beschlussfassung durch den Rat wird sich die Verkündung im Amtsblatt anschließen (Stand April 2024).

Die Verordnung tritt am 20. Tag nach ihrer Veröffentlichung im EU-Amtsblatt in Kraft **42**
und wird im Wesentlichen nach 24 Monaten anwendbar, Art. 113, mit Ausnahme der folgenden spezifischen Bestimmungen, die in Art. 113a) bis c) genannt sind.:

Die Regelungen für verbotene KI-Systeme sind bereits nach 6 Monaten anzuwenden, die **43**
Verpflichtungen für sogenannte Foundation Models gelten nach 12 Monaten, Verpflichtungen für KI-Systeme mit hohem Risiko im Sinne von Art. 6 Abs. 1 werden nach 36 Monaten gelten.

Die Verordnung gilt, soweit der der **Anwendungsbereich des EU-Rechts generell eröffnet 44**
ist, also nicht bei mitgliedstaatlichen Zuständigkeiten oder wenn die Bereiche in die Kompetenz anderer, mit entsprechenden Aufgaben betrauter Stellen in Bezug auf die nationale Sicherheit fallen. Das KI-Gesetz enthält Verpflichtungen für Anbieter, Betreiber, Importeure, Händler und Produkthersteller von KI-Systemen, die mit dem EU-Markt verbunden sind. Das KI-Gesetz gilt beispielsweise für Anbieter, die KI-Systeme auf dem EU-Markt in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle für allgemeine Zwecke („GPAI-Modelle") auf dem EU-Markt in Verkehr bringen; (2) Bereitsteller von KI-Systemen, die einen Niederlassungsort in der EU haben bzw. in der EU ansässig sind, sowie für Anbieter und Bereitstel-

[33] https://www.europarl.europa.eu/news/de/press-room/20240308IPR19015/gesetz-uber-kunstliche-intelligenz-parlament-verabschiedet-wegweisende-regeln abgerufen am 2.4.2024.

ler von KI-Systemen in Drittländern, wenn der von einem KI-System erzeugte Output in der EU verwendet wird (Art. 2 Abs. 1 KI-Gesetz). Das KI-Gesetz ist nicht für Systeme mit ausschließlich militärischen oder verteidigungspolitischen Zwecken anwendbar. Schließlich ist die Verordnung auch nicht anzuwenden für KI-Systeme, die ausschließlich für Forschung und Innovation verwendet werden, sowie Personen, die KI aus nichtgewerblichen Gründen nutzen.

45 Der räumliche Anwendungsbereich erstreckt sich gemäß Art. 2 Abs. 1 lit.c dem Marktortprinzip entsprechend auch auf Anbieter von AI aus Drittländern mit einem „Output" in der EU.

46 Die **Definition der Künstlichen Intelligenz** wurde lange diskutiert, da diese von einfachen Softwaresystemen abgegrenzt werden muss. So definiert Art. 3 ein KI-System als „ein maschinengestütztes System, das für einen in wechselndem Maße autonomen Betrieb ausgelegt sind, das nach seiner Einführung anpassungsfähig sein kann und das aus den erhaltenen Eingabe für explizite oder implizite Ziele ableitet, wie Ergebnisse wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen hervorgebracht werden, die physische oder virtuelle Umgebungen beeinflussen können".[34] Diese Definition stimmt weitgehend mit der Definition der OECD überein. Nicht darunter fallen KI-Systeme, die ausschließlich für wissenschaftliche Forschungszwecke entwickelt und in Betrieb genommen werden. Ferner sollen die Regelungen des KI-Gesetzes nicht für auf Open Source basierende Künstliche Intelligenz gelten, sofern es sich um keine verbotenen oder hochriskante KI-Systeme handelt, Art. 2 Abs. 12. Ferner sind vom Anwendungsbereich ausgeschlossen Forschungs-, Test und Entwicklungstätigkeiten vor der Markteinführung bzw. vor der Inbetriebnahme, sofern diese nicht unter realen Bedingungen erfolgt. Eine sogenannte Haushaltsausnahme sieht vor, dass der KI-Einsatz durch natürliche Personen für private Zwecke ohne die sonst im KI-Gesetz vorgesehenen Bedingungen erlaubt ist.

47 Die Mitgliedstaaten können Regelungen beibehalten oder einführen, die die Rechte der Arbeitnehmer bei der Nutzung von KI-Systemen durch Arbeitgeber besser schützen (Art. 2 Abs. 11 KI-Gesetz.

48 Die einzuhaltenden Pflichten richten sich nach der **Risikoklassifizierung** von KI-Systemen. Je höher das Risiko ist, desto strenger ist das einzuhaltende regulatorische Regime. Gemäß Erwägungsgrund 28a ist das Ausmaß der durch das KI-System verursachten negativen Auswirkungen auf die durch die Charta geschützten Grundrechte von besonderer Bedeutung für die Einstufung eines KI-Systems als hochriskant. Bezug genommen wird auf die Grundrechte der EU-Grundrechtecharta, etwa auf die Menschenwürde (Art. 1), die Achtung des Privat- und Familienlebens und den Schutz personenbezogener Daten (Art. 7 und 8), das Diskriminierungsverbot (Art. 21) und die Gleichstellung von Frauen und Männern (Art. 23). Verhindert werden soll eine Beeinträchtigung der Rechte auf freie Meinungsäußerung (Art. 11) und Versammlungsfreiheit (Art. 12). Zu den zu schützenden Rechten zählt der Erwägungsgrund auch das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht, die Unschuldsvermutung und das Verteidigungsrecht.

49 Ein **unannehmbares Risiko** führt zur Konsequenz des Verbots bestimmter Anwendungen bzw. erheblicher Restriktionen (Art. 5 KI-Gesetz). Dazu zählt etwa Social Scoring mithilfe Künstlicher Intelligenz und Emotionserkennung am Arbeitsplatz. Zur biometrischen Fernidentifikation enthält die Verordnung strenge und einschränkende Vorgaben und beugt einer flächendeckenden biometrischen Überwachung vor.

50 Die meisten durch die KI-Verordnung normierten Pflichten knüpfen an sogenannte **Hochrisikosysteme** (Art. 6) an. Als hochriskant eingestufte Systeme können nur dann zugelassen werden, wenn sie die Anforderungen für eine vertrauenswürdige KI erfüllen, die Anbieter eine Risikoeinschätzung und beabsichtigte Schutzmaßnahmen darlegen, wenn sie einen Prüfungsprozess mit Qualitätsmanagement- und Konformitätsbewertungsverfahren (Art. 17) durchlaufen haben, bevor sie auf dem Unionsmarkt in Verkehr gebracht werden können, und die Einrichtung, Durchführung und Aufrechterhaltung eines Systems zur Überwachung

[34] Die hier und im Folgenden verwandten deutschsprachigen Zitate des KI-Gesetzes beruhen auf der Fassung, die dem Europäischen Parlament zur Beschlussfassung vorlag.

nach dem Inverkehrbringen sicherstellen. Anwender von Hochrisiko-KI müssen ein Risikomanagement einrichten sowie hohe Anforderungen an Datenqualität, Dokumentation, Transparenz und technischer Robustheit beachten. Weiters sind grundrechtliche Folgenabschätzungen (Human Rights Impact Assessments) zwingend durchzuführen.

Zu den Hochrisiko-Anwendungen zählen Systeme, die einem der Bereiche des **Anhang III der KI-Verordnung** unterfallen. 51

Generell sollen gemäß Art. 6 Abs. 3 KI-Gesetz die **Anwendungen von der Klassifizierung als Hochrisiko ausgenommen** werden, die kein signifikantes Risiko für die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen haben. Dies ist der Fall, wenn eines oder mehrere der folgenden Kriterien erfüllt sind: Das KI-System ist dazu bestimmt, eine eng begrenzte Verfahrensaufgabe auszuführen, das Ergebnis einer zuvor ausgeführten menschlichen Tätigkeit zu verbessern, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu bestimmt, die zuvor abgeschlossene menschliche Beurteilung zu ersetzen oder zu beeinflussen, ohne dass eine ordnungsgemäße menschliche Überprüfung stattfindet. Eine Ausnahme kommt auch in Betracht, wenn das KI-System eine vorbereitende Aufgabe, für die in Anhang III aufgeführten Hochrisiko-Systeme wahrnehmen. 52

Kommt ein Anbieter zu der Auffassung, dass ein KI-System nach Anhang III kein hohes Risiko darstellt, muss er seine Einschätzung dokumentieren, bevor das System in Verkehr gebracht oder in Betrieb genommen wird, und muss das KI-System registrieren. Auf Verlangen der zuständigen nationalen Behörden muss Anbieter die Dokumentation der Bewertung vorlegen. 53

Um die Anwendung der Ausnahmeregelungen zu erleichtern, sieht Art. 6 Abs. 5 vor, dass die Kommission nach Anhörung des KI-Ausschusses spätestens 18 Monate nach Inkrafttreten der Verordnung **Leitlinien für die praktische Umsetzung** mit einer umfassenden Liste praktischer Beispiele für risikoreiche und nicht risikoreiche Anwendungsfälle von KI-Systemen vor. Ferner sieht Art. 6 Abs. 6 Ermächtigungen für delegierte Rechtsakte für die Änderung der Ausnahmekriterien vor. Die Änderungen dürfen jedoch das Gesamtniveau des Schutzes der Gesundheit, der Sicherheit und der Grundrechte in der Union nicht verringern. Im Einzelnen werden die in der Verwaltung für den Einsatz vorgesehenen KI-Systeme genau daraufhin zu prüfen sein, ob sie der Hochrisikoklasse zuzuordnen sind. Ein die Verwaltung unterstützendes IT-System, das bereits dem Begriff der künstlichen Intelligenz der KI-Verordnung nicht zuzurechnen sind, etwa weil es in keiner Weise autonom arbeitet, wäre nicht von dem KI-Gesetz erfasst. 54

Kapitel V enthält Sonderregelungen für KI-Modelle mit allgemeinem Verwendungszweck (sogenannte **General Purpose AI Models oder DPAI-Modelle**), Art. 51 ff. Ein „KI-Modell mit allgemeinem Verwendungszweck" ist gemäß Art. 3 Abs. 63 des KI-Gesetzes ein Modell, „das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrer Markteinführung für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen verwendet werden." 55

Hier gelten besondere Pflichten, wobei gemäß den Art. 51 ff. zwischen **einfachen GPAI-Modellen** und solchen mit **systemischem Risiko** (also einer Rechenleistung für das KI-Training mit mehr als 10^25 FLOPS) zu unterscheiden ist (Art 51 Abs. 1). So gelten für alle Anbieter von GPAI die folgenden Pflichten: 56

GPAI-Modelle müssen die Wirkung des KI-Systems in einem maschinenlesbaren Format und wirksam, interoperabel, robust und zuverlässig als solchen kennzeichnen und als künstlich erzeugt oder verändert markieren. 57

Bei einfachen Modellen müssen insbesondere Training, das Testen und der Evaluierungsprozess dokumentiert, Informationspflichten erfüllt, Urheberrechte gewahrt und eine Zusammenfassung der Trainingsinhalte veröffentlicht werden. Bei GPAI- Modellen mit systemischem Risiko müssen zusätzlich die potenziellen Risiken bewertet und verringert, 58

besondere Vorfälle gemeldet und ein ausreichendes Niveau an Cyber-Sicherheit gewährleistet werden.

59 Der **Einsatz von KI-Systemen mit hohem Risiko** bedarf gemäß Art. 14 stets einer **wirksamen „menschlichen Aufsicht".** Verwaltungsmitarbeiter dürfen sich also nicht auf den von einem KI-System mit hohem Risiko erzeugten Output zu verlassen bzw. müssen sich der Gefahren einer „automation bias" (die Neigung von Menschen, Vorschläge von automatisierten Entscheidungssystemen zu bevorzugen), insbesondere wenn KI dazu verwendet wird, Informationen oder Empfehlungen für Entscheidungen zu liefern. „Menschliche Aufsicht" bedeutet, dass „der Nutzer keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange dies nicht von mindestens zwei natürlichen Personen überprüft und bestätigt wurde" (Art. 14 Abs. 5). Der Verwaltungsangehörige als „Mensch" muss insoweit in der Lage sein, das AI-System für hohe Risiken nicht zu verwenden oder die Ergebnisse des AI-Systems für hohe Risiken anderweitig zu ignorieren, außer Kraft zu setzen oder umzukehren.

60 Die Mitgliedsstaaten müssen: (1) mindestens eine notifizierende Behörde und eine Marktüberwachungsbehörde benennen; und (2) der Kommission die Identität der zuständigen Behörden und des einheitlichen Ansprechpartners mitteilen. Außerdem müssen sie Informationen darüber veröffentlichen, wie die zuständigen Behörden und die zentrale Kontaktstelle ab 12 Monaten nach Inkrafttreten kontaktiert werden können.

61 Die Verordnung sieht bei einem Verstoß gegen die Auflagen für verbotene KI-Systeme Geldbußen von bis zu 35 Mio. € oder von bis zu 7 % des gesamten weltweiten Jahresumsatzes, bei Missachtung der Auflagen an Hochrisikosysteme Geldbußen von bis zu 15 Mio. € oder von bis zu 3 % des gesamten weltweiten Jahresumsatzes vor, was über den Rahmen der DSGVO hinausgeht. Unrichtige, unvollständige oder irreführende Auskünfte an zuständige nationale Behörden können zu Geldbußen von bis zu 7,5 Mio. € oder bis zu 1 % des gesamten weltweiten Jahresumsatzes führen.

62 **bb**) Auswirkungen auf die **Verwaltung:** Erwägungsgrund 34 führt an, dass es im Hinblick auf die **Verwaltung** und den Betrieb kritischer Infrastrukturen angebracht sei, die in Anhang I Nummer 8 der Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen, den Straßenverkehr und die Wasser-, Gas-, Wärme- und Stromversorgung aufgeführten KI-Systeme, die als Sicherheitskomponenten bei der Verwaltung und dem Betrieb kritischer digitaler Infrastrukturen eingesetzt werden sollen, als **mit hohem Risiko behaftet einzustufen,** da ihr Ausfall oder ihre Fehlfunktion das Leben und die Gesundheit von Personen in großem Umfang gefährden und zu spürbaren Störungen des normalen Ablaufs sozialer und wirtschaftlicher Tätigkeiten führen kann.

63 Erwägungsgrund 36 stellt klar, dass KI-Systeme, die eingesetzt werden im **Bereich der Beschäftigung von Arbeitnehmern** insbesondere für die Einstellung und Auswahl von Personen, für Entscheidungen, die sich auf die Bedingungen des Arbeitsverhältnisses auswirken, für die Beförderung und Beendigung von arbeitsbezogenen Vertragsverhältnissen, für die Zuweisung von Aufgaben auf der Grundlage von individuellem Verhalten, persönlichen Eigenschaften oder Merkmalen und für die Überwachung oder Bewertung von Personen in arbeitsbezogenen Vertragsverhältnissen, der hohen Risikoklasse zuzuordnen sind, da diese Systeme sich spürbar auf die künftigen Berufsaussichten, den Lebensunterhalt dieser Personen und die Rechte der Arbeitnehmer auswirken können.

64 Erwägungsgrund 37 erwähnt die **Verwaltungen** ua im Bereich der Gesundheitsdienste, sozialen Sicherheit, Sozialdienste, Sozial- und Wohnbeihilfen. Werden KI-Systeme verwendet, um zu entscheiden, ob solche Leistungen und Dienste von den Behörden gewährt, verweigert, gekürzt, widerrufen oder zurückgefordert werden sollten einschließlich der Frage des Rechtsanspruchs der Leistungsempfänger, können diese Systeme erhebliche Auswirkungen auf die Lebensgrundlage der Personen haben und ihre Grundrechte wie das Recht auf sozialen Schutz, Nichtdiskriminierung, Menschenwürde oder einen wirksamen Rechtsbehelf verletzen. Deshalb sollten entsprechende Systeme **als hochriskant** eingestuft werden. Einschränkend wird jedoch erklärt: „Dennoch sollte diese Verordnung die Entwicklung und den Einsatz innovativer Ansätze in der öffentlichen Verwaltung nicht behindern, die von ei-

nem breiteren Einsatz regelkonformer und sicherer KI-Systeme profitieren würde, sofern diese Systeme kein hohes Risiko für juristische und natürliche Personen mit sich bringen".

65 Erwägungsgrund 38 **nimmt bestimmte Verwaltungen aus der Risikoklasse aus:** KI-Systeme, die speziell für **Verwaltungsverfahren von Steuer- und Zollbehörden** sowie von **Finanzermittlungsstellen, die Verwaltungsaufgaben wahrnehmen** und Informationen gemäß den Unionsvorschriften zur Bekämpfung der Geldwäsche analysieren, eingesetzt werden sollen.

66 Gemäß Erwägungsgrund 39 sollen KI-Systeme, die dazu bestimmt sind, von oder im Namen von **zuständigen Behörden oder von Agenturen, Ämtern oder Einrichtungen der Union,** die **mit Aufgaben in den Bereichen Migrations-, Asyl- und Grenzkontrollmanagement** betraut sind, als Lügendetektoren und ähnliche Instrumente zur **Bewertung bestimmter Risiken,** die von natürlichen Personen ausgehen, die in das Hoheitsgebiet eines Mitgliedstaats einreisen oder einen Visum- oder Asylantrag stellen, sowie zur Unterstützung der zuständigen Behörden bei der Prüfung, einschließlich der damit zusammenhängenden Bewertung, folgender Aspekte eingesetzt zu werden, als mit hohem Risiko behaftet eingestuft werden.

67 Im Regelungstext – nämlich in Anhang III – werden Verwaltungsbereiche genannt, die der Hochrisikoklasse zuzurechnen sind. Das betrifft

- KI-Systeme, die bestimmungsgemäß als Sicherheitskomponenten im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs sowie der Wasser-, Gas-, Wärme- und Stromversorgung verwendet werden sollen (Nr. 2);
- bestimmte KI-Systeme zum Zugang zu Einrichtungen der allgemeinen und beruflichen Bildung, Bewertung von Leistungen und Bekämpfung von Manipulationen in der Prüfung bzw. KI für bestimmte Entscheidungen innerhalb des Arbeitsverhältnisses (Nr. 3);
- KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen (auch in der Verwaltung) verwendet werden sollen (Nr. 4);
- KI-Systeme zur Zugänglichkeit und Inanspruchnahme grundlegender öffentlicher Dienste und Leistungen und KI-Systeme zur Bewertung und Klassifizierung von Notrufen von natürlichen Personen oder für die Entsendung oder Priorisierung des Einsatzes von Not- und Rettungsdiensten, einschließlich Polizei, Feuerwehr und medizinischer Nothilfe (Nr. 5);
- bestimmte KI-Systeme zur Unterstützung der Strafverfolgung durch die Polizei (Nr. 6)
- KI-Systeme im Hinblick auf Migration, Asyl und Grenzkontrolle, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist (mit Ausnahme der Überprüfung von Reisedokumenten).

3. EU-Richtlinien

68 Richtlinien geben den EU-Ländern ein bestimmtes Ziel vor, stellen ihnen jedoch frei, wie sie dieses verwirklichen. Die Länder müssen die zum Erreichen der Zielvorgabe erforderlichen gesetzlichen Maßnahmen treffen, also in nationales Recht innerhalb der von der Richtlinie bestimmten Frist „umsetzen". Bei Nichtumsetzung einer Richtlinie innerhalb der vorgegebenen Frist, kann die Kommission Vertragsverletzungsverfahren einleiten.

69 **a) Die Richtlinie 2006/123/EG vom 12.12.2006 über Dienstleistungen im Binnenmarkt.**[35] Gemäß Art. 8 Abs. 1 der Richtlinie mussten die Mitgliedstaaten für die von ihrem Anwendungsbereich erfassten Sachbereiche sicherstellen, „dass alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch […] abgewickelt werden können." Die Richtlinie trat am 28.12.2006 in Kraft. Bis spätestens zum 28.12.2009 mussten alle EU-Mitgliedstaaten die Vorgaben in nationales Recht umsetzen. Unter anderem mussten die Mitgliedstaaten folgende, für das E-Government wesentliche Maßnahmen treffen: Die in der Richtlinie definierten EU-Dienstleister sollten in jedem Land eine feste Anlaufstelle erhalten, über die alle nötigen Schritte für die Niederlassung im jeweiligen Land abgewickelt werden können

[35] ABl. 2016, L 376/36.

(„einheitlicher Ansprechpartner").[36] Dies löste in Deutschland erhebliche organisatorische Fragen aus. [37]Ferner sollten alle Verfahren, die für die Ausübung einer Dienstleistung befolgt werden müssen, elektronisch und standortunabhängig abgewickelt werden können. Einheitliche Ansprechpartner und Behörden mussten die hierfür nötige IT-Infrastruktur bereitstellen. Die Richtlinie wurde in Deutschland mit § 71e VwVfG und den korrespondierenden Regelungen im Fachrecht umgesetzt.

70 **b) EU-Richtlinie vom 16.4.2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen.** Die Richtlinie sollte für eine größere Verbreitung der elektronischen Rechnungsstellung (E-Invoicing) unter Auftragnehmern sorgen, die Leistungen für den öffentlichen Sektor erbringen oder Waren an den öffentlichen Sektor liefern. Ziel war, auf das Fehlen der Interoperabilität bzw. auf inkompatible E-Invoicing-Systeme für erbrachte Leistungen bzw. gelieferte Waren in den EU-Mitgliedstaaten zu reagieren, wenn der öffentliche Auftraggeber sich in einem anderen EU-Land befand als das beauftragte Unternehmen. Betroffen sind Rechnungen, die in den Anwendungsbereich der Richtlinien zu öffentlichen Aufträgen fallen, allerdings nicht für Aufträge im Anwendungsbereich der Richtlinie 2009/81/EG (Bereiche Verteidigung und Sicherheit). Gemäß der Verpflichtung aus der Richtlinie veröffentlichte die Europäische Kommission die europäische Norm für die elektronische Rechnungsstellung und die Liste von Syntaxen am 17.10.2017[38] und setzte damit die Verpflichtung offiziell in Kraft, wonach alle öffentlichen Auftraggeber EU-weit nun dieser Norm entsprechend elektronische Rechnungen entgegenzunehmen und zu verarbeiten hatten.

71 **c) NIS-Richtlinie.**[39] Die erste Fassung der Richtlinie trat im August 2016 in Kraft. Sie definiert Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU. Sie schafft einen einheitlichen Rechtsrahmen für den Aufbau nationaler Kapazitäten für die Cybersicherheit, verpflichtet zu einer stärkeren Zusammenarbeit der EU- Mitgliedstaaten und setzt Mindestsicherheitsanforderungen und Meldepflichten für Kritische Infrastrukturen sowie für bestimmte Anbieter digitaler Dienste wie Cloud-Services und Online-Marktplätze fest. Im Einzelnen verpflichtet Art. 7 zur Ausarbeitung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen mit entsprechenden Prioritäten. Sie fordert einen Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen Strategie einschließlich der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure. Sie verpflichtet zu Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor. Ferner verpflichtet sie zur Aufstellung von Ausbildungs-, Aufklärungs- und Schulungsprogrammen, Forschungs- und Entwicklungsplänen sowie eines Risikobewertungsplans zur Bestimmung von Risiken. Ua verpflichtet Art. 8 zur Benennung national zuständiger Behörden und zur Festlegung der Aufgaben, Art. 9 zur Schaffung von Computer-Notfallteams (CSIRTs) sowie zur entsprechender Aufgabenfestlegung.

72 Die Richtlinie war bis Mai 2018 in den EU-Mitgliedstaaten in nationales Recht umzusetzen. In Deutschland war bereits zuvor im Juli 2015 das IT-Sicherheitsgesetz[40] in Kraft getreten, also zu einer Zeit, als einige Inhalte der bevorstehenden NIS-Richtlinie bereits absehbar waren und somit in das nationale Gesetz einfließen konnten. Das am 29.6.2017 verkündete NIS-Umsetzungsgesetz erweiterte ua die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber den KRITIS-Betreibern zur Wiederherstellung der Sicherheit oder Funktionsfä-

[36] Dazu näher: Windoffer NVwZ 2007, 495.

[37] Schulz DÖV 2008, 1028.

[38] Durchführungsbeschluss (EU) 2017/1870 der Kommission vom 16.10.2017 über die Veröffentlichung der Fundstelle der europäischen Norm für die elektronische Rechnungsstellung und die Liste von Syntaxen gemäß der Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates ABl 2017, L 266/.

[39] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. 2016, L 194/1.

[40] G. v. 17.7.2015 BGBl. I S. 1324 (Nr. 31); zuletzt geändert durch Artikel 6 Abs. 2 G. v. 18.5.2021 BGBl. I S. 1122.

higkeit informationstechnischer Systeme in herausgehobenen Fällen, § 5a BSIG. Ferner schuf es Regelungen zu besonderen Anforderungen an Anbieter Digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen, Cloud-Computing-,Dienste), § 8c BSIG.

73 Allerdings zeigte sich, dass die nationalen Umsetzungen sehr unterschiedlich waren. Vergleichbare Unternehmen wurden in einem Teil der EU-Mitgliedstaaten als kritische Dienste oder Betreiber gewertet, in anderen nicht.[41]

74 Die **NIS-2-Richtlinie** („The Network and Information Security (NIS) Directive")[42] ersetzt die Richtlinie (EU) 2016/1148 zur Netzwerk- und Informationssicherheit zum 18.10.2024, schafft Klarheit in der Geltungsweise für kritische Dienste und für die von diesen zu erfüllenden Anforderungen und erweitert die Regelungen zur Cyber- und Informationssicherheit von Unternehmen und Institutionen. Die NIS-2-Richtlinie verpflichtet die Unternehmen zur Verbesserung ihrer Maßnahmen zum Schutz vor Cyberangriffen und zur Etablierung strengerer Sicherheitsstandards und ihre IT-Systeme stets auf dem neuesten Stand zu halte. Die NIS-2 Richtlinie geht weit über die bisher einbezogenen Schlüsselunternehmen im Bereich der kritischen Infrastrukturen hinaus. Es wird nun unterschieden zwischen „wesentlichen Einrichtungen" und „wichtigen Einrichtungen". Als **wesentliche** Einrichtungen (Essential Entities) gelten Unternehmen mit über 249 Beschäftigten oder 50 Mio. EUR Umsatz und über 43 Mio. EUR Bilanz, in folgenden Bereichen (aufgeführt in Anhang I) Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten (Business-to-Business), öffentliche Verwaltung und Weltraum.

75 Zu den **wichtigen Einrichtungen** (Important Entities) werden Unternehmen ab 50 Mitarbeitern oder mit mindestens 10 Mio. EUR Jahresumsatz folgender Bereiche gezählt (Anhang II): Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/Herstellung von Waren, Anbieter digitaler Dienste (zB Online-Marktplätze, Suchmaschinen, soziale Netzwerke); Forschungseinrichtungen.

76 Bis Oktober 2024 müssen die EU-Mitgliedsstaaten diese in nationales Recht umsetzen.[43] Seit Juli 2023 gibt es in Deutschland einen Referentenentwurf des Bundesinnenministeriums für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)[44] sowie seit Oktober 2023 ein „Diskussionspapier des Bundesministeriums des Innern und für Heimat zu den wirtschaftsbezogenen Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland vom 29.9.2023 in Deutschland."[45]

77 **d) PSI-Richtlinie.** Die PSI-Richtlinie[46] trat im Juni 2019 in Kraft. Die Umsetzungsfrist von zwei Jahren endete am 17.7.2021. Ziel ist es, die Weiterverwendung der Daten des öffentlichen Sektors fördern. Mit der (neuen) PSI-Richtlinie wurde die ursprüngliche Richtlinie aus dem Jahr 2013[47] umfangreich überarbeitet. Der Anwendungsbereich wurde auf öffentliche Unternehmen und öffentlich finanzierte Forschungsdaten ausgedehnt, die über ein institutionelles oder thematisches Archiv zugänglich gemacht werden. Die Richtlinie verpflichtet die Mitgliedstaaten dazu, alle vorhandenen Dokumente weiterverwendbar zu machen, es sei denn, der Zugang ist im Rahmen der nationalen Vorschriften über den Zugang zu Doku-

[41] So lag die Zahl der kritischen Dienste in den EUI-Mitgliedstaaten zwischen 12 und 87, die der Betreiber zwischen 20 und 10.897, siehe dazu: Haufe Online Redaktion vom 27.9.2023, https://www.haufe.de/compliance/recht-politik/nis-2-richtlinie-muss-bis-oktober-2024-umgesetzt-werden_230132_606072.html.

[42] Richtlinie(EU) 2022/2555 vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl L 333/80 vom 27.12.2022, ist am 16.1.2023 in Kraft getreten.

[43] Art. 41 Abs. 1 NIS-2-Richtlinie.

[44] https://intrapol.org/wp-content/uploads/2023/05/NIS2UmsuCG.pdf, abgerufen am 29.2.2024.

[45] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/diskussionspapier-NIS-2-umsetzung.html, abgerufen am 29.2.2024.

[46] Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20.6.2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors.

[47] Richtlinie 2013/37/EU vom 26.6.2013 zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors.

menten eingeschränkt oder ausgeschlossen oder unterliegt den anderen in dieser Richtlinie niedergelegten Ausnahmen. Die neue Richtlinie bezieht die kommunalen Unternehmen in den Wirkungsbereich ein. Sogenannte „hochwertige Datensätze" (High Value Datasets) werden bestimmt, deren Weiterverwendung wichtig für die Gesellschaft, die Umwelt und die Wirtschaft ist, insbesondere aufgrund ihrer Eignung für die Schaffung von Mehrwertdiensten, Anwendungen und neuen, hochwertigen und menschenwürdigen Arbeitsplätzen, sowie aufgrund der Zahl der potenziellen Nutznießer der Mehrwertdienste und -anwendungen auf der Grundlage dieser Datensätze. Bis 2022 sollen hochwertige Datensätze in den Kategorien Georaum, Erdbeobachtung und Umwelt, Meteorologie, Statistik, Unternehmen und Eigentümerschaft von Unternehmen sowie Mobilität im EU-Ausschuss für offene Daten definiert und die Weiterverwendung von Informationen des öffentlichen Sektors (Open Data Committee) bestimmt werden (vgl. Anhang I der EU-Richtlinie). Diese müssen zukünftig kostenfrei und maschinenlesbar (aufbereitet und in bestimmten Formaten) über Programmierschnittstellen (APIs) verfügbar gemacht werden. Generell werden Obergrenzen für Gebühren und der Grenzkostenansatz festgelegt – mit nur wenigen Ausnahmen. Die Datensätze sollen vereinbar sein mit bestehenden Rechtsakten, wie etwa mit der Richtlinie über die Einführung intelligenter Verkehrssysteme (IVS-Richtlinie 2010/40/EU[48]) oder mit der Richtlinie zur Schaffung einer Geodateninfrastruktur (INSPIRE Richtlinie 2007/2/EG[49]). Die Verwendung von Standardlizenzen wird geregelt. Vermieden werden sollen Ausschließlichkeitsvereinbarungen des öffentlichen Sektors mit Wirtschaftsakteuren.

4. Europäisches E-Government in der Praxis

78 **a) E-Government-Aktionsplan.** Die tatsächlichen Aktivitäten auf europäischer Ebene basierten in der Vergangenheit vor allem auf dem E-Government-Plänen wie dem **E-Government-Aktionsplan 2016–2020,** der für einen Fünfjahreszeitraum verabschiedet wurde, auf Kooperationsmechanismen von Kommission und EU-Mitgliedstaaten setzte[50] und in entsprechenden Kooperationsgremien von Vertretern der Mitgliedstaaten mit dem Ziel effektiver Umsetzungsmaßnahmen erörtert wurden.[51] Dieser Aktionsplan setzte vor allem auf folgende „Ziele und Grundsätze":[52]

- **Standardmäßig digital** („digital by default"): Vorzugsweise Erbringung von Verwaltungsdienstleistungen in digitaler und maschinenlesbarer Form
- **Once-Only-Prinzip** („once only principle"): Bürgerinnen und Bürger sowie die Unternehmen sollen den Verwaltungen dieselben Informationen nur einmal übermitteln müssen; automatischer Austausch von Daten zwischen den Behörden, soweit hierzu die datenschutzrechtlich erforderliche Einwilligung der Betroffenen vorliegt.
- **Inklusion und Barrierefreiheit:** Einbeziehung verschiedener Bedürfnisse auch der Menschen mit Behinderungen und der älteren Bürgerinnen und Bürger
- **Offenheit und Transparenz:** Bürgerinnen, Bürger sowie Unternehmen sollen Zugang zu ihren Daten erhalten, auch zum Stand ihres Verwaltungsverfahrens

[48] Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7.7.2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern, ABl. 2010 L 207/1.

[49] Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14.3.2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE). ABl. 2007 L 108/1.

[50] S. o. Fn. 2.

[51] Der E-Government Aktionsplan diente vor allem als politisches Instrument zur Beschleunigung der Verwaltungsmodernisierung in der EU, zur Beseitigung von Barrieren für den digitalen Binnenmarkt und Verhinderung weiterer Fragmentierungen der öffentlichen Verwaltungen in Europa. Folgende Schwerpunkte für die Jahre bis 2020 werden darin aufgeführt: Modernisierung der öffentlichen Verwaltung mit Hilfe der IKT auf der Basis zentraler digitaler Grundlagentechnologien (Maßnahmen 1–6); grenzübergreifende Mobilität dank interoperabler digitaler öffentlicher Dienste (Maßnahmen 7–17) und Vereinfachung der digitalen Interaktion zwischen Behörden und Bürger oder Unternehmen mit dem Ziel hochwertiger öffentlicher Dienste (Maßnahmen 18–20).

[52] Mitteilung der Kommission vom 19.4.2016, COM(2016) 179 final.

- **Standardmäßig grenzübergreifend („cross-border by default"):** Öffentliche Verwaltungen sollten einschlägige digitale öffentliche Dienste grenzübergreifend anbieten und eine weitere Fragmentierung verhindern, um die Mobilität im Binnenmarkt zu erleichtern.
- **Standardmäßig interoperabel („interoperability by default")** Öffentliche Dienste sollten so konzipiert sein, dass sie nahtlos im gesamten Binnenmarkt und über organisatorische Grenzen hinweg erbracht werden können. Ferner ist ein freier Austausch von Daten und digitalen Dienstleistungen in der EU zu gewährleisten.[53]
- **Vertrauenswürdigkeit und Sicherheit.** Bereits in der Konzeptphase sollte der Schutz der personenbezogenen Daten, der Privatsphäre und der IT-Sicherheit berücksichtigt werden.

b) Digitaler Kompass 2030. Ein erheblich breiterer Ansatz der Digitalisierungspolitik der EU-Kommission für die Zukunft lässt sich der Mitteilung mit dem Titel „Digitaler Kompass 2030- Der Europäische Weg in die digitale Dekade" vom 9.3.2021 entnehmen. Darin formulierte die Kommission die Zielvorstellung und die Wege für den digitalen Wandel in Europa bis 2030. Die Kommission diagnostizierte zunächst eine starke Beschleunigung der Digitalisierung aufgrund der Pandemie. Es seien gerade in dieser Phase auch Schwächen deutlich geworden, nämlich die Abhängigkeit von außereuropäischen Technologieunternehmen oder die daraus folgende Desinformation mit nachteiligen Konsequenzen für die demokratische Gesellschaft. Es entstehe auch eine neue digitale Kluft bei den Bürgerinnen und Bürgern sowie den Unternehmen. Die Digitalisierung sei geeignet, neue Wohlstandsquellen zu erschließen. Sie trage zu klimaneutralerer Wirtschaft bei. So ermöglichten etwa Videokonferenzen einen Verzicht auf klimaschädliche Dienstreisen. Nötig seien massive Aufstockung von Investitionen mit EU-Mitteln, um die EU im Weltvergleich zu stärken. Die Kommission schlägt einen digitalen Kompass vor, um die Digitalziele der EU für 2030 in konkrete Zielsetzungen umzusetzen und dafür zu sorgen, dass diese auch erreicht werden. Dem Kompass wird ein erweitertes Überwachungssystem zugrunde liegen, um den Kurs der EU im Hinblick auf das Tempo des digitalen Wandels, bei der Überwindung der bestehenden Lücken bei den strategischen digitalen Kapazitäten Europas und bei der Anwendung der Digitalgrundsätze verfolgen zu können. Er wird auch die Mittel zur Verwirklichung der Zielvorstellung und wichtige Meilensteine benennen, die auf vier Kernpunkte ausgerichtet sind. Neben den Zielfaktoren „digital befähigte Bürgerinnen und Bürger und hoch qualifizierte digitale Fachkräfte, „sichere, leistungsfähige und tragfähige digitale Infrastrukturen", „digitaler Umbau der Unternehmen" wird das Ziel der Digitalisierung öffentlicher Dienste besonders betont. Dabei strebt die Kommission an, bis 2030 alle wesentlichen öffentlichen Dienste barrierefrei online verfügbar zu machen, hohe Sicherheits- und Datenschutzstandards einzuhalten und die Möglichkeit der elektronischen Stimmabgabe zur Beteiligung der Öffentlichkeit am demokratischen Leben zu schaffen. Behörden sollen als Online- Plattform mit einfachem Zugang zu öffentlichen Diensten unter Verwendung künstlicher Intelligenz und virtueller Realität auftreten. Datenplattformen der Städte und Gemeinden sollen über verschiedene Sektoren und Städte hinweg geschaffen und die Entwicklung von „intelligenten Dörfern" gefördert werden. Zwischen allen öffentlichen Diensten auf allen Verwaltungsebenen soll Interoperabilität geschaffen werden. Die Nutzung der elektronischen Identität soll für Online-Interaktionen und Online-Präsenz unter Kontrolle der Nutzer und Beachtung der Privatsphäre gefördert werden. Zur Erreichung der Ziele der digitalen Dekade bis 2030 schlägt die Kommission die Schaffung eines Governance-Rahmens vor. Die Kommission werde demgemäß zunächst mit den Mitgliedstaaten gemeinsame EU-Zielpfade für jedes Ziel abstecken. Die Mitgliedstaaten würden dann ihrerseits nationale strategische Fahrpläne zur Erreichung dieser Ziele vorschlagen. 79

Der Kooperationsmechanismus sieht vor: 80

[53] Hierzu dient auch der Europäische Interoperabilitätsrahmen (EIF), Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschaft- und Sozialausschuss und den Ausschuss der Regionen, Europäischer Interoperabilitätsrahmen – Umsetzungsstrategie, COM/2017/0134 final. Siehe dazu auch die Pressemitteilung der EU-Kommission vom 23.3.2017zu den neuen Leitlinien für digitale öffentliche Dienste EuZW 2017, 364.

- ein strukturiertes, transparentes und gemeinsames Überwachungssystem auf der Grundlage des Indexes für die digitale Wirtschaft und Gesellschaft (DESI) zur Messung der Fortschritte bei der Verwirklichung der einzelnen Ziele für 2030;
- einen jährlichen „Bericht über den Stand der digitalen Dekade", in dem die Kommission die Fortschritte bewertet und Empfehlungen für Maßnahmen ausspricht;
- mehrjährige strategische Fahrpläne für die digitale Dekade, in denen die Mitgliedstaaten ihre beschlossenen oder geplanten Strategien und Maßnahmen zur Verwirklichung der Ziele für 2030 darlegen;
- einen strukturierten Rahmen, in dem unzureichende Fortschritte erörtert und durch gemeinsame Zusagen der Kommission und der Mitgliedstaaten in Angriff genommen werden können;
- einen Mechanismus zur Unterstützung von Mehrländerprojekten.

81 **c) Benchmarking als Instrument zur Förderung von eGovernment in der EU.** Die sogenannten Benchmark-Studien enthalten vergleichende Analysen des Entwicklungsstands von E-Government in den Mitgliedstaaten. Sie vergleichen die Performance der mitgliedstaatlichen Verwaltungen beim Stand der Digitalisierung, identifizieren Best-Practice-Beispiele und erhöhen den Druck auf die mitgliedstaatlichen Regierungen und Verwaltungen, im Wettbewerb mit den europäischen die Verwaltungsdigitalisierung voranzutreiben.[54]

82 **d) eGovernment Benchmark Report.** Seit 2001 lässt die EU-Kommission den eGovernment Benchmark Report erstellen. Dieser vergleicht die Fortschritte bei der Umstellung der Verwaltungen auf verschiedene digitale Dienstleistungen nach den Indikatoren Nutzerzentriertheit, Transparenz, grenzüberschreitende Mobilität und technologische Schlüsselelemente in 35 europäischen Ländern (27 EU-Mitgliedstaaten und acht weitere Länder). Der eGovernment-Benchmark 2023[55] zeigt, dass in Europa noch teilweise viel für das Ziel unternommen werden muss, die wichtigsten öffentlichen Verwaltungsleistungen in Europa bis 2030 zu 100 Prozent online verfügbar zu machen. Dabei gibt es eine Lücke zwischen grenzüberschreitenden und nationalen Nutzern. Während beispielsweise 84 Prozent der Behördendienste für nationale Nutzer in Europa vollständig online verfügbar sind, sind nur 49 Prozent der Leistungen für grenzüberschreitende Nutzer in gleicher Weise verfügbar. Unternehmen profitieren von besseren digitalen Verwaltungsleistungen mehr als die Bürgerinnen und Bürger.[56] Der Benchmark Report 2023 zeigt, dass es in mehreren Ländern einen bemerkenswerten Fortschritt bei der Reife digitaler Behördendienste sowie einen Aufschwung bei der Nutzung von Schlüsseltechnologien wie der elektronischen Identifizierung (eID) und digitalen Briefkastenlösungen gibt. Die Unterschiede im Reifegrad der Digitalisierung in Europa sind allerdings weiterhin groß. Die europäischen Spitzenreiter sind Malta (96 Punkte) und Estland (92), gefolgt von Luxemburg (89), Island (88), Finnland (86), den Niederlanden (85), Litauen (85), Dänemark (85), Lettland (82). Weiter hinten rangieren die größten Länder der EU – Frankreich (70), das genau den EU-Durchschnitt abbildet, sowie Deutschland (65) und Italien (61), die bisher in unterdurchschnittlichem Maße ihren Bürgern Online-Dienste bieten.

83 **e) Digital Economy and Society Index (DESI).** Die Europäische Kommission veröffentlicht seit 2014 den Digital Economy and Society Index (DESI), in dem der digitale Fortschritt von Wirtschaft und Gesellschaft in der EU gemessen wird. Dabei stehen der Breitbandausbau, die Onlinekompetenzen sowie die Möglichkeit digitaler Behördengänge im Vordergrund. Enthalten im Index sind Länderprofile, die den Mitgliedstaaten dabei helfen, Bereiche mit vorrangigem Handlungsbedarf zu ermitteln, sowie thematische Kapitel, die eine Analyse auf europäischer Ebene für die wichtigsten digitalen Bereiche bieten und eine wichtige Grundlage für politische Entscheidungen bilden.[57] Ab 2023 und im Einklang mit dem Strategieprogramm 2030 für die digitale Dekade wird DESI nun in den Bericht über

[54] Siehe zur Bedeutung der Benchmarks Bernhardt DGRI Jahrbuch 2018, 213, 214 ff.

[55] https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2023, abgerufen am 29.2.2024.

[56] Siehe dazu Auswertung https://www.capgemini.com/de-de/insights/research/egovernment-benchmark-2023-connecting-digital-governments/, abgerufen am 29.2.2024.

[57] https://digital-strategy.ec.europa.eu/de/node/9773, abgerufen am 15.4.2022.

die digitale Dekade integriert und zur Überwachung der Fortschritte bei der Verwirklichung der digitalen Ziele genutzt.[58] Aus dem DESI 2023 lassen sich Angaben entnehmen, wie die EU-Mitgliedstaaten bei den digitalen Skills, der digitalen Infrastruktur, der digitalen Transformation der Unternehmen, und der Digitalisierung der öffentlichen Verwaltung stehen. Deutschlands Verwaltungsdigitalisierung bewegt sich in etwa im Durchschnitt der EU-Mitgliedstaaten.[59]

II. E-JUSTICE

1. Begriff und Bedeutung

Der Begriff „E-Justice" wurde in Deutschland seit 2001 verwendet. Im Zusammenhang mit der Konzeption und der Realisierung des E-Government-Programmes „Bund Online 2005"[60] sollte mit diesem Begriff die Eigenständigkeit der Justiz gegenüber der Exekutive auch bei der Unterstützung durch Informationstechnik verdeutlicht werden, um zu verhindern, dass etwa die finanzielle Förderung von Projekten zur Einführung des elektronischen Rechtsverkehrs beim BGH als Unterfall der Förderung der elektronischen Verwaltung gesehen wurde.[61] Auch in der BLK (Bund-Länder-Kommission zur Datenverarbeitung und Rationalisierung der Justiz) wurde auf meine Initiative als damaliger Vertreter des Bundesministeriums der Justiz zunehmend dieser Begriff verwendet. **84**

Heute kennzeichnet der Begriff den Einsatz der Informations- und Kommunikationstechnologien (einschließlich neuer Technologien wie Künstliche Intelligenz oder Blockchain sowie der Systeme der Videokonferenz) innerhalb der Justiz und zwischen den Justizorganen und den Justizanwendern/innen. Aber auch die digitalen Instrumente der Informationsbeschaffung wie die Nutzung elektronischer Literatur- und Rechtsprechungsdatenbanken sind begrifflich damit erfasst.[62] **85**

2. Abgrenzung von E-Government und verfassungsrechtliche Grundlagen

a) Begriff. Ausgehend von der im Grundgesetz benannten Eigenständigkeit der Justiz als eine der Staatsgewalten, die sich in den Prinzipien der richterlichen Unabhängigkeit, des Legalitätsprinzips, der sachlichen Unabhängigkeit der Rechtspfleger manifestiert, erfasst „E-Justice" die besonderen Regelungen, die für die Digitalisierung der Justiz getroffen wurden und die sich teilweise von den E-Government-Regelungen unterscheiden.[63] Dennoch gibt es auch weiterhin Parallelen zum E-Government, da sich auch die IT-Unterstützung der Justiz wie diejenige der Exekutive von den Prinzipien der Effizienz mit dem Abbau von bürokratischen Hürden, des Nutzens für die Bürgerinnen und Bürger, der Transparenz und allgemein der Beachtung rechtstaatlicher Prinzipien leiten lassen sollte. Dies führt auch zu dem anzustrebenden Ziel, möglichst gleiche oder vergleichbare digitale Kommunikationswege der Bürgerinnen und Bürger sowie der Unternehmen zur Justiz vorzusehen. **86**

---

[58] https://digital-strategy.ec.europa.eu/de/policies/desi.

[59] https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/compare-countries-progress?indicator=desi_4a2&breakdown=all_egov_le&unit=egov_score&country=EU,DE&period=desi_2023, abgerufen am 29.2.2024.

[60] Seit 2000 hatte die Bundesregierung unter Federführung des Bundesministeriums des Innern mit dem Projekt Bund Online 2005 das Ziel verfolgt, alle internetfähigen Dienstleistungen der Bundesverwaltung online zu stellen. Etwa 100 Bundesbehörden sollten innerhalb von fünf Jahren ihre Verwaltungsprozesse elektronifizieren und ihre Dienstleistungen im Internet bereitstellen.

[61] So wurde etwa im Einzelplan 07 des Bundesministeriums der Justiz des Bundeshaushalts 2005, S. 12, (Haushaltsgesetz 2005) bei der Titelgruppe 55 ein Haushaltsvermerk so beschrieben: „Einsparungen bei den Ausgaben für E-Justice dienen zur Deckung von Mehrausgaben bei folgendem Titel: 981 55.

[62] Siehe dazu näher Heckmann/Paschke/Bernhardt/Leeb juris-Praxiskommentar Internetrecht, 7. Aufl. 2021, Kap. 6, Rn. 1 ff.

[63] Bernhardt JURPC Web-Dok. 75/2007, Abs. 3; Köbler NJW 2006, 2089; Wirtz/Heckmann, E-Government, 2020, S. 93, 97 ff.

87 Da anfänglich der Schwerpunkt der Bemühungen um den IT-Einsatz für die Justiz vor allem darauf lag, die elektronische Kommunikation mit den Nutzerinnen und Nutzern der Justiz (den Verfahrensbeteiligten) zu ermöglichen, wurde zunächst der Begriff „E-Justice" weitgehend synonym mit dem älteren Begriff des elektronischen Rechtsverkehrs benutzt. Nachdem die gesetzlichen Grundlagen für eine die Papierkommunikation ersetzende digitale Justizkommunikation geschaffen waren, ging es darum, die interne Verarbeitung von Justizdaten, vor allem die elektronische Aktenführung rechtlich und tatsächlich zu ermöglichen und zu realisieren. Die Verkündung, Dokumentation und Veröffentlichung gerichtlicher Entscheidung sind ebenfalls der Rubrik „E-Justice" zuzuordnen. Auch lässt sich die in der Justiz während der Hochphase der Pandemie verstärkt zum Einsatz gelangte und zukünftig sicherlich noch bedeutsamer werdende Videokonferenztechnik auch unter „E-Justice" subsumieren. Und schließlich zählt zu E-Justice auch die elektronische Führung von Justizregistern (wie Handelsregister, Elektronisches Unternehmensregister, Elektronisches Genossenschaft- und Partnerschaftsregister, Elektronisches Vereinsregister, das mit dem dem Inkrafttreten des Gesetzes zur Modernisierung von Personengesellschaften (MoPeG) am 1.1.2024 neu eingeführte Gesellschaftsregister, Bundeszentralregister, Zentrales Staatsanwaltschaftliches Verfahrensregister, Elektronisches Grundbuch, das Zentrale Schutzschriftenregister, die bei der Bundesnotarkammer eingerichteten Register wie das Zentrale Testamentsregister, das Zentrale Vorsorgeregister und das Elektronische Urkundenarchiv).[64] Demgegenüber rechnen nicht zu E-Justice (bzw. zum elektronischen Rechtsverkehr) der elektronische Geschäftsverkehrs („E-Commerce" oder „eCommerce") und das Internet- und Telekommunikationsrecht.[65]

88 „E-Justice" verfügt auch über eine **europäische Dimension:** Deutschland hatte während der EU-Ratspräsidentschaft im ersten Halbjahr 2007 erfolgreich die Einsetzung einer eigenen „E-Justice"-Ratsarbeitsgruppe initiiert und neben der grenzüberschreitenden Vernetzung der Register vor allem den Aufbau eines europäischen E-Justice-Portals[66] auf den Weg gebracht.[67] Das Portal dient als zentraler Zugangspunkt für Informationen über die nationalen Justizsysteme und das europäische Justizsystem. Es soll allgemein den Zugang zum Recht in der EU erleichtern. Somit können bestimmte Verfahren – wie das Europäische Mahnverfahren – über das Europäische Justizportal initiiert und Verfahrenshandlungen digital über das Justizportal geleitet werden. Dabei werden Komponenten aus dem E-CODEX-Projekt[68] genutzt. Es können standardisierte Informationen über geltende Rechtsvorschriften für EU-Bürgerinnen und Bürger und anwendbares Fallrecht in der EU abgerufen werden. Auch ist der grenzüberschreitende Zugang zu vielen Justizregistern über das E-Justice-Portal eröffnet. Während die E-Justice-Aktivitäten auf europäischer Ebene anfänglich weitgehend auf Ratsbeschlüssen beruhten, ohne dass hierfür neue Rechtsgrundlagen geschaffen werden mussten, sind mittlerweile einige Rechtsgrundlagen in Kraft gesetzt oder auf den Weg gebracht worden. Dazu zählen die **ECRIS-Verordnung,**[69] die **ECRIS-TCN-Verordnung,**[70] die **Verordnung über das europäische Mahnverfahren,**[71] die **EU-Verordnung**

[64] Siehe zu dem weiten Begriffsverständnis bereits Radke, JurPC Web-Dok. 46/2006, Abs. 1 – 28.

[65] Hähnchen, JurPC Web-Dok. 151/2007, Abs. 2

[66] Heute eher als „Europäisches Justizportal" bezeichnet: https://e-justice.europa.eu/home?plang=de&action=home, abgerufen am 29.2.2024.

[67] Bernhardt JurPC Web-Dok. 75/2007, Abs. 29. Schlussfolgerungen des Rates (Justiz und Inneres) vom 12./13.6.2007, Ratsdokument 10267/07, A. 43.

[68] https://www.e-codex.eu/, abgerufen am 29.2.2024.

[69] Beschluss 2009/316/JI des Rates v. 6.4.2009 zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gem. Art. 11 des Rahmenbeschlusses 2009/315/JI des Rates v. 26.2.2009. Siehe ferner Informationen auf der Website des Bundesamts für Justiz unter https://www.bundesjustizamt.de/DE/Themen/ZentraleRegister/Datenaustausch/Behoerdenportal/Registervernetzung/Registervernetzung_node.html, abgerufen am 29.2.2024.

[70] Verordnung (EU) 2019/816 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Nicht-EU-Staatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, vom 17.4.2019, ABl. EU L 135/1 v. 22.5.2019.

[71] VO (EG) Nr. 1896/2006, ABl. EU L 399/1 v. 30.12.2006.

über ein Verfahren bei geringfügigen Forderungen,[72] die **E-CODEX-Verordnung,**[73] die **Verordnung (EU) 2020/1784 vom 25.11.2020 über die Zustellung gerichtlicher und außergerichtlicher Schriftstücke in Zivil- oder Handelssachen in den Mitgliedstaaten („Zustellung von Schriftstücken") – Neufassung –,**[74] **die Verordnung (EU) 2020/1783 vom 25.11.2020 über die Zusammenarbeit zwischen den Gerichten der Mitgliedstaaten auf dem Gebiet der Beweisaufnahme in Zivil- oder Handelssachen (Beweisaufnahme) – Neufassung –,**[75] die **e-Evidence-Verordnung**[76] (Europäische Herausgabeanordnung und Europäische Sicherungsanordnung), die **Verordnung (EU) 2023/2844 vom 13.12.2023 über die Digitalisierung der justiziellen Zusammenarbeit und des Zugangs zur Justiz in grenzüberschreitenden Zivil-, Handels- und Strafsachen und zur Änderung bestimmter Rechtsakte im Bereich der justiziellen Zusammenarbeit**[77] sowie die **Richtlinie über die Benennung gesetzlicher Vertreter von innerhalb der EU agierenden Dienstanbietern**[78] Daneben haben natürlich etliche europäische Regulierungen wie die Datenschutzgrundverordnung und das europäische KI-Gesetz ebenfalls Bedeutung für die Justiz.

b) Die **Eigenständigkeit von E-Justice gegenüber E-Government** hat auch **institutionelle Konsequenzen.** Art. 91c GG sieht eine IT-Zusammenarbeit zwischen Bund und Ländern sowie der Länder untereinander vor. Diese Zusammenarbeit ist nicht auf die Verwaltungen beschränkt. Vielmehr kann sich auch die Zusammenarbeit in der Justiz (-verwaltung) auf Art. 91c GG stützen. Die Norm eröffnet Bund und Ländern die Möglichkeit, bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenzuwirken. Dies beinhaltet auch die Errichtung der hierzu erforderlichen Gremienstruktur. Entsprechend hat der IT-Staatsvertrag die Einrichtung, Arbeitsweise und Entscheidungsmodalitäten des IT-Planungsrates beschrieben.[79] Dieses von Bund und Ländern gemeinsam getragene Gremium übernimmt demnach die Koordinierung in Fragen der Informationstechnik wie etwa die Festlegung von IT-Interoperabilitätsstandards und IT-Sicherheitsstandards. 89

Bereits mit Aufnahme seiner Tätigkeit diskutierte der IT-Planungsrat im Jahre 2000 intensiv über die Frage, welche Reichweite den Entscheidungen dieses Gremiums – insbesondere bei der Standardsetzung – zukommen würden. So ist zu berücksichtigen, dass das grundgesetzlich verankerte Gewaltenteilungsprinzip[80] neben der räumlichen, personalen und organisatorischen Trennung der Gewalten und das Verfassungsprinzip der Unabhängigkeit der Richter[81] auch eine strikte Datenherrschaft der Justiz erfordern. Zentralisierungs- und Stan- 90

[72] Verordnung (EG) Nr. 861/2007 vom 11.7.2007zur Einführung eines europäischen Verfahrens für geringfügige Forderungen (ABl. L 199 vom 31.7.2007, S. 1).

[73] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein EDV-System für die grenzüberschreitende Kommunikation in Zivil- und Strafverfahren (e-CODEX) und zur Änderung der Verordnung (EU)2018/1726, COM(2020) 712 vom 2.12.2020.

[74] Verordnung (EU) 2020/1784 des Europäischen Parlaments und des Rates vom 25.11.2020 über die Zustellung gerichtlicher und außergerichtlicher Schriftstücke in Zivil- oder Handelssachen in den Mitgliedstaaten („Zustellung von Schriftstücken")- Neufassung, ABl. L 405/40 vom 2.12.2020.

[75] ABl. L 405 vom 2.12.2020, S. 1.

[76] Verordnung (EU) 2023/1543 vom 12.7.2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, ABl. L 191/118 vom 28.7.2023.

[77] ABl. L, 2023/2844, 27.12.2023.

[78] ■■■.

[79] Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (IT-Staatsvertrag) vom 30.10.2009, für die Bundesrepublik Deutschland: G v. 27.5.2010 (BGBl. I S. 662). Neu bekannt gemacht durch Bek. v. 13.12.2019 (BGBl. I S. 2852).

[80] Es wird aus Art. 20 Abs. 2 GG abgeleitet („Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt."). Die Gewaltenteilungslehre geht vor allem auf den englischen Philosophen John Locke (1632–1704) und den französischen Aufklärer Charles de Montesquieu (1689–1755) zurück. Klassischerweise wird darunter die Aufteilung der staatlichen Gewalt in mehrere Gewalten (Legislative, Exekutive, Judikative) verstanden, die sich gegenseitig kontrollieren und beschränken und von verschiedenen Personen ausgeübt werden.

[81] Art. 97 Abs. 1 GG: „Die Richter sind unabhängig und nur dem Gesetze unterworfen".

dardisierungsbemühungen von Institutionen, die nicht in der Verantwortung der Justiz stehen, könnten diese Datenherrschaft beeinträchtigen.[82] Auch unter Berücksichtigung des Erfordernisses eines auf die Nutzer bezogenen Interessens an dem Zusammenwirken von Verwaltung und Justiz ist die Frage prüfungsbedürftig, ob und in welchem Umfang einzelne Sachbereiche der Justiz-IT einer Lenkung durch den IT-Planungsrat unterliegen dürfen. In der Begründung des Entwurfes eines Zustimmungsgesetzes zum „Vertrag zur Ausführung von Art. 91c GG (IT-Staatsvertrag[83])" wurde die verfassungsrechtlich notwendige Berücksichtigung justizspezifischer Belange im Falle des Tätigwerdens des IT-Planungsrates erkannt und klargestellt.[84] So wird darauf hingewiesen, dass der IT-Planungsrat eng mit den Fachministerkonferenzen (also auch der Justizministerkonferenz) zusammenarbeitet, da ein effektiver Einsatz der Informationstechnik nur unter Berücksichtigung der jeweiligen fachlichen Belange gewährleistet werden kann. Dem folgte auch der IT-Planungsrat: Durch schriftliche Erklärung zur Geschäftsordnung wurde klargestellt, dass die aus den verfassungs- und einfachrechtlich garantierten Positionen der unabhängigen Rechtspflegeorgane resultierenden Besonderheiten zu beachten sind und die richterliche Unabhängigkeit zu wahren ist.[85] In der praktischen Arbeit des IT-Planungsrats wird den E-Justice-Aspekten dadurch Rechnung getragen, dass über das Mitglied im IT-Planungsrat, das als Ansprechpartner der Justizministerkonferenz fungiert, die zur Beschlussfassung im IT-Planungsrat vorgesehenen Tagesordnungspunkte vorab über den E-Justice-Rat der Bund-Länder-Kommission für Informationstechnik in der Justiz zur Stellungnahme zugeleitet werden. Diese Stellungnahmen werden sodann wiederum über den Justiz-Ansprechpartner in die IT-Planungsratssitzungen eingebracht.

91 Aus Gründen der **institutionellen Sonderstellung der Justiz** arbeiten das Bundesjustizministerium und die Landesjustizverwaltungen bereits seit Jahrzehnten zusammen, um ihre Aktivitäten beim Einsatz der Informationstechnologie in der Justiz und für die Justiz zu koordinieren. Bereits die 37. Justizministerkonferenz am 30. und 31.5.1969 hatte beschlossen, eine „Kommission für Datenverarbeitung" mit dem Ziel zu gründen, ein juristisches Informationssystem zu entwickeln und alle Rechtsgebiete im Hinblick auf ihre Eignung für die elektronische Datenverarbeitung prüfen zu lassen. Nach dem Zusammenschluss mit dem Ländergremium für allgemeine Rationalisierungsfragen erhielt sie den Namen „Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz (BLK)".[86] Als Reaktion auf den Abschluss des IT-Staatsvertrages und die Gründung des IT-Planungsrats wurde im Juni 2012 als neues hochrangiges Koordinierungsgremium für die Justizverwaltungen von Bund- und Ländern auf Staatssekretärsebene (Amtschefebene) der **E-Justice-Rat**[87] gegründet. Die BLK nahm seitdem die Rolle einer ständigen Arbeitsgruppe des im Juni 2012 neu gegründeten E-Justice-Rats ein und firmierte fortan unter der Bezeichnung **„Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK)".**

92 c) Dem **Gewaltenteilungsgrundsatz** wie aber auch dem Grundsatz der richterlichen Unabhängigkeit kommt auch Bedeutung zu, wenn es um die Frage der Verantwortung für die

[82] Heckmann/Paschke/Bernhardt/Leeb juris-Praxiskommentar Internetrecht, 7. Aufl. 2021, Kap. 6, Rn. 71 mwN.

[83] Gesetz zum Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG vom 27.5.2010, BGBl. I 2010, 662.

[84] Siehe Begründung zum Entwurf eines Gesetzes zum Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG in BT-Drs. 17/247 S. 6, www.cio.bund.de/SharedDocs/Publikationen/DE/Bundesbeauftragter-fuer-Informationstechnik/it_planungsrat_gesetzentwurf_download.pdf?__blob=publicationFile, abgerufen am 30.3.2022.

[85] Ehemals zu § 10 der Geschäftsordnung. Mittlerweile wurde die Geschäftsordnung fortentwickelt, so dass sich die Protokollerklärung nunmehr auf § 17 bezieht: Siehe aktuelle Fassung der Geschäftsordnung vom 3.11.2023, https://www.it-planungsrat.de/fileadmin/beschluesse/2023/Beschluss2023-40_Gesch%C3%A4ftsordnung_GO_IT-PLR.pdf (abgerufen am 26.2.2024).

[86] https://justiz.de/laender-bund-europa/BLK/index.php.

[87] https://justiz.de/laender-bund-europa/e_justice_rat/index.php, abgerufen am 16.4.2022.

Datenhaltung der Justiz geht.[88] So sah das BVerfG in einem richtungsweisenden Nichtannahmebeschluss vom 17.1.2013 keine Erfolgsaussicht einer Verfassungsbeschwerde einer Vorsitzenden Richterin am Oberlandesgericht Hessen gegen die Zentralisierung von Justizdaten bei der Hessischen Zentrale für Datenhaltung (HDZ). Es definierte in der Entscheidung die Reichweite der richterlichen Unabhängigkeit bei Zentralisierung der Justiz-IT. Eine Verletzung des Art. 33 Abs. 5 iVm Art. 97 Abs. 1 GG sei nicht ersichtlich. Auch gebe es keine Anhaltspunkte für einen Verstoß gegen das verfassungsrechtliche Gebot organisatorischer Selbständigkeit der Gerichte aus Art. 20 Abs. 2 S. 2, Art. 92 und 97 GG. Zwar gehöre zu den hergebrachten Grundsätzen des Richteramtsrechts (Art. 33 Abs. 5 GG) auch der Grundsatz der sachlichen und persönlichen Unabhängigkeit des Richters. Dabei gewährleiste der Grundsatz der Unabhängigkeit, dass ein Richter seine Entscheidungen frei von Weisungen fällen kann. Art. 97 Abs. 1 GG verbiete auch jede vermeidbare, auch mittelbare, subtile und psychologische Einflussnahme der Exekutive auf die Rechtsstellung des Richters. Solche Einflussnahme könne auch vorliegen, wenn ein besonnener Richter durch ein Gefühl des unkontrollierbaren Beobachtetwerdens von der Verwendung der ihm zur Erfüllung seiner richterlichen Aufgaben zur Verfügung gestellten Arbeitsmittel abgehalten würde. Allein die Zentralisierung der elektronischen Datenverarbeitung der Daten der Justiz sei jedoch nicht verfassungswidrig, wenn Exekutive und Dritte „jedenfalls nach den in der angegriffenen Entscheidung des Hessischen Dienstgerichtshofs für Richter formulierten Bedingungen für die Überlassung der Verwaltung des EDV-Netzes der Hessischen Justiz an die HZD über keine Zugriffserlaubnisse hinsichtlich der von der Beschwerdeführerin für ihre dienstlichen Aufgaben verwendeten Daten“ verfügen. Die den Systemadministratoren eingeräumten Zugriffsrechts seien streng limitiert und beschränkten sich auf Maßnahmen, die zum Funktionieren des EDV-Netzes betriebsnotwendig sind. Die Weitergabe richterlicher Dokumente an die Exekutive oder an Dritte sei den Administratoren untersagt. Auch die Speicherung und Weitergabe sogenannter Metadaten richterlicher Dokumente (Autor und Erststellungszeitpunkt) seien unzulässig, soweit nicht konkreter Verdacht eines Missbrauchs des EDV-Netzes zu dienstfremden Zwecken besteht.

93 **d**) Richtungsweisend im Hinblick auf die Wirkung der **Garantie richterlicher Unabhängigkeit beim Zwang zur Nutzung der elektronischen Akte** durch einen Richter war auch die Entscheidung des BGH in einem Urteil vom 21.10.2010.[89] Die Weigerung der Dienstaufsicht, einem mit Handelsregistersachen befassten Richter die elektronisch eingereichten Eingaben zum Handelsregister in ausgedruckter Form zur Bearbeitung vorzulegen, stelle keine Verletzung der richterlichen Unabhängigkeit dar. Zwar folge aus der Unabhängigkeit des Richters, dass er grundsätzlich seine Arbeit nicht innerhalb fester Dienstzeiten und nicht an der Gerichtsstelle erledigen muss. Das gelte aber nicht, wenn die Ausführung der ihm obliegenden Dienstgeschäfte die Anwesenheit an der Gerichtsstelle erfordert. Denn die richterliche Unabhängigkeit sei kein Standesprivileg der Richter. Erfordere die Bearbeitung der gemäß den Anforderungen des Gesetzgebers in elektronischer Form vorliegenden Eingaben zum Handelsregister die Anwesenheit des Richters an seinem computergestützten Arbeitsplatz, liege darin keine Beeinträchtigung der richterlichen Unabhängigkeit durch die Dienstaufsicht.[90]

94 **e**) Weitere verfassungsrechtliche Rahmenbedingungen für E-Justice ergeben sich aus der dem **Prinzip effektiven Rechtsschutzes (Art. 19 Abs. 4 GG)** bzw. aus dem **Justizgewährungsanspruch des Art. 2 Abs. 1 GG iVm dem Rechtsstaatsprinzip** im Zivilprozess. So müssen die

[88] So hatte Bertrams DRiZ 2010, S. 248 ff. die Meinung vertreten, selbst die Eingliederung der Justiz IT in eine dem Justizministerium unterstellte „IT-Betriebsstelle“ sei verfassungswidrig; ders. NWVBl. 2007, 205; ders. NWVBl. 2010, 209.

[89] BGH 21.10.2010 – RiZ (R) 5/09, NJOZ 2011, 1461.

[90] Zustimmend Marly LMK 2011, 313258. Ebenfalls zustimmend zur entsprechenden Interpretation der „richterlichen Unabhängigkeit“ Berlit, eJustice, eAkte und Richterschaft, Betrifft JUSTIZ Nr. 121, März 2015, S. 15 ff.

Formvorgaben beim elektronischen Rechtsverkehr dieses Verfassungsprinzip beachten.[91] Der verfassungsrechtlich verbriefte Justizgewährungsanspruch verlangt zum einen, dass Verfahren in einer angemessenen Zeit durch die Gerichte bearbeitet und entschieden werden. Daraus ergibt sich, dass Gerichte die zur Verfügung stehende elektronische Unterstützung nutzen sollten, um ein gerichtliches Verfahren in angemessener Zeit bewältigen zu können.[92] Der Justizgewährungsanspruch verlangt aber auch von den Gerichten, das Verfahrensrecht so zu handhaben, dass die eigentlichen materiellen Rechtsfragen entschieden werden und diesen Rechtsfragen nicht durch übertriebene Anforderungen an das formelle Recht ausgewichen wird.[93] Die formellen Einschränkungen bei der Justizgewährleistung müssen mit den Belangen einer rechtsstaatlichen Verfahrensordnung vereinbar sein und dürfen den Rechtsuchenden nicht unverhältnismäßig belasten.

95 **f) Artikel 103 Abs. 1 GG** (Anspruch auf rechtliches Gehör) „gebietet, dass sowohl die normative Ausgestaltung des Verfahrensrechts als auch das gerichtliche Verfahren im Einzelfall ein Maß an rechtlichem Gehör eröffnen, das sachangemessen ist, um dem in bürgerlichrechtlichen Streitigkeiten aus dem Rechtsstaatsprinzip folgenden Erfordernis eines wirkungsvollen Rechtsschutzes gerecht zu werden und das den Beteiligten die Möglichkeit gibt, sich im Prozess mit tatsächlichen und rechtlichen Argumenten zu behaupten".[94] Insoweit dürfen auch die formalen Hürden für die Nutzung der digitalen Instrumente nicht zu hoch sein; selbst von einem professionellen Nutzer der Justiz darf der erwartbare Aufwand nicht zu groß sein. Dies gilt erst recht für nicht anwaltlich vertretene Bürgerinnen und Bürger.

96 **g)** Auch die Grundrechte wie das **Nichtdiskriminierungsverbot** (**Art. 3 GG**) sind stets bei der Gestaltung der der IT-Unterstützung der Justiz zu beachten. Dies gilt insbesondere bei der Nutzung künstlicher Intelligenz, bei der die sogenannte Bias-Problematik beachtet werden muss. Aber auch weiteren Grundrechten kommt eine digitale Dimension zu.[95]

97 **h)** Eine bedeutsame Rolle spielt auch das **Recht auf informationelle Selbstbestimmung** und das Recht auf die **Gewährleistung der IT-Sicherheit.**[96] Regelmäßig und in erheblichem Umfang werden in der Justiz und in der Kommunikation mit der Justiz hochsensible personenbezogene Daten verarbeitet. Bei zentraler Datenvorhaltung entstehen durch gebündelte Datenvorhaltung hochsensible Datensammlungen. Die Vertraulichkeit und die Integrität der Kommunikation mit der Justiz ist eine unentbehrliche Grundlage für den Fortbestand des Vertrauens in die Dritte Gewalt. Deshalb sind besonders hohe Anforderungen an den Schutz von Integrität, Vertraulichkeit und datenschutzkonformen beim IT-Einsatz in der Justiz zu stellen. Die am 25.5.2016 in Kraft getretene und seit dem 25.5.2018 anwendbare EU-Datenschutz- Grundverordnung (DSGVO) entfaltet auch im Kontext von E-Justice Wirkung für den Schutz des Rechts auf informationelle Selbstbestimmung. Der Bereich der Strafverfolgung ist explizit durch Art. 2 Abs. 2 lit. b DSGVO vom sachlichen Anwendungsbereich

[91] Müller NZS 2018, 207: Den Gerichten sei vor dem Hintergrund der Gewährung effektiven Rechtsschutzes ein pragmatischer Umgang mit diesem neuen Formerfordernis (der Durchsuchbarkeit eines Dokuments) anzuraten. Die Formvorschrift solle „vor dem Hintergrund eventuell betroffener Prozessgrundrechte" „nicht unnötig überbetont werden".

[92] Bernhardt, The Use of Artificial Intelligence in the Field of Justice, in: Szostek/Załucki (Hrsg.) Internet and New Technologies Law, S. 188. Siehe auch Völzmann DÖV 2021, S. 474, 483 . Er verweist darauf, dass die vom Recht geschützten Werte „durch Technik, eben Legal Tech, auch unterstützt, verstärkt, verwirklicht werden" können. Siehe Wahedi, Verfassungsrechtliche Anforderungen an die Automatisierung der Justiz, die zwar das Wirtschaftlichkeitsgebot aus Art. 114 GG, den Beschleunigungsgrundsatz als Inhalt der Rechtsschutzgarantien in Art. 19 Abs. 4 und Art. 2 Abs. 1 iVm Art. 20 Abs. 3 GG sowie den Grundsatz der Funktionsfähigkeit der Rechtspflege (abgeleitet aus Art. 20 Abs. 1, 3) auch für die Justiz bindende Verfassungsprinzipien definiert, aber keine daraus folgende Automationspflicht ableiten will.

[93] Oltmanns/Fuhlrott NZA 2020, 897; BVerfGE 88, 118, 123; BVerfG 25.8.2015 – 1 BvR 1528/14, NZA 2016, 122.

[94] BVerfG 25.8.2015 – 1 BvR 1528/14, NZA 2016, 122.

[95] Hoffmann/Luch/Schul/Borchers, Die digitale Dimension der Grundrechte, 2015.

[96] Hessel/Rebmann, IT-Sicherheit in der Justiz- Wege aus einer drohenden Krise, in: Schweighofer/Hötzendorfer/Kummer/Saarenpää (Hrsg.) Verantwortungsbewusste Digitalisierung Tagungsband des 23. Internationalen Rechtinformatik Symposiums IRIS 2020, 369 ff.; zu den potentiellen IT-Risiken in der Justiz siehe Vogelgesang Datensicherheit und IT-Sicherheit in der Justiz jM 2018. S. 2 ff.

ausgenommen. Hierfür ist vielmehr die JI-Richtlinie vom 27.4.2016[97] einschlägig, die mit dem neuen Bundesdatenschutzgesetz mit Wirkung vom 25.5.2018 umgesetzt wurde. Die Hochverfügbarkeit von Justizdaten ist zu gewährleisten. Den typischen Gefährdungslagen wie (D)DoS-Attacken, Hackerangriffen, Virenbefall, Systemausfall, Datenmanipulation, Identitätsdiebstahl usw. ist wirkungsvoll vorzubeugen.

3. Elektronischer Rechtsverkehr

a) Allgemeines und Entwicklung. Der rechtliche Rahmen für die Justizkommunikation wurde in mehreren Etappen gesetzt: Mit dem Formvorschriftenanpassungsgesetz vom 13.7.2001[98] wurde die Ersetzung der Schriftform durch die elektronische Form in den Prozessordnungen ermöglicht. Das Zustellungsreformgesetz vom 25.6.2001[99] regelte die Zustellung von elektronischen Dokumenten (zB § 174 Abs. 3,4 ZPO). Das am 1.4.2005 in Kraft getretene Justizkommunikationsgesetz[100] regelte die elektronischen Verfahrensabläufe zwischen dem Eingang und dem Ausgang elektronischer Dokumente innerhalb der Gerichte, also vor allem die elektronische Aktenführung an den Gerichten. Das am 1.12.2008 in Kraft getretene Zweite Justizmodernisierungsgesetz[101] sah vor allem die Verpflichtung der Rechtsanwälte vor, am automatisierten Mahnverfahren teilzunehmen (§ 707 Abs. 2 ZPO). Durch das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung v. 29.7.2009 wurde ein elektronischer Antrag auf Erlass eines Pfändungs- und Überweisungsbeschlusses bei Vollstreckungsbescheiden ermöglicht (§ 829a ZPO). Das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013[102] erweiterte die elektronischen Schriftformersatzmöglichkeiten über den Einsatz der qualifizierten elektronischen Signatur hinaus ua auf die Kommunikation über sogenannte sichere Übermittlungswege, nämlich über eine absenderbestätigte DE-Mail, über besondere elektronische Postfächer ua für Anwälte (beA) und Behörden (beBPo) und weitere sichere Verfahren. Ferner sah dieses Gesetz bestimmte Fristen vor, ab denen die Gerichte elektronische Eingänge entgegenzunehmen hatten (ab 1.1.2018)[103] bzw. bestimmte professionelle Justizanwender die besonderen Postfächer passiv (1.1.2018)[104] bzw. aktiv (spätestens ab 1.1.2022) zu nutzen hatten.[105] Das Empfangsbekenntnis wurde auf eine elektronische Variante umgestellt.[106] Das Gesetz zur Durchführung der Verordnung (EU) Nr. 655/2014 sowie zur Änderung sonstiger zivilprozessualer Vorschriften (EuKoPfVODG) bestimmte zum 1.1.2018 die Eröffnung des elektronischen Rechtsverkehrs bei den Gerichtsvollziehern. Schriftlich einzureichende Anträge und Erklärungen, dh die von der Gerichtsvollzieherformular-Verordnung erfassten Vollstreckungsaufträge sowie die zur Vollstreckung im vereinfachten Verfahren nach § 754a ZPO benötigten Unterlagen konnten ab diesem Zeitpunkt auch als elektronisches Dokument bei Gerichtsvollziehern eingereicht werden (§ 753 Abs. 4 ZPO). Das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5.7.2017[107] sah im Wesentlichen eine Ausdehnung der 98

[97] Richtlinie (EU) 2016/680 vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

[98] BGBl. I 2001, 1542.

[99] Gesetz zur Reform des Verfahrens bei Zustellungen im gerichtlichen Verfahren (ZustRG) v. 25.6.2001, BGBl. I 2006, 1206.

[100] BGBl. I 2005, 837.

[101] BGBl. I 2006, 3416.

[102] BGBl. I 2013, 3786.

[103] Artikel 26 – Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (FördElRV k. a. Abk.).

[104] Etwa § 31a Abs. 6 BRAO die sogenannte passive Nutzungspflicht des beA für die Rechtsanwältinnen und Rechtsanwälte.

[105] Art. 26 Abs. 7 des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013.

[106] § 174 Abs. 4 Satz 3 ZPO.

[107] BGBl. I 2017, 2208.

Vorschriften für den elektronischen Rechtsverkehr und die elektronische Aktenführung auf die Staatsanwaltschaften und den Strafprozess vor. Das am 7.7.2021 verkündete „Gesetz zur Neuregelung des Berufsrechts der anwaltlichen und steuerberatenden Berufsausübungsgesellschaften“[108] sah ein Kanzleipostfach für Rechtsanwaltsgesellschaften[109] und das besondere elektronische Steuerberaterpostfach (beSt) vor.[110] Das Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer Vorschriften (ERVAG) v. 5.10.2021[111] normierte die Einrichtungspflicht für besondere elektronische Postfächer der Gerichtsvollzieher (ab 1.1.2022)[112] und für Steuerberater (ab 1.1.2023)[113] sowie ab 1.1.2024 für sonstige in professioneller Eigenschaft am Prozess beteiligte Personen, Vereinigungen und Organisationen, bei denen von einer erhöhten Zuverlässigkeit ausgegangen werden kann.[114] Schließlich sieht dieses Gesetz in den Prozessordnungen auch einen „sicheren Übermittlungsweg zwischen besonderen elektronischen Postfach einer natürlichen oder juristischen Person oder einer sonstigen Vereinigung und der elektronischen Poststelle des Gerichts vor, bei dem das Anbringen einer qualifizierten elektronischen Signatur verzichtbar ist.“ Auch das im Rahmen des Verwaltungsportalverbunds einzurichtende Nutzerkonto im Sinne des § 2 Abs. 5 Onlinezugangsgesetz (OZG) soll für eine schriftformersetzende Kommunikation mit den Gerichten nutzbar sein.[115] Gemäß § 157e StBerG in der ab 1.8.2022 geltenden Fassung sind die Regelungen zur Steuerberaterplattform allerdings seit 31.12.2022 anwendbar.

99 **b) Elektronisches Gerichts- und Verwaltungspostfach.** Grundlage für eine sichere Kommunikationsstruktur für die Justiz war die Entwicklung des Elektronischen Gerichts- und verwaltungspostfachs von 2004 (EGVP),[116] eine Software, die damals von der Firma bremen onlineservices GmbH & Co. KG (bos) unter Beteiligung des Bundesministeriums der Justiz gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik, dem Bundesfinanzhof, dem Bundesverwaltungsgericht und dem Land Nordrhein-Westfalen entwickelt wurde. Ferner basiert die Justizkommunikation auf dem Registrierungsdienst SAFE (Secure Access to Federated e-Justice/e-Government),[117] der sichere elektronische Identitäten für Personen und Organisationen zur Verfügung stellt. Die elektronischen Identitäten können in verschiedenen Anwendungsszenarien über den elektronischen Rechtsverkehr hinaus auch für den Zugang zu zentralen Justizregistern genutzt werden.

---

[108] BGBl. I 2021, 2363.

[109] § 31b BRAO, gültig ab 1.8.2022.

[110] § 86e Abs. 1 StBerG in der ab 1.8.2022 maßgebenden Fassung.

[111] BGBl. I 2021, 4607.

[112] Seit dem 1.1.2022 müssen vorbereitende Schriftsätze und deren Anlagen, sowie schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse, als elektronisches Dokument beim Gericht eingereicht werden. Dies findet gemäß §§ 753 Abs. 4, 5 ZPO auch bei der Kommunikation mit den Gerichtsvollzieherinnen und Gerichtsvollziehern Anwendung. Vollstreckungsaufträge an Gerichtsvollzieherinnen und Gerichtsvollzieher können also vom oben genannten Personenkreis nur noch auf elektronischem Weg eingereicht werden. Das Gesetz zur Durchführung der Verordnung (EU) Nr. 655/2014 sowie zur Änderung sonstiger zivilprozessualer Vorschriften (EuKoPfVODG) bestimmt zum 1.1.2018 die Eröffnung des elektronischen Rechtsverkehrs bei den Gerichtsvollziehern. Schriftlich einzureichende Anträge und Erklärungen, dh die von der Gerichtsvollzieherformular-Verordnung erfassten Vollstreckungsaufträge, sowie die zur Vollstreckung im vereinfachten Verfahren nach § 754a ZPO benötigten Unterlagen können ab diesem Zeitpunkt auch als elektronisches Dokument bei Gerichtsvollziehern eingereicht werden (§ 753 Abs. 4 ZPO).

[113] Über das dann anwendbare besondere elektronische Steuerberaterpostfach (beSt), § 86d StBerG in der ab 1.8.2022 geltenden Fassung.

[114] § 173 Abs. 2 S. 2 ZPO („sonstige in professioneller Eigenschaft am Prozess beteiligte Personen, Vereinigungen und Organisationen, bei denen von einer erhöhten Zuverlässigkeit ausgegangen werden kann, sollen einen sicheren Übermittlungsweg für die elektronische Zustellung eröffnen“) wird mit Wirkung vom 1.1.2024 aufgehoben, so dass auch dieser Kreis von Personen und Organisationen ab 1.1.2024 einen

[115] § 130a Abs. 4 Nr. 5 ZPO.

[116] https://egvp.justiz.de/, abgerufen am 16.4.2022. Weitere Informationen bei Heckmann/Paschke/Bernhardt/Leeb, jurisPK-Internetrecht, 7. Aufl., Kap. 6 (Stand: 23.1.2024) Rn. 262 ff.

[117] Heckmann/Paschke/Bernhardt/Leeb, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 6 (Stand: 7.3.2022) Rn. 177.

c) Strukturierter Datenaustausch. Wesentlich für einen effizienten elektronischen Rechtsverkehr ist die Entwicklung eines bundesweit einheitlichen Standards für den Austausch elektronischer Informationen. Einzelne verfahrensbezogene Daten – etwa die Namen und die Adressen von Prozessbeteiligten – sollen insbesondere zwischen Anwälten, Gerichten und Staatsanwaltschaften problemlos eingelesen und weiterverarbeitet werden können, unabhängig vom jeweils eingesetzten Betriebssystem und unabhängig von der verwendeten Kanzlei- oder Gerichtssoftware. Bereits vor 19 Jahren hat die damalige Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz (später Bund-Länder-Kommission für Informationstechnik in der Justiz) den Datensatz XJustiz entwickelt. Dieser besteht aus einer Sammlung von XML-Schemata, in denen die Regeln zum Austausch der im Justiz- Informationen festgelegt sind. Diese sollen es allen interessierten Software-Herstellern ermöglichen, in ihre Programme Import- und Exportschnittstellen für den Austausch von XJustiz-Daten einzubauen. Damit ist die Grundlage geschaffen, dass alle Beteiligten am elektronischen Rechtsverkehr effizient teilnehmen können. Der Grunddatensatz von XJustiz wurde in Fachmodulen um zusätzliche Angaben erweitert. XJustiz umfasst zurzeit 27 Fachmodule für besondere Verfahrensarten (zB Grundbuch, Ordnungswidrigkeiten, Verfahren vor Verwaltungsgerichten, Sozialgerichten, Zoll, Kommunikation mit Behörden außerhalb der Justiz usw.) und wird kontinuierlich um weitere Fachmodule erweitert.[118] Ein Anwendungsfall war der Versorgungsausgleich, bei dem XJustiz-Datensätze zusammen mit der Deutschen Rentenversicherung Bund (DRV Bund) zum Einsatz kommen.[119] Das Verfahren ist in § 229 FamFG geregelt. 100

Über die Beteiligtendaten hinaus wird auch über eine inhaltliche Strukturierung durch einen (verpflichtenden) Datensatz diskutiert, um eine automationsunterstützte Bearbeitung zu ermöglichen.[120] Auch der 70. Deutsche Juristentag hat dies 2014 gefordert.[121] Dem ist der Gesetzgeber[122] durch die Ergänzung des § 139 Abs. 1 ZPO in Ansätzen gefolgt: „Das Gericht kann durch Maßnahmen der Prozessleitung das Verfahren strukturieren und den Streitstoff abschichten." Auch eine für Reformüberlegungen eingesetzte Arbeitsgruppe der Präsidentinnen hat Konzepte gefordert. 101

d) Schriftformersatz. *aa) Qualifizierte elektronische Signatur.* Für die elektronische Kommunikation mit den Gerichten stehen verschiedene Instrumente zur Verfügung, mit denen zugleich die Schriftformerfordernisse der Prozessordnungen erfüllt werden können.[123] So können gemäß § 130a ZPO bzw. gemäß den parallelen Vorschriften in den anderen Verfahrensordnungen[124] vorbereitende Schriftsätze und deren Anlagen, schriftlich einzureichende Anträge und Erklärungen der Parteien sowie schriftlich einzureichende Auskünfte, Aussagen, Gutachten, Übersetzungen und Erklärungen Dritter als elektronische Dokumente bei Gericht eingereicht werden. Ein elektronisches Dokument muss mit einer qualifizierten elektronischen Signatur (qeS) der verantwortenden Person versehen sein **oder** von der verantwortenden Person (einfach) signiert und auf einem sicheren Übermittlungsweg eingereicht werden. Die qualifizierte elektronische Signatur hat in der elektronischen Welt denselben Wert wie die herkömmliche manuelle Unterschrift. Wirksam ist eine qualifizierte digitale Signatur nur, wenn sie von einer qualifizierten elektronischen Signaturerstellungs- 102

[118] https://xjustiz.justiz.de/, abgerufen am 16.4.2022.

[119] Ory/Weth/Viefhues, jurisPK-ERV Band 1, 1. Aufl., Kapitel 1, (Stand: 4.1.2022), Rn. 25 ff.

[120] Schnelle/Bender, DRiZ 1993, 97; Zwickel, Die digitale Strukturierung und inhaltliche Erschließung zivilprozessualer Schriftsätze im Spannungsfeld zwischen Parteiherrschaft und Richtermacht, in: Buschmann/Gläß/Gonska et al., Digitalisierung der gerichtlichen Verfahren und das Prozessrecht – 3. Tagung junger Prozessrechtswissenschaftler und -wissenschaftlerinnen am 29./30.9.2017 in Leipzig, 2018, S. 179 ff.; Effer-Uhe MDR 2019, 69;, Gaier NJW 2013, 2871, 3429, Köbler AnwBl Online 2018, 399; Vorwerk NJW 2017, 2326; Bernhardt, Structuring Judicial Communication, in: Bergener/Räckers/Stein (Hrsg.) , The Art of Structuring, 2019, S. 241 ff.

[121] Beschluss Nr. 13.

[122] Gesetz zur Regelung der Wertgrenze für die Nichtzulassungsbeschwerde in Zivilsachen, zum Ausbau der Spezialisierung bei den Gerichten sowie zur Änderung weiterer prozessrechtlicher Vorschriften vom 12.12.2019.

[123] Erläuterungen bei Meyer-Seitz AnwBl 2013, 89, 90; Brosch K&R 2014, 9, 10 f.

[124] § 55a VwGO, § 65a SGG, § 46c ArbGG, § 52a FGO oder § 32a StPO.

einheit erstellt wurde (vgl. Art. 29 und Anhang II eIDAS-Verordnung) und auf einem im Zeitpunkt ihrer Erstellung gültigen qualifizierten Zertifikat beruht, das von einem qualifizierten Vertrauensdiensteanbieter ausgestellt ist und die Anforderungen von Anhang I der eIDAS-VO erfüllt (Art. 3 Nr. 10–12, Nr. 15, Art. 28 eIDAS-VO). Während vor Inkrafttreten der eIDAS-VO auf der Basis des damals geltenden deutschen Signaturgesetzes zur Erzeugung einer qeS Chipkarten in Kombination mit der Eingabe einer individuellen PIN zu nutzen waren, können heute im Einklang mit den Vorgaben der eIDAS-VO auch Alternativen zur Chipkarte, insbesondere Fernsignaturen auf der Basis von Softwarezertifikaten zum Einsatz kommen.[125]

103 Die qualifizierte elektronische Signatur wurde erstmals flächendeckend von den Notaren genutzt, nachdem im Zuge der Einführung des elektronischen Handelsregisters die Notare verpflichtet worden waren, die Anmeldungen zum Handels-, Genossenschafts- und Partnerschaftsregister elektronisch zu übermitteln. Zur Übermittlung diente seitdem das EGVP, die Schriftform bei der Einreichung etwa der Handelsregisteranmeldungen wurde durch ein elektronisches Äquivalent ersetzt. Bei der Diskussion über die Verpflichtung der Anwälte zur Nutzung des elektronischen Rechtsverkehrs vertraten insbesondere die Anwaltsverbände die Ansicht, dass der Einsatz von Chipkarten zur Erzeugung einer qeS dem notwendigen Anwendungskomfort in der täglichen Arbeit der Anwälte und Anwältinnen entgegenstünde. Der Gesetzgeber entschloss sich daher 2013, weitere Möglichkeiten für den Schriftformersatz in den Prozessordnungen vorzusehen, um auf den Einsatz einer qeS verzichten zu können. So sieht § 130 Abs. 4 ZPO sogenannte „sichere Übermittlungswege" vor, bei deren Nutzung keine qeS, sondern eine einfache Signatur (Wiedergabe der Unterschrift der verantwortenden Person oder auch lediglich einfache Namenswiedergabe am Ende des Dokuments) als Schriftformersatz ausreicht. Die Authentizität und die Integrität des Dokuments werden dann alleine durch den gesicherten Übertragungsweg sichergestellt.

104 Bei einer Übermittlung eines Dokuments auf dem Weg über das „einfache" EGVP (also ohne Nutzung besonderer elektronischer Postfächer) kann demgegenüber nicht auf das Anbringen einer qualifizierten elektronischen Signatur abgesehen werden.[126] Ferner ist darauf hinzuweisen, dass der sichere Übermittlungsweg lediglich die verfahrensrechtlichen Schriftformanforderungen ersetzen kann, nicht aber die Schriftlichkeitserfordernisse nach materiellem Recht.[127]

105 *bb) De-Mail.* Schriftformersetzend ist die Übermittlung über **De-Mail,** sofern der Absender bei Versand der Nachricht sicher im Sinne des § 4 Abs. 1 S. 2 des De-Mail-Gesetzes angemeldet ist und er sich die sichere Anmeldung gemäß § 5 Abs. 5 des De-Mail-Gesetzes durch eine qualifizierte Signatur des De-Mail-Anbieters bestätigen lässt, § 130a Abs. 4 Nr. 1 ZPO.[128] Die wirksame Einreichung per De-Mail setzt voraus, dass die Person, deren (einfache) Signatur auf dem Dokument aufgebracht ist, mit der verantwortenden Person identisch ist.[129] Die De-Mail ist dabei der Übermittlungsweg ohne Nutzung des Elektronischen Gerichts- und Verwaltungspostfach (EGVP)als Basistechnologie.[130] Fehlt die Absenderbestätigung des Diensteanbieters, wirkt die Nutzung des De-Mail-Kontos nicht schriftformersetzend. Auch wenn die De-Mail im Gericht ausgedruckt wird, führt dies nicht zur Heilung des

[125] Explizit sehen die Erwgr. 51 und 52 der eIDAS-VO die Fernsignatur vor. Bei der Fernsignatur verbleibt die qualifizierte Signaturerstellungseinheit beim Vertrauensdiensteanbieter. Nicht die direkte Kontrolle des Unterzeichners über die Signaturerstellungseinheit, sondern technische Maßnahmen sollen Missbrauch durch Dritte verhindern. Ferner muss eine sichere Identifikation des Unterzeichners (beispielsweise über die eID des Personalausweises) gewährleistet sein. Siehe dazu Ory/Weth/Sorge, jurisPK-ERV Band 1, 1. Aufl., Kapitel 3 (Stand: 28.8.2020), Rn. 30.

[126] So etwa OVG Lüneburg 6.5.2020 – 2 LA 722/19 im Anschluss an das OVG Bautzen 16.12.2019 – 4 A 1158/19.A.

[127] Etwa §§ 550, 568, 623, 650h und 766 BGB.

[128] Parallel hierzu § 55a Abs. 4 S. 1 Nr. 1 VwGO, § 65a Abs. 4 S. 1 Nr. 1 SGG, § 46c Abs. 4 S. 1 Nr. 1 ArbGG, § 52a Abs. 4 S. 1 Nr. 1 FGO oder § 32a Abs. 4 S. 1 Nr. 1 StPO. Zu den Besonderheiten im arbeitsgerichtlichen Verfahren siehe Müller NZA 2019, 11 ff.

[129] So LSG Schleswig-Holstein 2.6.2021 – L 5 KR 230/20, BeckRS 2021, 18144. Siehe dazu auch Praxishinweise von Müller NZS 2021, 863.

[130] Ulrich/Schmieder NJW 2019, 113; Anders/Gehle/Anders, 80. Aufl. 2022, ZPO § 130a Rn. 17.

Formmangels, denn dann ist der durch die Formvorschriften des De-Mail-Weges vorgesehene Integritäts- und Authentizitätsschutz nicht gewahrt.[131] Die Nutzung der De-Mail-Kommunikationsstruktur blieb allerdings weit hinter den Erwartungen zurück. Zu erwarten ist deshalb, dass die Pflichten zur Öffnung eines De-Mail Zugangs wieder nach und nach abgeschafft werden, wie dies bereits das OZG-Änderungsgesetz vorsieht.[132]

106 *cc) Kommunikation über besondere elektronische Postfächer. (1) Besonderes elektronisches Anwaltspostfach (beA).* Gemäß § 130a Abs. 4 Nr. 2 ZPO[133] ist das **besondere elektronische Anwaltspostfach (beA) als** sicherer Übermittlungsweg festgelegt. Die Bundesrechtsanwaltskammer hat für alle Rechtsanwältinnen und Rechtsanwälte ein solches Postfach zu errichten, zu führen und einen Verzeichnisdienst besonderer elektronischer Anwaltspostfächer zu schaffen (§ 31a BRAO), wobei die Postfachadresse und die Zugangsberechtigung von der Rechtsanwaltskammer erst nach Überprüfung der Zulassung vergeben werden kann. Der Zugang zum beA darf nur über ein sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln erfolgen, § 31a Abs. 3 Satz 1 BRAO. Die Rechtsanwaltskammer hat auch Vertretern, Abwicklern und Zustellungsbevollmächtigten die Nutzung des beA zu ermöglichen, § 31a Abs. 3 Satz 2 BRAO. Auch wenn das beA bereits zum 1.1.2016 zur Verfügung stehen sollte, musste es aufgrund technischer Probleme und Zweifeln an der geforderten Sicherheit mehrfach überarbeitet werden[134] und stand faktisch erst seit 3.9.2018 zur Verfügung.

107 Seit 1.1.2018 obliegt den Anwältinnen und Anwälten die Pflicht zur „passiven" Nutzung" des beA, § 31a Abs. 6 BRAO. Demnach müssen Anwälte die für die Nutzung des beA erforderlichen technischen Einrichtungen vorhalten sowie Zustellungen und den Zugang von Mitteilungen über das beA zur Kenntnis nehmen.

108 Seit 1.1.2022 sehen die Verfahrensordnungen (fast) aller Gerichtsbarkeiten eine **aktive Nutzungspflicht für alle Rechtsanwältinnen und Rechtsanwälte** vor, also die Pflicht zur ausschließlich elektronischen Einreichung der das Verfahren betreffenden Dokumente.[135] Demnach sind vorbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen als elektronisches Dokument zu übermitteln. Nur wenn dies aus technischen Gründen vorübergehend nicht möglich ist, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, kann also auf einem beliebigen anderen prozessrechtlich vorgesehenen Wege erfolgen – per Post, Fax oder Bote, § 130d S. 2 und 3 ZPO. Die vorübergehende Unmöglichkeit muss bei der Ersatzeinreichung oder unverzüglich danach glaubhaft gemacht, auf Anforderung ein elektronisches Dokument nachgereicht werden.[136]

109 Die Störung muss „vorübergehender Natur" sein, woran es fehlt, wenn etwa das beA noch nicht in Betrieb genommen oder eingerichtet worden ist. Probleme durch Mängel in der Anwaltsbüroorganisation, etwa wenn die beA-Chipkarte nicht gefunden wird oder das beA wegen unterlassender Aktualisierung der Client Security nicht aufgerufen werden kann,

---

131 BFH NJW 2012, 334; OVG Bautzen NVwZ-RR 2016, 404; FG Köln MDR 2018, 630.

132 Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG).

133 Parallel hierzu § 55a Abs. 4 S. 1 Nr. 2 VwGO, § 65a Abs. 4 S. 1 Nr. 2 SGG, § 46c Abs. 4 S. 1 Nr. 2 ArbGG, § 52a Abs. 4 S. 1 Nr. 2 FGO oder § 32a Abs. 4 S. 1 Nr. 2StPO.

134 Heckmann/Paschke/Bernhardt/Leeb, jurisPK-Internetrecht 7.Aufl. Kap. 6, Rn. 125 ff. So wurde die zum 1.1.2016 vorgesehene Öffnung der beAs zunächst aus technischen Gründen verschoben. Sodann wurde vor dem Anwaltsgerichtshof in Berlin gerichtlich über die Frage gestritten, ob im Hinblick auf Art. 12 GG das besondere elektronische Anwaltspostfach von Anwälten ohne deren Zustimmung empfangsbereit freigeschaltet werden durfte. Anwälte vertraten die Auffassung, erst zum 1.1.2018 würde mit § 174 Abs. 3 S. 4 ZPO die Verpflichtung geschaffen einen sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen. Demgegenüber vertraten Brosch/Lummel/Sandkühler/Freiheit, Elektronischer Rechtsverkehr mit dem beA 2017, Rn. 137, zu Recht die Auffassung, dass es aus dem Gesetz keine Anhaltspunkte für eine rein freiwillig Nutzung des beA gab.

135 § 130d ZPO, § 14b FamFG, § 46g ArbGG, § 65d SGG, § 55d VwGO und § 52d FGO.

136 Zu den Anforderungen zur parallelen Rechtslage des § 46g S. 4 ArbGG (Erfordernis, die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen) im Einzelnen siehe LAG Schleswig-Holstein 13.10.2021 – 6 Sa 337/20, BeckRS 2021, 40330.

sind nicht diesen „technischen Gründen“ zuzurechnen.[137] Im Strafverfahren gilt zwar die Pflicht zur elektronischen Einreichung von Dokumenten nur eingeschränkt, § 32d StPO. Demnach „sollen“ Verteidiger und Rechtsanwälte den Strafverfolgungsbehörden und Gerichten Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen als elektronisches Dokument übermitteln. Die Berufung und ihre Begründung, die Revision, ihre Begründung und die Gegenerklärung sowie die Privatklage und die Anschlusserklärung bei der Nebenklage „müssen“ sie als elektronisches Dokument übermitteln. Wie in den anderen Verfahrensordnungen gilt, dass die Übermittlung in Papierform zulässig ist, wenn aus technischen Gründen vorübergehend eine elektronische Übermittlung nicht möglich ist, wobei die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen und auf Anforderung ein elektronisches Dokument nachzureichen ist. Werden entgegen der gesetzlichen Pflicht Schriftsätze, Anträge und Erklärungen nicht wie vorgeschrieben elektronisch eingereicht, fehlt es an der gesetzlich vorgeschriebenen Form, die Einreichungen sind also unwirksam.

110 Die einzelnen **Anforderungen an die elektronisch einzureichenden Dokumente** ergeben sich aus der ERVV[138] und den auf § 5 ERVV gestützten Veröffentlichungen der Bundesregierung im Bundesanzeiger ERVB.[139] Geregelt sind das Dateiformat, die Durchsuchbarkeit, die Einbettung von Schriftarten, der Dateinamen (keine Verwendung von Sonderzeichen mit Ausnahme von Unterstrich und Minuszeichen) und die Beifügung einer entsprechenden XML-Datei. Demnach sind die Dokumente im PDF-Format zu übersenden. Ein PDF kann durch das Dateiformat TIFF ersetzt werden, wenn bildliche Darstellungen im PDF nicht verlustfrei wiedergegeben werden können. Die frühere weitere Anforderung in § 2 Abs. 1 ERVV, dass die elektronischen Dokumente „in druckbarer, kopierbarer und, soweit technisch möglich, durchsuchbarer Form“ zu übermitteln sind, entfiel zum 1.1.2022.[140]

111 Wird ein mit einer einfachen Signatur versehenes elektronisches Dokument über das beA eines anderen Rechtsanwalts – etwa eines Kanzleikollegen – eingereicht, liegt keine wirksame Einreichung vor.[141] Bei der Versendung von Dokumenten über das beA ist zu überprüfen, ob eine automatisierte Eingangsbestätigung des Gerichts eingeht, anderenfalls muss eine erneute Übermittlung, gegebenenfalls auch auf einem anderen Übermittlungsweg, versucht werden.[142] Da die Nachrichten im beA nicht dauerhaft gespeichert werden (§ 27 RAVPV), muss auch für ihre Archivierung gesorgt werden.

112 Anwälte müssen zwar die Dokumente elektronisch einreichen, sind aber nicht zur Nutzung des beA verpflichtet. Sie können also auch die anderen schriftformersetzenden Instrumente wählen also die De-Mail oder die qualifizierte elektronische Signatur. Dazu muss dann zur Erzeugung der qeS entweder eine Signaturkarte beschafft oder eine qeS von einem qualifizierten Vertrauensdiensteanbieter[143] im Auftrag der unterzeichnenden Person erstellt werden. Hierfür muss der Rechtsanwalt im Vorfeld seine Identität gegenüber dem Vertrauensdiensteanbieter sicher nachweisen. Das qeS-Signaturzertifikat lässt sich allerdings auf die beA-Basiskarte „nachladen“.

---

[137] BeckOK ZPO § 130d, 44. Edition, Stand: 1.3.2022, Rn. 4.

[138] Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV) vom 24.11.2017 (BGBl. I S. 3803), zuletzt geändert durch Art. 6 des Gesetzes vom 5.10.2021 (BGBl. I S. 4607).

[139] Bekanntmachung zu § 5 der Elektronischer-Rechtsverkehr-Verordnung (Elektronischer-Rechtsverkehr-Bekanntmachung 2022 – ERVB 2022) vom 22.11.2021. Sehr hilfreich ist die von Möller NJW 2021, 2182 dargestellte Checkliste für das anwaltliche Vorgehen beim Versand von Dokumenten an das Gericht.

[140] Siehe die Begründung in der Bundestagsdrucksache 17/12634, Seite 25: „§ 130a Abs. 2, den die ERVV näher ausgestaltet, soll gewährleisten, dass eingereichte elektronische Dokumente für das Gericht lesbar und bearbeitungsfähig sind. Es geht jedoch nicht um eine rein formale Prüfung. Formunwirksamkeit soll nur dann eintreten, wenn der Verstoß dazu führt, dass im konkreten Fall eine Bearbeitung durch das Gericht nicht möglich ist. Demgegenüber führen rein formale Verstöße gegen die ERVV dann nicht zur Formunwirksamkeit des Eingangs, wenn das Gericht das elektronische Dokument gleichwohl bearbeiten kann“. Siehe dazu auch jurisPK-ERV/Müller Band 2, § 130a ZPO 1. Überarbeitung Rn. 90.

[141] OLG Braunschweig NJW 2019, 2176.

[142] BGH NJW 2021, 2201 BAGE 167, BAG NJW 2019, 2793 Rn. 21.

[143] Siehe Liste der Bundesnetzagentur https://www.elektronische-vertrauensdienste.de/EVD/DE/Uebersicht_eVD/start.html, abgerufen am 29.2.2024.

Praxistipp:

Besitzt der Anwalt/die Anwältin das Instrument zur Erzeugung der qeS, dann kann er damit nicht nur die prozessuale Schriftform erfüllen, sondern zusätzlich die elektronische Form des § 126a BGB wahren. Dies kann für (formbedürftige) rechtsgestaltende Erklärungen in Schriftsätzen wichtig sein; denn das BGB kennt neben der qeS keine Möglichkeit des Ersatzes der manuellen Unterschrift.

Nach Anbringen einer qualifizierten elektronischen Signatur durch den Rechtsanwalt/die Rechtsanwältin kann das Dokument auch von Kanzleimitarbeitern an das Gericht versandt werden. Allerdings dürfen zwischen Signaturerzeugung und Versand keine Veränderungen am Dokument mehr vorgenommen werden (auch nicht durch ein Kanzleiprogramm), dies würde sonst zur Ungültigkeit der qeS führen.[144]

113 *(2) Rechtsanwaltsgesellschaftspostfach (Kanzleipostfach).* Gemäß § 31b Abs. 1 BRAO (seit 1.8.2022 geltende Fassung) richtet die BRAK für jede im Gesamtverzeichnis eingetragene Berufsausübungsgesellschaft ein beA empfangsbereit ein, und zwar gemäß § 21 Abs. 1 S. 2 RAVPV in der seit 1.8.2022 geltenden Fassung unverzüglich nach der Eintragung der Berufsausübungsgesellschaft. Gemäß § 59 Abs. 1 BRAO sind die Rechtsanwaltsgesellschaften selbst prozess- und postulationsfähig; die Anerkennung des Gesellschaftspostfachs als sicherer Übermittlungsweg gem. § 130a Abs. 4 ZPO setzt allerdings voraus, dass sowohl die Postulationsfähigkeit als auch die Vertretungsbefugnis der für die Berufsausübungsgesellschaft handelnden Person für den Empfänger feststellbar sind. § 21 Abs. 3 RAVPV in der ab 1.8.2022 geltenden Fassung schreibt daher vor, dass die Berufsausübungsgesellschaft der Rechtsanwaltskammer die Familiennamen und Vornamen der vertretungsberechtigten Rechtsanwälte mitzuteilen hat, die befugt sein sollen, für die Berufsausübungsgesellschaft Dokumente mit einer nicht-qualifizierten elektronischen Signatur auf einem sicheren Übermittlungsweg zu versenden. Dies soll sicherstellen, dass die Versendung tatsächlich durch entsprechend befugte und postulationsfähige Rechtsanwältinnen und Rechtsanwälte erfolgt. Der Versand durch eine vertretungsberechtigte Person ist durch den „vertrauenswürdigen Herkunftsnachweis" (VHN) nachzuweisen, der anhand des Eintrags „sicherer Übermittlungsweg aus einem besonderen elektronischen Anwaltspostfach" auf dem Transfervermerk oder den Prüfvermerk ersichtlich ist. Nicht vertretungsberechtigte Personen müssen formbedürftige elektronische Dokumente mit einer qualifizierten elektronischen Signatur versehen.[145]

114 *(3) Besonderes elektronisches Notarpostfach.* Auf § 130a Abs. 4 Nr. 2 ZPO iVm § 78n Abs. 1 und 4 BnotO stützt sich der sichere Übermittlungsweg über das besondere **besonderes elektronisches Notarpostfach (beN).** Die Bundesnotarkammer ist demnach seit 1.1.2018 verpflichtet, für die knapp 7.000 in Deutschland im Notarverzeichnis eingetragenen Notare und Notariatsverwalter ein besonderes elektronisches Notarpostfach (beN) einzurichten. § 78n Abs. 2 BNotO verpflichtet die Bundesnotarkammer dazu, sicherzustellen, dass der Zugang zum beN nur durch ein sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln möglich ist. Auf der Basis der Verordnungsermächtigung des § 78n Abs. 5 BnotO regelt § 12 Notarverzeichnis- und -postfachverordnung (NotVPV) vom 4.3.2019 die Einzelheiten der Einrichtung und der hierzu erforderlichen Datenübermittlung, die technischen Ausgestaltung einschließlich ihrer Barrierefreiheit, der Führung, der Zugangsberechtigung und der Nutzung, des Löschens von Nachrichten und der Löschung der Notarpostfächer.[146] Demnach dient das besondere elektronische Notarpostfach der elektronischen Kommunikation der Postfachinhaber mit den Gerichten auf einem sicheren Übermittlungsweg. Zudem dient es der Kommunikation der Postfachinhaber untereinander. Gemäß § 12

[144] OLG Braunschweig NJW 2021, 1604; Möller NJW 2021, 2179.
[145] Müller NJW 2021, 3283, Rn. 15, 16. Siehe ferner Müller/Gomm jM 2021, 222.
[146] BGBl. I S. 187 zuletzt geändert durch Artikel 5 V. v. 17.12.2021 BGBl. I S. 5219.

Abs. 2 NotVPV kann das besondere elektronische Notarpostfach auch der elektronischen Kommunikation mit anderen Stellen oder Personen dienen.

115 *(4) Besonderes elektronisches Behördenpostfach (beBPo).* 130a Abs. 3 S. 1, Abs. 4 Nr. 3 ZPO sieht[147] ferner als schriftformersetzenden den Übermittlungsweg zwischen einem nach Durchführung eines Identifizierungsverfahrens **eingerichteten Postfach einer Behörde oder einer juristischen Person des öffentlichen Rechts (beBPo)** und der elektronischen Poststelle des Gerichts vor. Seit 1.1.2018 sind diese verpflichtet, einen sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen. Seit 1.1.2022 sind die Behörden und juristische Personen des öffentlichen Rechts zur Übermittlung von vorbereitenden Schriftsätzen und deren Anlagen sowie von schriftlich einzureichenden Anträgen und Erklärungen als elektronische Dokumente verpflichtet (§ 130d ZPO, § 14b FamFG, § 46g ArbGG, § 65d SGG, § 52d FGO, § 55d VwGO). In der Regel ist daher das beBPo zu nutzen. Dies gilt auch für die Kommunikation mit den Gerichtsvollziehern (§ 753 Abs. 5 ZPO).

116 Auch das beBPo beruht auf der Infrastruktur des Elektronischen Gerichts- und Verwaltungspostfachs (EGVP). Im Einzelnen finden sich weitere Detailregelungen zur Einrichtung des besonderen Postfachs einer Behörde, zur Identifizierung und zum Zugang in den §§ 6 ff. der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV). Insbesondere muss eine der zugangsberechtigten Personen im Sinne des § 8 ERVV zum Zeitpunkt der Erstellung der Nachricht sicher am beBPo angemeldet sein, sonst gilt das Dokument nicht auf sicherem Übermittlungsweg übertragen und somit ohne qualifizierte elektronische Signatur als nicht wirksam eingereicht. Ferner muss das Gericht feststellen können, dass das elektronische Dokument vom Postfachinhaber des beBPo versandt wurde (§ 6 Abs. 1 Nr. 4 ERVV), was durch die Übermittlung eines sicheren bzw. vertrauenswürdigen Herkunftsnachweises (VHN) im Sinne einer Authentizitäts- und Integritätsbescheinigung erreicht wird. Dem dient ein spezieller, automatisch erzeugter OSCI-Header und eine durch den vorher durch den Postfachinhaber in die Sendekomponenten seines beBPos eingebundene fortgeschrittene prüfbare Signatur (Transportsignatur) am „äußeren Umschlag" einer EGVP-Nachricht.[148]

117 *(5) Gerichtsvollzieher.* Für die Kommunikation mit den Gerichtsvollziehern gilt: Schriftlich einzureichende Anträge und Erklärungen der Parteien sowie schriftlich einzureichende Auskünfte, Aussagen, Gutachten, Übersetzungen und Erklärungen Dritter können als elektronisches Dokument beim Gerichtsvollzieher eingereicht werden., § 753 Abs. 4 ZPO. Die Bundesregierung kann in einer Rechtsverordnung besondere technische Rahmenbedingungen für die Übermittlung und Bearbeitung elektronischer Dokumente in Zwangsvollstreckungsverfahren durch Gerichtsvollzieher bestimmen (§ 753 Abs. 4 S. 3 ZPO). Seit 1.1.2022 können Rechtsanwälte, Behörden oder juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse Vollstreckungsaufträge an die Gerichtsvollzieherinnen und Gerichtsvollziehern seit 1.1.2022 nur noch auf elektronischem Weg einreichen.

118 *(6) Besonderes elektronisches Steuerberaterpostfach (beSt).* Das besonderes elektronische Steuerberaterpostfach ist in § 52a Abs. 4 Nr. 2 FGO geregelt („der Übermittlungsweg zwischen dem besonderen elektronischen Anwaltspostfach nach § 31a der Bundesrechtsanwaltsordnung *oder einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach* und der elektronischen Poststelle des Gerichts). Gemäß § 86d StBerG in der ab 1.8.2022 geltenden Fassung richtet die Bundessteuerberaterkammer über die Steuerberaterplattform für jeden Steuerberater und Steuerbevollmächtigten ein besonderes elektronisches Steuerberaterpostfach empfangsbereit ein. Sie hat auch Vertretern, Praxisabwicklern, Praxistreuhändern und Zustellungsbevollmächtigten die Nutzung des besonderen elektronischen Steuerberaterpostfachs zu ermöglichen und kann unterschiedlich ausgestaltete Zu-

[147] Parallele Regelungen in § 55a Abs. 3 S. 1, Abs. 4 Nr. 3 VwGO, § 65a Abs. 3 S. 1, Abs. 4 Nr. 3 SGG, § 46c Abs. 3 S. 1, Abs. 4 Nr. 3 ArbGG, § 52a Abs. 3 S. 1, Abs. 4 Nr. 3 FGO und § 32a Abs. 3, Abs. 4 Nr. 3 StPO.

[148] OVG Bremen 22.4.2020 – 2 LA 317/19, BeckRS 2020, 8066, Rn. 8.

gangsberechtigungen für Kammermitglieder und andere Personen vorsehen. Gemäß § 86d Abs. 6 StBerG ist der Inhaber des besonderen elektronischen Steuerberaterpostfachs verpflichtet, die für dessen Nutzung erforderlichen technischen Einrichtungen vorzuhalten sowie Zustellungen und den Zugang von Mitteilungen über das besondere elektronische Steuerberaterpostfach zur Kenntnis zu nehmen. Gem. § 157e StBerG in der ab 1.8.2022 geltenden Fassung sind die neuen Regelungen zur Steuerberaterplattform ab 31.12.2022 anwendbar. Eine „aktive Nutzungspflicht", also die Pflicht der Steuerberater, ausschließlich elektronisch mit den Gerichten zu nutzen, besteht gemäß § 52d S. 2 FGO iVm § 52a Abs. 4 S. 1 Nr. 2 ab dem Zeitpunkt der tatsächlichen Zurverfügungstellung des beSt durch die Bundessteuerberaterkammer, also ab 1.1.2023.

(7) Besonderes elektronisches Bürger- und Organisationenpostfach (eBO). Als sicherer (und damit schriftformersetzend) gilt auch der Übermittlungsweg zwischen einem nach Durchführung eines Identifizierungsverfahrens eingerichteten elektronischen Postfach einer natürlichen oder juristischen Person oder einer sonstigen Vereinigung und der elektronischen Poststelle des Gerichts.[149] Die am 1.1.2022 in Kraft getretene Regelung sieht somit die Einrichtung eines **besonderen elektronischen Bürger- und Organisationenpostfach (eBO)** vor, über das Bürgerinnen, Bürger und Organisationen sicher und zuverlässig mit der Justiz elektronisch kommunizieren können: Anträge können schriftformersetzend durch die Postfachinhaber an die Gerichte versandt und die Zustellung von elektronischen Dokumenten an die jeweiligen Postfachinhaber bewirkt werden.[150] Der sichere Übermittlungsweg steht aber auch für nicht formbedürftige Nachrichten etwa zwischen Anwaltschaft und Mandantschaft zur Verfügung. Freigeschaltet wird das Postfach gemäß § 11 Abs. 1 ERVV durch eine Landesbehörde, nachdem der Postfachinhaber gem. § 11 Abs. 2 ERVV durch die eID gem. § 18 des Personalausweisgesetzes, § 12 des eID-Karte-Gesetzes oder § 78 Abs. 5 des Aufenthaltsgesetzes, durch ein qualifiziertes elektronisches Siegel oder ein Identifizierungsverfahren bei einem Notar identifiziert ist. Die Länder sind gemäß § 11 Abs. 1 ERVV verpflichtet, öffentlich-rechtliche Stellen zu benennen, um nach der Prüfung der Identität des Postfachinhabers die Freischaltung des Postfachs vorzunehmen. **119**

(8) Kommunikation über Nutzerkonto des Portalverbundes. Schließlich können auch die nach § 2 Onlinezugangsgesetz (OZG) zu errichtenden Nutzerkonten des Verwaltungsportalverbundes in die Kommunikation mit den Gerichten eingebunden werden: Insoweit sieht der neue § 130a Abs. 4 Nr. 5 ZPO als schriftformersetzend den Übermittlungsweg zwischen einem nach Durchführung eines Identifizierungsverfahrens genutzten Postfach- und Versanddienst eines Nutzerkontos im Sinne des § 2 Abs. 5 des Onlinezugangsgesetzes und der elektronischen Poststelle des Gerichts vor.[151] **120**

So hat das Bundesministerium der Justiz ein von Bürgerinnen und Bürgern im Rahmen des Portalverbundes nach dem OZG nutzare **„Mein Justizpostfach"** im Pilotbetrieb gestartet, das eine verschlüsselte Kommunikation im Sinne eines sicheren Übermittlungsweg (§ 130a Abs. 3 S. 1 ZPO) ermöglicht, und zwar mit der Justiz sowie mit Behörden, Anwälten, Notaren und Steuerberatern. Vor der Einrichtung ist ein Nutzerkonto im Portalverbund mithilfe der BundID zu eröffnen.[152] **121**

(9) Kommunikation über Onlineformulare und Authentifizierung/Identifizierung mithilfe elektronischer ID. Seit dem 1.7.2014 können auf der Basis einer Rechtsverordnung des Bundesministeriums der Justiz (mit Zustimmung des Bundesrats) **Onlineformulare** ausgefüllt und mithilfe der eID-Funktion des Personalausweises (und mittlerweile der Unionsbürgerkarte gem. § 12 des eID-Karte-Gesetzes oder des elektronischen Aufenthaltstitels gem. **122**

[149] § 130a Abs. 4 Nr. 4 ZPO, § 55a Abs. 4 Nr. 4 VwGO, § 46c Abs. 4 Nr. 4 ArbGG, § 65a Abs. 4 Nr. 4 SGG, § 52a Abs. 4 Nr. 4 FGO, § 32a Abs. 4 Nr. 4 StPO, jeweils iVm §§ 10, 11, 12 ERVV in der jeweils ab dem 1.1.2022 gültigen Fassung.

[150] Weitere Erläuterungen bei jurisPK-ERV/Müller Band 2, § 130a ZPO 1. Überarbeitung Rn. 227.

[151] Parallele Regelungen in § 55a Abs. 3 S. 1, Abs. 4 Nr. 5 VwGO, § 65a Abs. 3 S. 1, Abs. 4 Nr. 5 SGG, § 46c Abs. 3 S. 1, Abs. 4 Nr. 5 ArbGG, § 52a Abs. 3 S. 1, Abs. 4 Nr. 5 FGO und § 32a Abs. 3, Abs. 4 Nr. 5 StPO.

[152] https://id.bund.de/.

§ 78 Absatz 5 des Aufenthaltsgesetzes authentifiziert und schriftformersetzend an die Gerichte übermittelt werden (§ 130c Satz 4 ZPO, § 130a Abs. 3 ZPO).[153]

123 *(10) Sonderproblem: Nutzung des Telefax.* Gemäß § 130 Nr. 6 ZPO soll der vorbereitende Schriftsatz die Unterschrift desjenigen tragen, der den Schriftsatz verantwortet, bei Übermittlung durch einen Telefaxdienst (Telekopie) die Wiedergabe der Unterschrift in der Kopie. Nach einer Entscheidung des gemeinsamen Senats der obersten Gerichtshöfe[154] können auch mittels Computerfax bestimmende Schriftsätze wirksam übermittelt werden. Dies setzt allerdings voraus, dass das Computerfax mit eingescannter Unterschrift des Prozessbevollmächtigten versandt wird. Ein Computerfax unterfällt allerdings nicht dem § 130a ZPO, also der dort geregelten elektronischen Übermittlung, weil es die dort genannten Voraussetzungen nicht erfüllt, vielmehr (erst) durch den Ausdruck beim Empfänger den Charakter eines Schriftstücks erhält.[155] Nach Inkrafttreten der Pflicht zur Nutzung des elektronischen Rechtsverkehrs durch die professionellen Einreicher seit 1.1.2022 ist die Übermittlung von Schriftsätzen als Telefax ist im Grundsatz nur noch durch nicht anwaltlich vertretene Personen möglich. Für professionelle Einreicher, die der Pflicht zur elektronischen Einreichung unterliegen, kommt das Telefax nur dann in Betracht, wenn der Fall des § 130d S. 2 ZPO vorliegt, also bei einer vorübergehenden Unmöglichkeit der elektronischen Übersendung. Unterdimensionierte Internetanschlüsse sind jedoch nicht mit einer vorübergehenden Unmöglichkeit gleichzusetzen. Im Extremfall ist an eine Verlegung des Kanzleistandorts oder durch kostenintensive Investitionen zu denken.[156] Insgesamt ist die Sicherheit der Dokumentenübermittlung mithilfe eines Telefaxes gegenüber der elektronischen Übermittlung mithilfe eines qeS unterzeichneten Dokuments oder auf einem sicheren Übermittlungsweg unterlegen.

124 e) **Eingang und Form des elektronischen Dokuments.** § 130a Abs. 5 ZPO[157] definiert den Zeitpunkt des Eingangs eines elektronischen Dokuments: Es kommt darauf an, dass es auf der für den Empfang bestimmten Einrichtung des Gerichts gespeichert ist. Dem Absender ist eine automatisierte Bestätigung über den Zeitpunkt des Eingangs zu erteilen. Sofern ein elektronisches Dokument für das Gericht zur Bearbeitung nicht geeignet ist, obliegt es dem Gericht, dies dem Absender unter Hinweis auf die Unwirksamkeit des Eingangs unverzüglich mitzuteilen. Das Dokument gilt als zum Zeitpunkt der früheren Einreichung eingegangen, sofern der Absender es unverzüglich in einer für das Gericht zur Bearbeitung geeigneten Form nachreicht und glaubhaft macht, dass es mit dem zuerst eingereichten Dokument inhaltlich übereinstimmt (§ 130a Abs. 6 ZPO).[158]

125 Formunwirksamkeit soll nur dann eintreten, wenn der Verstoß dazu führt, dass im konkreten Fall eine Bearbeitung durch das Gericht nicht möglich ist. Demgegenüber führen rein formale Verstöße gegen die ERVV dann nicht zur Formunwirksamkeit des Eingangs, wenn das Gericht das elektronische Dokument gleichwohl bearbeiten kann.

126 f) **Zustellungsfragen.** Das Recht der **elektronischen Zustellung** wurde durch das Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer prozessrechtlicher Vorschriften geändert. Nunmehr gilt gemäß § 173 Abs. 2 ZPO Folgendes: Eine elektronische Zustellung durch ein Gericht setzt voraus, dass ein „sicherer Übermittlungsweg" zur Verfügung steht.

127 Eine unbedingte **Pflicht zur Eröffnung eines sicheren Übermittelungsweges** („haben einen sicheren Übermittlungsweg für die elektronische Zustellung eines elektronischen Doku-

[153] Parallele Regelungen in § 55c VwGO, § 65c SGG, § 46f ArbGG, § 52c FGO und § 32c StPO.

[154] GmS-OGB v. 5.4.2000 – GmS-OGB 1/98, NJW 2000, 2340.

[155] Zur parallelen Regelung in § 55a VwGO: BVerwGE 143, 50, 53 f.; Sodan/Ziekow, VwGO, 5. Auflage 2018, § 60 Rn 92 Baumbach/Lauterbach/Albers/Hartmann ZPO § 130a Rn. 4.

[156] Salz, Der elektronische Rechtsverkehr am Beispiel des elektronischen Gerichts- und Verwaltungspostfachs, 2019, S. 167.

[157] Parallele Regelungen in § 55a Abs. 5 VwGO, § 65a Abs. 5 SGG, § 46c Abs. 5 ArbGG, § 52a Abs. 5 FGO und § 32a Abs. 5 StPO.

[158] Parallele Regelungen in § 55a Abs. 6 VwGO, § 65a Abs. 6 SGG, § 46c Abs. 6 ArbGG, § 52a Abs. 6 FGO und § 32a Abs. 6 StPO.

ments zu eröffnen“) trifft **Rechtsanwälte, Notare, Gerichtsvollzieher sowie Behörden, Körperschaften oder Anstalten des öffentlichen Rechts.** Demgegenüber „sollen“ Steuerberater sowie sonstige in professioneller Eigenschaft am Prozess beteiligte Personen, Vereinigungen und Organisationen, bei denen von einer erhöhten Zuverlässigkeit ausgegangen werden kann, einen sicheren Übermittlungsweg für die elektronische Zustellung eröffnen. Die Formulierung deutet auf eine weniger stringente Verpflichtung des zuletzt genannten Personenkreises zur Eröffnung eines sicheren Übermittlungsweges hin. Allerdings gilt ab 1.1.2024 für diesen Personen- und Institutionenkreis gemäß der dann geltenden Fassung des § 173 Abs. 2 ZPO ebenfalls die striktere Fassung („haben… zu eröffnen“). Für den gesamten genannten Personenkreis wird die elektronische Zustellung durch ein elektronisches Empfangsbekenntnis nachgewiesen, das an das Gericht zu übermitteln ist, wobei für die Übermittlung der vom Gericht mit der Zustellung zur Verfügung gestellte Datensatz zu verwenden ist.[159] Stellt demgegenüber das Gericht keinen strukturierten Datensatz zur Verfügung, so ist dem Gericht das elektronische Empfangsbekenntnis als elektronisches Dokument (§ 130a ZPO) zu übermitteln. Es ist daher entweder qualifiziert elektronisch zu signieren oder auf einem sicheren Übermittlungsweg dem Gericht zu übersenden.

Nehmen am elektronischen Rechtsverkehr **nicht in professioneller Eigenschaft am Prozess beteiligte Personen, Vereinigungen und Organisationen** teil, so kann an diese ein elektronisches Dokument zugestellt werden, sofern sie der Zustellung *für das jeweilige Verfahren* zugestimmt haben. Konkludent gilt die Zustimmung hierzu erteilt, wenn die Nutzer des elektronischen Rechtsverkehrs ein elektronisches Dokument im jeweiligen Verfahren auf einem sicheren Übermittlungsweg eingereicht haben. Andere als natürliche Personen können die Zustimmung auch allgemein erteilen, also nicht nur für ein bestimmtes Verfahren. Bei den privaten Nutzern (also Verfahrensbeteiligte, die nicht zum Kreis der Privilegierten gem. § 173 Abs. 2 ZPO) gehören, gilt im Gegensatz zu den professionellen Einreichern, bei denen es auf die Rücksendung des Empfangsbekenntnisses ankommt, ein elektronisches Dokument am dritten Tag nach dem auf der automatisierten Eingangsbestätigung ausgewiesenen Tag des Eingangs in dem vom eröffneten elektronischen Postfach als zugestellt (Zustellungsfiktion), es sei denn, es wird nachgewiesen, dass das Dokument nicht oder zu einem späteren Zeitpunkt zugegangen ist.“ Deutlich wird hier, dass für diesen Adressatenkreis einer elektronischen Zustellung das „gewillkürte“ Element eines zurück zu versendenden Empfangsbekenntnisses nicht vorgesehen ist, vielmehr die Zugangsfiktion. Das beA kann auch für die Zustellung von Anwalt zu Anwalt gem. § 195 ZPO genutzt werden. 128

Durch den neuen § 193 Abs. 2 ZPO ist nun klarstellt, dass das Dokument dem **Gerichtsvollzieher** entweder in Papier mit den Abschriften übergeben oder auf elektronischem Wege übermittelt werden kann und der Gerichtsvollzieher dann die zuzustellenden Abschriften beglaubigt, wobei der die Beurkundung auf einem Ausdruck des zuzustellenden elektronischen Dokuments oder auf dem mit dem Ausdruck zu verbindenden hierfür vorgesehenen Formular vornimmt. 129

§ 193a ZPO regelt die Zustellung elektronischer Dokumente **durch den Gerichtsvollzieher.** Das zuzustellende Schriftstück kann dem Gerichtsvollzieher elektronisch oder als Schriftstück übermittelt werden. Der Gerichtsvollzieher Papierdokumente in ein elektronisches Dokument. Gemäß Satz 1 gilt als Zustellungsnachweis allein die automatisierte Eingangsbestätigung durch den Empfänger, also nicht das elektronische Empfangsbekenntnis und keine Drei-Tages-Fiktion. Damit soll eine effektive Zwangsvollstreckung sichergestellt und nicht von einer Handlung des Empfängers abhängig gemacht werden. Stellt also der Gerichtsvollzieher gem. § 193a ZPO elektronisch an einen Anwalt oder eine Anwältin zu, so entfällt das voluntative Element des Empfangsbekenntnisses. 130

§ 50 Abs. 2 ArbGG verweist für das **arbeitsgerichtliche Verfahren** auf die §§ 173, 175, 178 ZPO mit der Maßgabe, dass diese Vorschriften auf die nach § 11 ArbGG zur Prozessvertretung zugelassenen Personen entsprechend anzuwenden sind. Die Verbandsvertreter sind daher auch bei der Zustellung Rechtsanwälten gleichgestellt, sofern die vertretende 131

[159] Siehe zur Handhabung des elektronischen Empfangsbekenntnisses Biallaß NJW 2019, 3495 ff.

Partei Mitglied der Gewerkschaft/des Arbeitgeberverbandes ist. Allerdings kommt § 195 ZPO (Zustellung von Anwalt zu Anwalt) nicht bei Verbandsvertretern zur Anwendung.[160]

132 **g) Einsatz des qualifizierten elektronischen Siegels.** „Elektronische Siegel sind in Art. 3 Nr. 25 eIDAS-Verordnung definiert als „Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen." Da im Gegensatz zur elektronischen Signatur das Siegel nicht einer natürlichen Person zugeordnet wird, ist es insbesondere für juristische Personen anwendbar. Bis zum Inkrafttreten des Artikel 38 eIDAS-Verordnung[161] war das elektronische Siegel im deutschen Recht noch nicht verankert. Nunmehr könnte das qualifizierte elektronische Siegel dann zum Einsatz gelangen, wenn andernfalls die persönliche qualifizierte elektronischen Signatur eines Mitarbeiters zu nutzen wäre, auch wenn dieser nur in Vertretung der juristischen Person gehandelt hat und damit ein Eingriff in das informationelle Selbstbestimmungsrecht des Mitarbeiters verbunden ist. Aus dem eIDAS-Durchführungsgesetz lassen sich keine konkreten Regelungen zum Einsatz eines qualifizierten elektronischen Siegels entnehmen. Diese bedürfen vielmehr einer konkreten fachlichen Regelung. Nunmehr regelt § 11 Abs. 2 Nr. 2 ERVV, dass ein qualifiziertes elektronisches Siegel nach Artikel 38 eIDAS Verordnung als alternatives Identifizierungsmittel des Postfachinhabers für ein besonderes elektronisches Bürger- und Organisationenpostfach angewandt werden kann.

133 **h) Besondere Aspekte des elektronischen Rechtsverkehrs in den einzelnen Verfahrensordnungen.** *aa) Zivilgerichtsbarkeit: Mahnverfahren.* Aus der Strukturierung des Mahnverfahrens folgt die besondere Eignung für eine elektronische Durchführung. Das Bundesministerium der Justiz kann in einer Verordnung mit Zustimmung des Bundesrats maschinell bearbeitbare Formulare nach § 703c Abs. 1 S. 2 Nr. 1 ZPO einführen. Rechtsanwälte, registrierte Person nach § 10 Abs. 1 S. 1 Nr. 1 RDG, Behörden oder juristische Personen des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse sind verpflichtet, die Anträge mit dem Formular in maschinell bearbeitbarer Form zu übermitteln. Nicht anwaltlich vertretene Personen können Anträge und Erklärungen unter Nutzung des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, § 12 des eID-Karte-Gesetzes oder § 78 Abs. 5 des Aufenthaltsgesetzes stellen, einer handschriftlichen Unterzeichnung bedarf es nicht.

134 Stellt ein professioneller Justizanwender den Mahnantrag nicht in einer zur Bearbeitung zugelassenen Form, muss das Gericht ihn in entsprechender Anwendung des § 130a Abs. 6 S. 1 ZPO unverzüglich auf diesen Umstand und die geltenden technischen Rahmenbedingungen hinzuweisen. Zuständiges Mahngericht ist gem. § 689 Abs. 2 S. 1 ZPO grundsätzlich das Amtsgericht, bei dem der Antragsteller seinen allgemeinen Gerichtsstand hat. Hat der Antragsteller keinen allgemeinen Gerichtsstand im Inland, so ist das Amtsgericht Berlin-Wedding ausschließlich zuständig. Sämtliche Bundesländer haben von der Ermächtigung des § 689 Abs. 3 S. 1 und 2 ZPO Gebrauch gemacht und zentrale Mahngerichte eingerichtet bzw. die Möglichkeit des § 689 Abs. 3 S. 4 ZPO genutzt, dass mehrere Bundesländer sich auf ein gemeinsames Mahngericht verständigen:

- Sachsen, Sachsen-Anhalt und Thüringen: AG Aschersleben,
- Bremen: AG Bremen,
- Bayern: AG Coburg,
- NRW, OLG Bezirk Köln: AG Euskirchen,
- NRW, OLG-Bezirke Hamm und Düsseldorf: AG Hagen,
- Mecklenburg-Vorpommern und Hamburg: AG Hamburg-Altona,
- Hessen: AG Hünfeld,
- Rheinland-Pfalz und Saarland: AG Mayen,

[160] BeckOK ArbR, Hrsg. Rolfs/Giesen/Meßling/Udsching, 63. Edition, Stand: 1.3.2022, Rn. 34.

[161] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23.7.2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44).

- Schleswig-Holstein: AG Schleswig,
- Baden-Württemberg: AG Stuttgart,
- Niedersachsen: AG Uelzen,
- Berlin, Brandenburg, Antragsteller aus dem Ausland: AG Wedding.

bb) Verwaltungsgerichtbarkeit. (1) Allgemein. Seit 1.1.2018 ist der elektronische Rechtsverkehr flächendeckend zu allen Verwaltungsgerichten in Deutschland eröffnet, § 55a Abs. 1 VwGO. Das bedeutet, dass die vorbereitenden Schriftsätze und deren Anlagen, schriftlich einzureichenden Anträgen und Erklärungen der Beteiligten sowie schriftlich einzureichende Auskünfte, Aussagen, Gutachten, Übersetzungen und Erklärungen Dritter elektronisch eingereicht werden können. Gemäß § 55a Abs. 2 VwGO muss das elektronische Dokument für das Gericht lesbar und bearbeitungsfähig ist. Die Details ergeben sich aus der Elektronischer-Rechtsverkehr-Verordnung (ERVV). Parallel zur ZPO bestimmt 55a Abs. 3, Abs. 4 VwGO wiederum die Schriftersatzmöglichkeiten. Ferner können elektronische Formulare – sofern sie durch eine Rechtsverordnung des Bundesministeriums der Justiz mit Zustimmung des Bundesrates bestimmt wurden – durch Nutzung des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, § 12 des eID-Karte-Gesetzes oder § 78 Abs. 5 des Aufenthaltsgesetzes schriftformersetzend beim Verwaltungsgericht eingereicht werden.[162] Sofern keine Schriftform vorgeschrieben ist, besteht Formfreiheit und eine einfache elektronische Signatur reicht aus. Seit dem 1.1.2022 schreibt § 55d VwGO vor, dass vorbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, als elektronische Dokumente dem Gericht zu übermitteln sind. Ist eine Übermittlung aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen. Gemäß § 55a Abs. 5 S. 2 VwGO ist dem Absender zum Nachweis des Zugangs eine automatisierte Eingangsbestätigung zu erteilen. **135**

§ 56 VwGO regelt, welche gerichtlichen Verfügungen und Entscheidungen im verwaltungsgerichtlichen Verfahren **zugestellt** werden müssen (Abs. 1) und durch Verweisung auf die Vorschriften der ZPO in Abs. 2 , in welcher Form dies zu geschehen hat. Da diese Verweisung dynamisch ist gelten die Neuregelungen der ZPO im Zustellungsrecht automatisch auch für die Zustellungen der VwGO. **136**

(2) Gerichtliche elektronische Dokumente (§ 55a Abs. 7 VwGO). Soweit eine handschriftliche Unterzeichnung durch den Richter oder den Urkundsbeamten der Geschäftsstelle vorgeschrieben ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn die verantwortenden Personen am Ende des Dokuments ihren Namen hinzufügen und das Dokument mit einer qualifizierten elektronischen Signatur versehen. Dies betrifft gerichtliche Protokolle, Beschlüsse und Urteile.[163] Für die Entscheidung eines Kollegialgerichts bedeutet dies, dass alle Richterinnen und Richter ihre Namen sowie ihre qualifizierte elektronische Signatur unter das Dokument setzen müssen. Bei Verhinderung eines Richters, hat der Vorsitzende oder – bei dessen Verhinderung – der dienstälteste Richter, der bei der Entscheidung mitgewirkt hat, den Hinderungsgrund und den Namen des verhinderten Richters auf dem elektronischen Dokument zu vermerken.[164] **137**

Fehlt eine qualifizierte elektronische Signatur bzw. entspricht sie nicht den Anforderungen der eIDAS-Verordnung, dann ist die Entscheidung unwirksam; der Formmangel kann jedoch durch Berichtung analog § 118 VwGO geheilt werden.[165] **138**

[162] § 55c S. 4 VwGO.
[163] BeckOK VwGO/Schmitz, 60. Ed. 1.1.2022, VwGO § 55a Rn. 29.
[164] BeckOK VwGO/Schmitz, 60. Edition, § 55a VWGO Rn. 29.
[165] BeckOK VwGO/Schmitz, 60. Edition, § 55a VWGO Rn. 30.

139 *(3) Widerspruchsverfahren.* Für das Widerspruchsverfahren im Vorfeld eines verwaltungsgerichtlichen Verfahrens regelt § 70 VwGO, dass die „elektronischer Form nach § 3a Abs. 2 des Verwaltungsverfahrensgesetzes" zulässig ist. Dafür müsste aber die Behörde einen elektronischen Zugang eröffnet haben. Die (Landes-)EGovG sehen jedoch teilweise unterschiedliche Fristen zur verpflichtenden Eröffnung elektronischer Verfahren vor, die teilweise bis 2026 reichen. Die Zugangseröffnung erfolgt durch Widmung (Signalisierung der Bereitschaft zum elektronischen Rechtsverkehr auf einem bestimmten bereitgestellten Kommunikationsweg gegenüber einem potenziellen Kommunikationspartner), die auch konkludent möglich ist.[166]

140 Das beA kann unter Verzicht auf die qeS nicht für eine schriftformwahrenden Widerspruch genutzt werden. Auch gemäß § 36a Abs. 2 S. 1 SGB ist ein elektronisch eingereichter Widerspruch nur formwirksam, wenn der Empfänger –die Behörde – hierfür einen Zugang eröffnet hat und die E-Mail gemäß § 36a Abs. 2 S. 1 SGB I mit einer qualifizierten elektronischen Signatur gem. Art 3 Nr. 12 eIDAS-VO versehen ist.[167]

141 *cc) Elektronischer Rechtsverkehr bei der Strafverfolgung und in der Strafgerichtsbarkeit.* Durch das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs wurden die §§ 32-32f StPO eingefügt und damit der bis dahin geltende § 41a StPO abgelöst, der den elektronischen Rechtsverkehr nur rudimentär regelte. Nunmehr sind die Regelungen des elektronischen Rechtsverkehrs weitgehend an die anderen Verfahrensordnungen angepasst. Gemäß § 32d S. 1 StPO „sollen" Verteidiger und Rechtsanwälte seit 1.1.2022 den Strafverfolgungsbehörden und Gerichten Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen als elektronisches Dokument übermitteln. Demgegenüber *müssen* bestimmte prozessgestaltende Erklärungen wie Berufung und Revision nebst deren Begründung und Gegenerklärung ebenso wie Privatklagen und Anschlusserklärungen bei der Nebenklage elektronisch übermittelt werden., § 32d S. 2 StPO.[168]

4. Elektronische Aktenführung

142 **a) Allgemeines.** Gemäß § 298a Abs. 1 S. 2 ZPO, § 46e ArbGG, § 55b VwGO, § 52b FGO und § 65b SGG bestimmen bis zum 31.12.2025 die Bundesregierung und die Landesregierungen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Akten geführt werden, sowie die hierfür geltenden organisatorisch-technischen Rahmenbedingungen für die Bildung, Führung und Aufbewahrung der elektronischen Akten sowie die Übertragung von Papierdokumenten in die elektronische Form. Wird die dargestellte Möglichkeit einer Zulassungsbeschränkung auf einzelne Gerichte oder Verfahren wahrgenommen, kann zudem in der Rechtsverordnung bestimmt werden, dass durch öffentlich bekanntgemachte Verwaltungsvorschrift geregelt wird, in welchen Verfahren die Akten elektronisch zu führen sind. Ab dem 1.1.2026 ist gemäß § 298a Abs. 1a ZPO die Einführung elektronischer Gerichtsakten kraft Gesetzes vorgeschrieben.[169] Mittlerweile haben in praktisch allen Bundesländern Gerichte den „digitalen" Schalter von der führenden Papierakte zur elektronischen Akte umgelegt.[170] In der Ziviljustiz kommen im Wesentlichen drei Gerichtsaktensysteme zum Einsatz, für die sich jeweils mehrere Länder entschieden haben.[171]

---

[166] Müller NJW 2021, 3281, Rn. 8, 9.

[167] SG Darmstadt 22.9.2021 – S 33 AS 252/21; siehe auch Müller NJW2021, 3281, 3282.

[168] Diese Differenzierung wird in der Literatur teilweise kritisiert, weil sie sich nicht ausschließlich auf die Besonderheiten des Strafverfahrens stützen könne, etwa Werner jM 2016, 387, 389.

[169] Parallele Regelungen in § 46e Abs. 1a ArbGG, § 55b Abs. 1a VwGO, § 52b Abs. 1a FGO und § 65b Abs. 1a SGG.

[170] Bernhardt JM 2022, 90 f. Siehe im Einzelnen Heckmann/Paschke/Bernhardt/Leeb jurisPK Internetrecht, 7. Aufl., Rn. 170 ff.

[171] Der „e2-Verbund" (ergonomisch-elektronisch) mit den Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Saarland und Sachsen-Anhalt sowie dem Bundesarbeitsgericht als justizspezifische Eigenentwicklung des Unternehmens SINC GmbH mit den Komponenten elektronischer Arbeitsplatz (e^2A) Textsystem (e^2T), Posteingangs- und Postausgangsmanagement (e^2P) sowie Saalanzeige- und -managementsystem (e^2S)

Ab dem Zeitpunkt der Einführung der elektronischen Akte sind eingehende Papierdokumente gemäß § 298a Abs. 2 ZPO[172] in elektronische Dokumente zu übertragen. Das Übertragungsverfahren hat dem Stand der Technik zu entsprechen, die bildliche und inhaltliche Übereinstimmung muss sichergestellt und dokumentiert werden. Ausweislich der Begründung zum Gesetzentwurf sind „technisch bedingte Abweichungen in Größe und Farbe hinzunehmen, soweit sie den Inhalt des Papierdokuments nicht beeinträchtigen".[173] Die früher vorgesehene Bestätigung jeder einzelnen Übertragung bzw. der frühere vorgesehen Vermerk, wann und durch wen ein Schriftstück in ein elektronisches Dokument übertragen worden ist, sind nicht mehr geboten. **143**

Wird die Akte weiterhin als Papierakte geführt, sind gemäß § 298 ZPO die elektronischen Dokumente auszudrucken. Unzulässig im Grundsatz ist eine Hybridakte, also eine Akte, die teilweise in Papierform und teilweise in elektronischer Form geführt wird. Ausnahmsweise kann gemäß § 298 Abs. 1 S. 2 ZPO auf den Ausdruck umfangreicher Anlagen verzichtet werden, wenn der zu erwartende Aufwand im Vergleich zur Vollständigkeit der Akte außerhalb jedes angemessenen Verhältnisses steht. In einem solchen Fall ist die Datei ohne Ausdruck dauerhaft zu speichern, der Speicherort ist in einem ausgedruckten Vermerk festzuhalten, um die Vollständigkeit der Papierakte sicherzustellen, § 298 Abs. 1 S. 3 ZPO. Ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen und nicht auf einem sicheren Übermittlungsweg eingereicht worden, muss der Ausdruck mit einem Transfervermerk gemäß § 298 Abs. 4 ZPO, also mit einer qualifizierten elektronischen Signatur des Urkundsbeamten der Geschäftsstelle versehen werden, um auf diese Weise zu dokumentieren, dass das Dokument einen wirksamen Schriftformersatz enthielt.[174] Das kommt etwa bei von Bereitschafts- oder ehrenamtlichen Richtern unterzeichnete Entscheidungen in Betracht. Wenn das Dokument auf einem sicheren Übermittlungsweg im Sinne des § 130a Abs. 4 ZPO eingereicht wurde, muss dies aktenkundig gemacht werden, § 298 Abs. 3 ZPO.[175] **144**

b) Akteneinsicht. § 299 Abs. 3 ZPO[176] regelt die Akteneinsicht bei elektronischer Aktenführung. Ähnliche Regelungen sieht § 760 ZPO für die Einsicht in elektronisch geführte Akten des Gerichtsvollziehers vor, weitere gleichgelagerte Regelungen finden sich in den § 100 VwGO, § 78 FGO und § 120 SGG. Im arbeitsgerichtlichen Verfahren ist § 299 Abs. 3 ZPO über § 46 Abs. 2 ArbGG anwendbar. **145**

Prinzipiell gewährt die Geschäftsstelle Akteneinsicht durch Bereitstellung des Inhalts der Akten zum Abruf oder durch Übermittlung des Inhalts der Akten auf einem sicheren Übermittlungsweg, also bei Rechtsanwälten über das besondere elektronische Anwaltspostfach (beA). Nur auf besonderen Antrag wird Akteneinsicht durch Einsichtnahme in die Akten in Diensträumen gewährt. Schließlich werden ein Aktenausdruck oder ein Datenträger mit dem Inhalt der Akte auf besonders zu begründenden Antrag nur dann übermittelt, wenn der Antragsteller hieran ein berechtigtes Interesse darlegt; denn dieser „konventionelle" durch Medienbruch gekennzeichnete Weg verursacht zusätzlichen Aufwand und Kosten. Ein besonderes Interesse könnte etwa darin bestehen, dass der Antragsteller nicht über die techni- **146**

(siehe dazu Schürger/Kersting in: Viefhues, Elektronischer Rechtsverkehr, Ausgabe 2/2016, Rn. 52 ff.). Sodann das im Rahmen des ForumSTAR-Verbunds von Bayern (federführend), Rheinland-Pfalz, Brandenburg, Berlin, Hamburg und Mecklenburg-Vorpommern gemeinsam mit IBM entwickelte elektronische Integrationsportal (eIP), schließlich eAkte als Service (eAS), das auf dem Standardprodukt für Dokumentenmanagement und die Vorgangsbearbeitung (DMS/VBS) des Unternehmens PDV GmbH entwickelte DMS VIS beruht und von Baden-Württemberg, Sachsen, Schleswig-Holstein, Thüringen sowie der Bundesgerichtshof, der Generalbundesanwalt und das Bundespatentgericht eingesetzt wird.

[172] Parallele Vorschriften in § 46e Abs. 2 ArbGG, § 55b Abs. 2 VwGO, § 52b Abs. 2 FGO und § 65b Abs. 2 SGG.

[173] BR-Drs. 818/12, S. 40.

[174] Parallele Vorschriften in § 46e Abs. 4 ArbGG, § 55b Abs. 4 VwGO, § 52b Abs. 4 FGO und § 65b Abs. 4 SGG.

[175] Parallele Regelungen in § 46e Abs. 3 ArbGG, § 55b Abs. 3 VwGO, § 52b Abs. 3 FGO und § 65b Abs. 3 SGG.

[176] mit Wirkung vom 1.1.2018 geändert.

schen Möglichkeiten zum Abruf verfügt und eine Einsicht in den Diensträumen nicht zumutbar ist.[177] Ohne Antrag können die genannten, durch Medienbrüche gekennzeichneten Akteneinsichtsmöglichkeiten nur gewährt werden, wenn der prinzipiell elektronischen Akteneinsicht „wichtige Gründe entgegenstehen". Ein Anspruch darauf, in Papierform geführte Akten(-bestandteile) zu digitalisieren und die Akteneinsicht nach Maßgabe von § 299 Abs. 3 S. 1 ZPO zu gewähren, besteht jedoch nicht.[178]

147 In der Praxis wird Akteneinsicht vor allem über das Akteneinsichtsportal[179] gewährt. Dafür realisierte die Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) unter der Federführung des Landes Baden-Württemberg ein bundesweites Akteneinsichtsportal.[180] Der Akteneinsichtsantrag des Berechtigten (Rechtsanwalt, Behörde etc.) ist beim Gericht entweder per Post oder auf elektronischem Wege zu stellen, etwa über das besondere elektronische Anwalts- bzw. Behördenpostfach auf Basis von EGVP. Das Gericht prüft den Antrag und legt im Falle der Bewilligung die elektronische Akte unter einer bestimmten ID auf einem Server des Gerichts oder des Landes ab. Das Gericht übermittelt dem Akteneinsichtsportal die SAFE-ID des Akteneinsichtsberechtigten sowie die ID zu der auf dem Gerichts- oder Länderserver gespeicherten eAkte. Der Antragssteller kann sich nun mit seiner SAFE-ID beim Portal anmelden, wo ihm eine Übersicht über die für ihn bereitgestellten elektronischen Akten angezeigt wird. Mithilfe der ID zur gespeicherten eAkte kann der Antragsteller diese schließlich aufrufen und ganz oder teilweise herunterladen.[181]

148 **c) Anwaltliche Handakte.** § 50 Abs. 1 BRAO sieht eine anwaltliche Berufspflicht zur Führung einer anwaltlichen Handakte vor, wobei das Anlegen von Handakten ein geordnetes Bild über die Tätigkeit des Rechtsanwalts bieten muss. § 50 Abs. 2 BRAO regelt den Inhalt einer „Handakte im engeren Sinne". Auch eine elektronische oder hybride Handaktenführung ist zulässig.[182]

149 **d) Gemeinsames Fachverfahren (GEFA).** Da auch nach Einführung der elektronischen Gerichtsakte Schnittstellenprobleme mit der Verbindung zu einer Vielzahl unterschiedlicher elektronischer Fachverfahren bestehen, hat der E-Justice-Rat bereits in der 11. Sitzung 2017 beschlossen, ein gemeinsames Fachverfahren („GEFA") zu entwickeln, das sowohl bei den Gerichten der ordentlichen Gerichtsbarkeit und den Staatsanwaltschaften als auch bei den Fachgerichten einsetzbar sein soll. Es soll die unterschiedlichen Lösungen ersetzen, die heute in Bund und Ländern genutzt werden.[183] Das Projekt verläuft jedoch schleppend. Anlässlich des EDV-Gerichtstags 2021 wurde darüber berichtet, dass nach einer Neuausschreibung drei neue Dienstleister für die Softwareentwicklung beauftragt wurden. Die Bundesregierung will nun ebenfalls in das Projekt einsteigen.[184]

150 **e) Beweiswirkung und Beweiskraft elektronischer Dokumente (§§ 371, 371a, 371b ZPO).** Elektronische Dokumente wie E-Mails, Word/PDF-Texte oder Eintragungen in elektronischen Formularen sind gemäß § 371 Abs. 1 S. 2 ZPO im gerichtlichen Verfahren beweisrechtlich Objekte des Augenscheins. Der Beweis wird durch Vorlegung oder Übermittlung der Datei angetreten. Zwar ist der Richter gemäß § 286 Abs. 1 ZPO in der beweisrechtlichen Würdigung frei. Unsignierten oder fortgeschritten signierten Dokumente kommt jedoch eine sehr geringe Beweiskraft zu, wenn der Beweisgegner die Echtheit des Dokuments

[177] So die Gesetzesbegründung, BT-Drs. 18/9416, S. 78.

[178] BFH 6.9.2019 – III B 38/19 mit Blick auf den weitgehend inhaltsgleichen § 78 FGO.

[179] https://www.akteneinsichtsportal.de/, abgerufen am 29.2.2024.

[180] https://ejustice-bw.justiz-bw.de/pb/,Lde/Startseite/Behoerden/Akteneinsicht+und+_austausch, abgerufen am 12.4.2022.

[181] Zum Abrufverfahren siehe https://www.akteneinsichtsportal.de/web/guest/start, abgerufen am 29.2.2024. Dort finden sich auch weitere Erläuterungen zum Ablauf und auch Datenschutzhinweise.

[182] Zur Ausgestaltung der elektronischen Anwalts-Kommunikation und zur Organisation der digitalen Kanzlei siehe ferner Ory/Weth/Anton, jurisPK-ERV Band 1, 1. Aufl., Kapitel 5.1.1 (Stand: 4.1.2021).

[183] https://www.mj.niedersachsen.de/startseite/aktuelles/presseinformationen/eines-fuer-alles---die-justiz-arbeitet-bundesweit-kuenftig-mit-einem-gemeinsamen-fachverfahren-152541.html, abgerufen am 29.2.2024.

[184] Bericht in Legal Tribune Online vom 18.10.2023, https://www.lto.de/recht/justiz/j/digitalisierung-justiz-bundestag-haushalt-millionen-sprach-ki-bund-laender-digitalpakt/, abgerufen am 29.2.2024.

bestreitet. Art. 46 eIDAS-VO hat zwar elektronische Dokumente als Beweismittel ausdrücklich zugelassen, legt aber die Beweiswirkung nicht fest. Insoweit führte die eIDAS-Verordnung zu keiner Änderung gegenüber der bisherigen deutschen Rechtslage. Die Beweiskraft qualifiziert signierter elektronischer Dokumente nach Artikel 32 eIDAS-Verordnung reicht weiter (gilt über § 46 Abs. 2 ArbGG auch im arbeitsgerichtlichen Verfahren, über § 98 VwGO im verwaltungsgerichtlichen und über § 118 Abs. 1 SGG im sozialgerichtlichen Verfahren, während für die Verfahren der Finanzgerichte § 87a Abs. 5 AO einschlägig ist). § 371a ZPO unterscheidet wie bei einer schriftlichen Urkunde (§§ 415 ff.) zwischen einem privaten und einem öffentlichen Dokument. Die Absätze 1 und 2 regeln die Beweiskraft privater, mit qeS signierter Dokumente, Abs. 3 die Beweiskraft öffentlicher Dokumente. Sofern ein privates elektronisches Dokument mit einer qualifizierten elektronischen Signatur versehen ist, finden die Vorschriften (Anscheinsbeweis) über die Beweiskraft privater Urkunden entsprechende Anwendung. Also gilt entsprechend § 416 ZPO der Anscheinsbeweis dafür, dass die in der Urkunde enthaltene Erklärung von Aussteller abgegeben wurde. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung der qualifizierten elektronischen Signatur ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung von der verantwortenden Person abgegeben worden ist, etwa durch die Tatsachendarstellung, dass eine Signaturerstellungseinheit (Eingabegerät) in fremde Hände gelangt ist. Gelingt es, den Anschein der Echtheit zu erschüttern, dann muss die Partei die Echtheit beweisen, die aus dem elektronischen Dokument Rechte herleitet.

Da der Versand eines Dokuments mit absenderbestätigter De-Mail der qualifizierten elektronischen Signatur gleichgestellt ist, regelt Abs. 2 auch den Anscheinsbeweis für die von dem De-Mail-Konto versandte elektronische Nachricht. Der Anschein der Echtheit, der sich aus der Überprüfung der Absenderbestätigung gemäß § 5 Abs. 5 des De-Mail-Gesetzes ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Nachricht von dieser Person mit diesem Inhalt versandt wurde. Das Gericht ist an diese gesetzliche Beweisregeln gemäß § 286 Abs. 2 gebunden. **151**

Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einem mit öffentlichen Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden gemäß § 371a Abs. 3 S. 1 ZPO die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Es gilt demnach gemäß §§ 415 Abs. 1, 417, 418 Abs. 1 ZPO der volle Beweis für den beurkundeten Vorgang, amtliche Anordnungen, Entscheidungen und bezeugte Tatsachen, auch wenn das Dokument nicht mit einer qualifizierten elektronischen Signatur versehen ist. **152**

Wenn das öffentliche Dokument qualifiziert elektronisch signiert ist, dann gilt zusätzlich die Vermutung der Echtheit des Dokuments § 371a Abs. 3 S. 2 iVm § 437 Abs. 1 ZPO mit der Konsequenz, dass der Beweisgegner den Gegenbeweis führen muss. Diese Regelungen gelten wiederum sinngemäß für elektronische Dokumenten, die (anstelle einer qeS) mit absenderbestätigter De-Mail versandt wurden. **153**

Art. 46 eIDAS-VO legt für sämtliche elektronischen Dokumente fest, dass einem derartigen Dokument die Rechtswirkung sowie die Zulässigkeit als Beweismittel im Gerichtsverfahren nicht allein deshalb abgesprochen werden darf, weil es in elektronischer Form vorliegt. Aus der eIDAS-Verordnung ergeben sich dagegen keine weitergehenden hinausgehenden Anforderungen an die Beweisregelung für qeS-signierte Dokumente. Demgegenüber haben Art. 35 Abs. 2 eIDAS-Verordnung Auswirkungen auf die Beweiswirkung qualifizierter elektronischer Siegel, Art. 41 Abs. 1 eIDAS-Verordnung für elektronische Zeitstempel sowie Art. 43 Abs. 1 eIDAS-VO für elektronische Einschreiben. Spezifische deutsche Prozessrechtsreglungen gibt es insoweit nicht.[185] Bei qualifizierten elektronischen Siegeln be- **154**

[185] Mit den Folgen der eIDAS-VO für das deutsche Beweisrecht befassen sich ausführlich Heinze/Prado Ojea CR 2018, CR 2018, 37 ff.: Insoweit werfe die Verordnung in erster Linie Fragen im Bereich ihrer „Vermu-

steht gemäß Art. 35 Abs. 2 eIDAS-Verordnung die rechtliche Vermutung des Ursprungs (Authentizität) und der Unversehrtheit der damit verbunden Daten (Integrität). Allerdings kann die Berechtigung der für die juristische Person handelnden natürlichen Person nicht anhand des Zertifikats nachgeprüft werden. Evtl. können Unberechtigte das Wissen über mangelnde Berechtigung ausnutzen. Es ist insoweit für den Beweisgegner kaum möglich, zu beweisen, dass eine nicht berechtigte Person das Siegel angebracht hat. In der Literatur[186] wird insoweit darauf verwiesen, dass der Begriff „Vermutung" unionsautonom auszulegen sei. Er sei also nicht mit dem gleichlautenden Begriff „Vermutung" der nationalen ZPO gleichzusetzen, sondern vielmehr darüber hinaus auch im Sinne eines bloßen Anscheinsbeweises zu verstehen. Die eIDAS-VO definiert die beweisrechtliche „Vermutung" nicht und regelt nicht die Rechtsfolgen der „Vermutung".[187] Wenn die Vermutung in Art. 35 Abs. 2 eiDAS-VO im Sinne der „Vermutung" des § 292 ZPO ausgelegt würde, dann müsste der Siegelersteller – um die Vermutung zu widerlegen – beweisen, dass ihm ein anderer Text zur Siegelung vorgelegen hat, dass er diese Daten nicht gesiegelt hat oder dass ein Siegel von einer anderen Person missbräuchlich erzeugt worden ist. Die Beweiskraft des qualifizierten elektronischen Siegels ginge dann über die Beweiskraft der qeS hinaus, was inhaltlich nicht begründbar ist. Deshalb wird der europarechtliche Begriff der „Vermutung" wie der nationale Begriff des Anscheins bei § 371a Abs. 1 S. 2 ZPO zu werten sein.

155 **f) Elektronische Prozessaktenführung im Strafgerichtlichen Verfahren.** Gemäß § 32 Abs. 1 StPO kann **bis zum 31.12.2025** die **elektronische Akte im strafgerichtlichen Verfahren** auf der Grundlage von Rechtsverordnungen des Bundes und der Länder eingeführt werden. Die Bundesregierung und die Landesregierungen können jeweils für ihren Bereich durch Rechtsverordnung den Zeitpunkt bestimmen, von dem an die Akten elektronisch geführt werden, können dies entweder für das gesamte Strafverfahren anordnen oder auf einzelne Gerichte oder Strafverfolgungsbehörden oder auch auf einzelne Verfahren beschränken. Diese Ermächtigung kann durch Rechtsverordnung auf die zuständigen Bundes- und Landesministerien übertragen werden. Ferner bestimmen die Rechtsverordnungen die organisatorischen und dem Stand der Technik entsprechenden technischen Rahmenbedingungen einschließlich der einzuhaltenden Anforderungen der Barrierefreiheit sowie des Datenschutzes und der Datensicherheit. Dies ist so zu verstehen, dass das allgemeine Datenschutzrecht nicht verdrängt wird, sondern nur bereichsspezifische Sonderregelungen zu treffen sind. Allerdings ist die DSGVO nicht anwendbar (dort Art. 2 Abs. 2 lit.d), vielmehr die RL (EU) 2016/680 zum Datenschutz in Strafsachen (sog. JI-Richtlinie) gemäß ihrer Umsetzung in den §§ 45–61 BDSG. Ab 1.1.2026 sind die neu anzulegenden Akten bundesweit nur noch elektronisch zu führen, § 32 Abs. 1 S. 1 StPO. Eine hybride Aktenführung (auf Papier und elektronisch) ist nicht vorgesehen. Die Einsicht in elektronische Akten ist in § 32f StPO geregelt.

5. Digitaler Gerichtssaal

156 Schon seit längerer Zeit gibt es Bestrebungen, Gerichtssäle elektronisch so auszustatten, dass das Gericht und die Verfahrensbeteiligten weitgehend ihre elektronischen Instrumente nutzen und für die Beteiligten und die Öffentlichkeit die Schriftsätze visualisieren können.[188] Auch für den Strafprozess wird an ähnlichen Projekten gearbeitet. Ein Forschungsprojekt aus Wissenschaft, Justiz, Anwaltschaft und Wirtschaft an der Universität zu Köln[189] zielt darauf ab, die ersten *rechtlichen und technischen Rahmenbedingungen von Digitalisie-*

tungswirkung" auf. So sei die Konsequenz des in der eIDAS-VO verwendeten Begriffs der Vermutung im deutschen Beweisrecht bislang schon nicht eindeutig definiert. Möglich wäre es, ihn als Vermutung iSd § 292 ZPO zu verstehen, was Heinze/Prado Ojea zu Recht im Ergebnis ablehnen.

[186] ZB Roßnagel, MMR 2016, 647 ff.

[187] Lt. Erwgr. 22 durch nationales Recht festzulegen.

[188] Vgl. dazu elektronische Gerichtssäle in Frankfurt/Oder: www.lto.de/recht/justiz/j/elektronische-gerichtsakte-pilotprojekt-legal-tech/ (abgerufen am 17.4.2022) oder am Sozialgericht in Berlin (www.tagesspiegel.de/berlin/digitalisierung-berliner-sozialgericht-wird-digitaler-vorreiter/23634940.html, abgerufen am 17.4.2022).

[189] https://e-court.jura.uni-koeln.de/.

rungsprozessen im Gerichtssaal auszuloten und den ersten „elektronischen Strafgerichtssaal“ zu schaffen. Dabei sollen audiovisuelle Aufnahmen von allen Verfahrensbeteiligten während der Verhandlung und der Einsatz Künstlicher Intelligenz dazu dienten, eine digitale Verhandlungsaufzeichnung zu erstellen, die dann auch das bisher manuell gefertigte Protokoll ersetzen kann.

6. Einsatz von Videokonferenzsystemen

a) Allgemeines. Seit 2002 eröffnet § 128a ZPO die Möglichkeit der Verfahrensbeteiligten zur Teilnahme von einem anderen Ort als dem Gerichtssaal (Abs. 1) bzw. zur Beweisaufnahme mit weit entfernten Zeugen und/oder Sachverständigen (Abs. 2). Dabei liegt es im Ermessen des Gerichts,[190] ob es den Parteien, ihren Bevollmächtigten und Beiständen auf Antrag oder von Amts wegen gestattet, sich während einer mündlichen Verhandlung an einem anderen Ort aufzuhalten und dort Verfahrenshandlungen vorzunehmen. In die Ermessensentscheidung fließen insbesondere die -vom Antragsteller geäußerten Motive für die Videokonferenz ein. Die Ermöglichung einer Videoverhandlung eröffnet viele Vorteile für die effiziente Durchführung einer Verhandlung für die Richterinnen und Richter, aber auch für die Anwälte, Zeugen und Sachverständigen. So kommt es evtl. zu weniger Terminverlegungsanträgen, weil die mit den Fragen des konkreten Verfahrens vertrauten Anwälte sich seltener vertreten lassen, Sachverständige eher verfügbar sind und die Verfügbarkeit von Gerichtssälen nicht mehr ausschlaggebend für die Terminierung sein muss. Dennoch kam es erst während der COVID-19-Pandemie zu einer intensiveren Nutzung der Instrumente der Videokonferenz im gerichtlichen Verfahren, denn dabei ging darum, möglichst physische Personenkontakte zwischen den Verfahrensbeteiligten, den Zeugen und dem Gericht zu vermeiden und damit die Ausbreitung von Infektionen zu verhindern. Allerdings kann das Gericht selbst die Verhandlung nicht vom heimischen Arbeitszimmer aus leiten, sondern muss sich während der Videokonferenzverhandlung im Sitzungsraum aufhalten. Die Öffentlichkeit wird dabei durch öffentliche Übertragung der Verfahrenshandlungen in den Gerichtssaal am Sitzungsort hergestellt. Allerdings gaben § 114 ArbGG und § 211 SGG vom 29.5.2020 bis 31.12.2021 – über die weiterhin geltenden § 128a ZPO und § 110a SGG hinaus – die Möglichkeit, einem ehrenamtlichen Richter „bei einer epidemischen Lage von nationaler Tragweite nach § 5 Abs. 1 S. 1 des Infektionsschutzgesetzes“ von Amts wegen zu gestatten, an einer mündlichen Verhandlung im Sitzungszimmer von einem anderen Ort aus per Videokonferenz teilzunehmen, wenn es für ihn aufgrund der epidemischen Lage unzumutbar war, persönlich an der Gerichtsstelle zu erscheinen (Entscheidung im pflichtgemäßen Ermessen des Gerichts). Motiv für die vorübergehende Einfügung dieser Möglichkeiten in §§ 114 ArbGG und § 211 SGG war, unter den ehrenamtlichen Richterinnen und Richtern insbesondere die sogenannten Risikogruppen (ältere bzw., vorerkrankte Menschen) von schweren Verläufen der Viruserkrankung zu schützen. Eine Video-Teilnahme der ehrenamtlichen Richterinnen und Richter war auch für die Beratung, Abstimmung und Verkündung der Entscheidung möglich, wobei gemäß § 114 Abs. 2 S. 3 ArbGG bzw. § 211 SGG die an der Beratung und Abstimmung Teilnehmenden „durch geeignete Maßnahmen die Wahrung des Beratungsgeheimnisses sicherzustellen“ hatten. Mit dem Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer Vorschriften vom 5.10.2021[191] hat der Gesetzgeber mit Wirkung ab dem 1.1.2022 geklärt, dass auch für die Güteverhandlung die Möglichkeit der Videoverhandlung besteht. 157

b) Zukünftige Erweiterungen der Möglichkeiten einer Videokonferenz. Bereits im Mai 2021 hatte die damals oppositionelle FDP-Fraktion im Bundestag verschiedene Erweiterungen und rechtliche Klarstellungen beantragt,[192] die damals mit den Stimmen der Regierungsfraktionen abgelehnt worden waren. So sollte durch eine Erweiterung des § 128a ZPO auf 158

[190] Ory/Weth/Klasen, jurisPK-ERV Band 2, 2. Aufl., § 128a ZPO (Stand: 6.2.2024), Rn. 11.
[191] BGBl. I 2021, 4607.
[192] BT-Drs. 19/19120.

Antrag einer Partei die Verhandlung im Wege der Bild- und Tonübertragung angeordnet werden müssen. Ferner war eine Regelung vorgesehen, wonach es bei Zustimmung der Parteien der Allgemeinheit ermöglicht wird, allein im Wege eines Livestreams an Verhandlungen teilzunehmen, ohne dass dadurch der Öffentlichkeitsgrundsatz gemäß§ 169 Abs. 1 GVG verletzt wird.

159 Die Koalitionsvereinbarung für die „Ampelregierung" für die Jahre 2021 bis 2024 sieht eine Rechtsänderung vor, wonach Beweisaufnahmen „audio-visuell dokumentiert" werden sollen.[193] Damit stellt sich die Frage, ob virtuelle Verfahren auch verpflichtend angeordnet werden können, also das bisherige Recht der Parteien einzuschränken ist, auch bei Ermöglichung einer Videokonferenz an der unmittelbaren Verhandlung in Anwesenheit des Richters teilzunehmen. In der Vergangenheit führte zuweilen gerade das kurzfristige Erscheinen einer Partei trotz erlaubter Videokonferenz zu Herausforderungen technischer Art, weil „hybride" Verhandlungen sehr aufwendig sind.[194] Denn dann muss im Gerichtssaal eine entsprechende Infrastruktur vorhanden sein, um den dort Anwesenden eine effektive Verhandlungsteilnahme zu ermöglichen und für die Online-Teilnehmenden auch die anwesenden Verfahrensbeteiligten mit der Kamera zu erfassen. Ferner könnte das Gericht zur Anordnung der Videokonferenz verpflichtet werden, wenn eine Partei diese beantragt. Die während der Pandemie geltenden (mittlerweile wieder aufgehobenen) Sonderregelungen des § 114 Abs. 2 S. 1 ArbGG und § 211 Abs. 2 S. 1 SGG sahen für das Gericht ein eingeschränktes Ermessen bei der Anordnung der Videokonferenz[195] vor. Sodann wäre zu erwägen, in der BORA eine Anwaltspflicht zu verankern, Videokonferenztechnik vorzuhalten. Zu klären wäre, ob es auch dem Gericht gestattet werden sollte, eine Gerichtsverhandlung vom Homeoffice aus zu veranstalten. Das hätte zur Folge, dass eventuell die Öffentlichkeitsbeteiligung neu zu organisieren wäre. Denn es erscheint nicht überzeugend, die Öffentlichkeit in einen Gerichtssaal zu verweisen, während das Gericht und die Prozessbeteiligten ausschließlich virtuell am Prozessgeschehen teilnehmen.[196] Das Öffentlichkeitsprinzip folgt aus Art. 6 Abs. 1 EMRK und § 169 GVG. Auch ist der bisher geltende Grundsatz der Unmittelbarkeit (§§ 285, 355 ZPO) zu beachten. Auf die Herstellung der Öffentlichkeit in entsprechender Anwendung des „Rechtsgedankens des § 128 Abs. 2 ZPO" zu verzichten,[197] wäre dann kaum zu rechtfertigen, wenn die Videoverhandlungen über den Ausnahmecharakter hinausgehen und zum Regelfall werden.

160 Sodann ist zu klären, ob die vom Koalitionsvertrag vorgesehene durchgehende Videoaufzeichnung von Vernehmungen in der ZPO weiterhin als vorläufige Protokollaufzeichnung gemäß § 160a ZPO zu werten oder als Protokollaufnahme gemäß § 159 ZPO wäre. Schließlich ist die datenschutzrechtliche Frage zu beantworten, wie bei Nutzung der von amerikanischen Anbietern angebotenen Videokonferenzsoftware verhindert werden kann, dass Datenströme aus gerichtlichen Verfahren amerikanische Server erreichen, was die Einhaltung der Grundsätze der Art. 44 ff. DSGVO gefährdet (die Übermittlung personenbezogener Daten in Drittländer ist nur unter engen Voraussetzungen zulässig) und ob sogenannte On-Premises -Lösungen (Betrieb von Videokonferenzsystemen auf gerichtseigenen Servern)praktikabel und mit den Datenschutzanforderungen vereinbar sind, ob das Beteiligten in die Konferenz über Links auf der Ladung eingebunden werden können, ohne dass diese über eine eigene Lizenz verfügen oder Softwareclients installieren müssen, ob und wie verschiedene Kameras – auch bei mehreren Beteiligten – Videosignale aus dem Gerichtssaal übertragen können, über welche Einstellungen die Kameras verfügen müssen (Portrait- oder Weitwinkeldarstellung zur vollständigen und lückenlosen Sichtbarkeit der Richter und der Prozessbeteiligten), ob und wie die zuschauende Öffentlichkeit gezeigt wird und wie die im

[193] https://fragdenstaat.de/dokumente/142083-koalitionsvertrag-2021–2025 3537 ff. abgerufen am 29.2. 2024.
[194] Bernhardt jM 2022, S. 93.
[195] LSG München 16.6.2021 – L 13 R 201/20, BeckRS 2021, 17820, MMR 2022, 246, Rn. 3.
[196] Dazu Paschke, Digitale Gerichtsöffentlichkeit, 2018, S. 258 ff.
[197] So Köbler, NJW 2021, 1073.

Gerichtsverfahren gegenständlichen Dokumente den Beteiligten – etwa im Wege des Dokumenten-Sharings- zur Verfügung gestellt werden können. Dem aus dem Recht auf informationelle Selbstbestimmung der Prozessbeteiligten zu folgernden staatlichen Schutzpflicht dürfte auch nicht dadurch ausreichend Rechnung getragen sein, die Aufnahmefunktion zu sperren, um eine nicht autorisierte Verfolgung oder Aufzeichnung bei der Videokonferenz zu verhindern, denn es gibt technische Umgehungsmöglichkeiten.[198] Ferner ist der virtuelle Wartebereich ist zu nutzen, um einen unkontrollierten Zugang Externer zum gerichtlichen Verfahren zu verhindern. Alle diese Sicherungsmaßnahmen können zwar die Gefahren mindern, aber nicht ausschalten, die von den Geräten und Anwendungen bei den Endnutzern ausgehen. Um einen „Flickenteppich" beim Einsatz der Videokonferenzsysteme und ganz unterschiedliche Anforderungen zu vermeiden, ist der E-Justice-Rat gefordert, Landesgrenzen übergreifend Festlegungen für Standards der Videokonferenzsysteme zu treffen.

Die Videokommunikation ist auch im Strafprozess nutzbar und erweiterbar. Schon jetzt **161**
sind unter dem Aspekt des Zeugenschutzes Videoaufzeichnungen von Vernehmungen im Strafverfahren von Zeugen außerhalb der Hauptverhandlung durch Richter und Staatsanwalt zugelassen (§§ 58a, 161a Abs. 1 Satz 2 StPO) und in den Fällen des § 58a Abs. 1 S. 3 StPO zwingend, bedürfen aber der Zustimmung des Zeugen. § 255a StPO sieht eine „Vorführung einer aufgezeichneten Vernehmung" eines Zeugen unter 18 Jahren in Verfahren wegen Straftaten gegen die sexuelle Selbstbestimmung oder gegen das Leben, wegen Misshandlung von Schutzbefohlenen oder wegen Straftaten gegen die persönliche Freiheit vor, wenn der Angeklagte und sein Verteidiger Gelegenheit hatten, an dieser mitzuwirken, und wenn der Zeuge der vernehmungsersetzenden Vorführung dieser Aufzeichnung in der Hauptverhandlung nicht unmittelbar nach der aufgezeichneten Vernehmung widersprochen hat.

Die Aufzeichnung einer Vernehmung ist allerdings nur im Fall des § 247a Abs. 1 S. 4 **162**
StPO vorgesehen. Die Videoübertragung einer Zeugenvernehmung im Strafverfahren ist nach §§ 168e, 247a StPO außerhalb und in der Hauptverhandlung aus Zeugenschutzgründen zulässig, in der Hauptverhandlung auch unter den Voraussetzungen des § 251 Abs. 2 StPO, zB bei großer Entfernung des Zeugen. Für die Zukunft sieht die Ampel-Koalitionsvereinbarung vor: „Vernehmungen und Hauptverhandlung müssen in Bild und Ton aufgezeichnet werden".[199] Dabei bedarf es allerdings der Klärung, ob die Aufzeichnungen zukünftig lediglich dafür genutzt werden sollen, die Abfassung von Protokolldokumenten zu erleichtern oder als Ersatz für das Vernehmungsprotokoll vorzusehen.[200] Zu bedenken ist, dass es schwieriger sein mag, Videoaufzeichnungen auf bestimmte Aussagen zu durchzusuchen, als innerhalb von Dokumenten zu recherchieren. Allerdings könnten neuere technische Möglichkeiten dazu genutzt werden, möglichst komfortabel in Video/Ton-Aufzeichnungen etwa nach bestimmten Stichworten und bestimmten Personen zu suchen. Ferner ist die Wirkung der Videodokumentation der Hauptverhandlung als Protokoll auf die Grundstrukturen des Strafverfahrensrechts, insbesondere die Aufgabenverteilung zwischen Tat- und Revisionsgerichten zu klären.[201]

7. Besondere Fragen zum elektronischen Rechtsverkehr aus Anwaltssicht

[198] LSG München 16.6.2021 – L 13 R 201/20, BeckRS 2021, 17820, MMR 2022, 246, Rn. 5 Der Antrag eines Klägers auf Teilnahme an einer mündlichen Verhandlung im Wege der Bild- und Tonübertragung gem. § 110a SGG wurde mit der Begründung abgelehnt, das Verbot der Aufzeichnung sei in der Wohnung nicht durchsetzbar.

[199] https://fragdenstaat.de/dokumente/142083-koalitionsvertrag-2021–2025/ Rn. 3557 ff., abgerufen am 29.12.2024.

[200] Bernhardt jM 2022. 95.

[201] Siehe zu dem gesamten Themenkomplex den Abschlussbericht der von der Bundesministerin der Justiz und für Verbraucherschutz Christine Lambrecht Anfang 2020 eingesetzten Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung (mit Anlagenband) https://www.bmj.de/SharedDocs/Publikationen/DE/Fachpublikationen/2021_Abschlussbericht_Hauptverhandlung_Anlagenband.pdf?__blob=publicationFile&v=3, abgerufen am 29.2.2024.

163 § 43a BRAO und insbesondere § 203 Abs. 1 Nr. 3 StGB normieren die Verschwiegenheitsverpflichtung und schützen das sogenannte Anwaltsgeheimnis vor unbefugter Weitergabe von Informationen der Mandanten. Die daraus folgenden Pflichten führten bei zunehmender Digitalisierung vor allem zu der Frage, welche Konsequenzen dies auf die Beschäftigung freier IT –Dienstleister in der Anwaltskanzlei hat. Hier hat eine gesetzliche Novellierung[202] zu einer gewissen Klärung geführt. So regelt nunmehr § 203 Abs. 3 StGB: „Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglichmachen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken“ Um den Schutz des sogenannten Anwaltsgeheimnisses nicht abzusenken, wurden die für Anwälte geltenden Strafvorschriften durch § 203 Abs. 4 StGB auf Gehilfen ausgedehnt.

8. Einsatz künstlicher Intelligenz in der Justiz

164 **a) Einsatzszenarien.** Es gibt kein einheitliches Begriffsverständnis von Künstlicher Intelligenz. Hier wird das Verständnis der Europäischen Kommission zugrunde gelegt: Demnach sind KI-Systeme, die „mit einem ‚intelligenten‘ Verhalten ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen“.[203] Die Einsatzszenarien für Künstliche Intelligenz (KI) in der Justiz sind vielfältig.[204]

165 *aa) Klassifizierung und Analyse.* KI kann bei der Klassifizierung und Analyse helfen. So können mithilfe von KI eingehende Dokumente analysiert, auf verschiedene Rechtsgebiete verteilt, vorhandenen Akten bzw. zuständigen Richterinnen und Richtern zugeordnet und deren richterliche Analysearbeit erleichtert werden, etwa durch Sichtbarmachung bestimmter Zusammenhänge von Sachverhalten und Rechtsargumenten sowie durch Vorsortierung. KI dient insoweit der effizienten Durchdringung des Streitstoffs, der Aufwandsminderung für die Richterinnen und Richter sowie letztlich auch der Beschleunigung des Verfahrens. Auch Strafermittlungsorgane können vom KI-Einsatz profitieren, etwa wenn kognitive Systeme Bild-, Video- und Audiomaterial automatisch analysieren, um die Sichtbarkeit einer bestimmten Person herauszufinden oder deren Alter im Hinblick auf sexualstrafrechtliche Tatbestände zu bestimmen.[205] Dabei kann KI aus großen Datenmengen schnell bestimmte Beweismittel herausfiltern und den menschlichen Auswerter in einem sehr frühen Ermitt-

[202] 30.10.2017 (BGBl. I 2017, 3618).

[203] Mitteilung der Kommission an das Europäische Parlament, den europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Künstliche Intelligenz für Europa-, COM(2018) 237 (final), S. 1.

[204] Siehe zu den diversen Einsatzszenarien Szostek/Zalucki/Bernhardt (Hrsg.), Internet and New Technologies Law – Perpectives and Challenges –, Baden-Baden, 2021, S. 173, 178 ff.; Biallaß nimmt eine ähnliche Einteilung unter dem Titel „Legal Tech“ ein, in: Ory/Weth, jurisPK-ERV Band 1, 1. Aufl., Kapitel 8 (Stand: 28.8.2020), Rn. 13 ff. mwN.

[205] Etwa das Projekt des nordrhein-westfälische Ministers der Justiz und weiterer Projektpartner für ein hybrides Cloud-Szenario ZAC – AIRA ("AI enabled Rapid Assessment“), siehe Bericht der Süddeutschen Zeitung vom 10.5.2022, https://www.sueddeutsche.de/panorama/justiz-koeln-ermittler-neues-instrument-gegen-kinderpornografie-dpa.urn-newsml-dpa-com-20090101-220510-99–230008, abgerufen am 29.2.2024.

Weitere KI-Projekte im Bereich der Strafermittlungstätigkeit: niedersächsische Pressemitteilung vom 10.6.2020, https://www.lka.polizei-nds.de/a/presse/pressemeldungen/kuenstliche-intelligenz-lka-niedersachsen-stellt-software-zur-bekaempfung-von-kinderpornografie-bundesweit-zur-verfuegung-114750.html, abgerufen am 29.2.2024; Überblick bei Wissenschaftliche Dienste des Deutschen Bundestages „ Künstliche Intelligenz in der Justiz -Internationaler Überblick“, WD 7 –3000 -017/21 vom März 2021, S. 6, https://www.bundestag.de/resource/blob/832204/6813d064fab52e9b6d54cbbf5319cea3/WD-7–017-21-pdf-data.pdf, abgerufen am 29.2.2024.

lungsstadium unterstützen, allerdings nicht vollständig ersetzen. Auch in Wirtschaftsstrafsachen können relevante Sachverhalte innerhalb großer Datenmengen mithilfe von KI kenntlich gemacht werden. Die Einsatzmöglichkeiten der KI zur Durchsuchung großer Datenbestände wird auch als „E-Discovery" bezeichnet.[206]

bb) Automatische Übersetzung. Ein in Zeiten der Europäisierung und Internationalisierung immer wichtigeres Einsatzfeld der KI ist die automatische Übersetzung von Dokumenten in andere (EU-)Amtssprachen mithilfe von neuronalen maschinellen Übersetzungen, um den Herausforderungen Rechnung zu tragen, die aus einem Anwachsen grenzüberschreitender Rechtsfälle und aus einem immer größer werdenden Übersetzungsbedarf entstehen.[207] **166**

cc) Anonymisierung von Gerichtsurteilen. Zur Realisierung des Ziels der Koalitionsvereinbarung der Ampelkoalition,[208] für die Veröffentlichung grundsätzlich aller Gerichtsurteile zu sorgen, bedarf es einer KI-gestützten Anonymisierung von Gerichtsurteilen. Denn es reicht zumeist nicht aus, lediglich Personennamen unkenntlich zu machen, um eine De-Anonymisierung zu verhindern. **167**

dd) Interaktion. Die größten Zukunftschancen des Einsatzes der KI im Justizbereich dürften in der sogenannten Interaktion liegen. Schon heute setzen Online-Schlichtungsverfahren – sowohl bei der Einreichung von Anträgen als auch bei der Entscheidung bzw. Entscheidungsvorbereitung der Schlichtungsstellen – in starkem Maße auf Automation.[209] Allerdings sind die rechtlichen Bedingungen für einen KI-Einsatz in Justizverfahren andere als in den Schlichtungsverfahren, denen keine rechtliche Bindung zukommt. In Justizverfahren könnte KI zum Einsatz kommen, wenn einem Vorschlag der Arbeitsgruppe „Modernisierung des Zivilprozesses" im Auftrag der Präsidentinnen und Präsidenten der Oberlandesgerichte, des Kammergerichts, des Bayerischen Obersten Landesgerichts und des Bundesgerichtshofs entsprechend ein beschleunigtes, formularbasiertes Online-Verfahren eingeführt wird, das in der Regel vollständig im Wege elektronischer Kommunikation zu führen ist, bei bestimmten Gerichten konzentriert werden kann und für Streitwerte bis 5.000 EUR vorgesehen ist[210] und eventuell zunächst in Massenverfahren zwischen klagenden Verbraucherinnen und Verbrauchern einerseits und beklagten Unternehmen andererseits Anwendung finden könnte. In ähnlicher Weise verfolgt auch der Ampel-Koalitionsvertrag auf Bundesebene von 2021 die Einführung eines formularbasierten Online-Verfahrens.[211] Ferner könnte KI zur Einrichtung von Chatbots[212] bei Rechtsantragsstellen[213] oder für die Beteiligung an Musterfeststellungsklagen genutzt werden. Ferner sind Chatbots auch vorstellbar zur Aufnahme von Strafanzeigen im Falle von Hate-Speech im Internet[214] oder in Anwaltskanzleien für den Kontakt **168**

[206] Ory/Weth/Biallaß, jurisPK-ERV Band 1, 2. Aufl., Kapitel 8 (Stand: 23.11.2022), Rn. 35 ff. mwN.

[207] Siehe dazu die während der deutschen EU-Ratspräsidentschaft 2020 freigeschaltete Website des EU Council „Presidency Translator" mit verschiedenen automatischen Übersetzungsprogrammen, der nunmehr nach Anmeldung genutzt werden kann (https://www.eu2020.de/eu2020-en/presidency/uebersetzungstool/2361002), abgerufen am 29.2.2024. Zum Einsatz der KI in Übersetzungen NEGZ-Kurzstudie von Djeffal https://negz.org/2021/05/19/negz-kurzstudie-uebersetzung-und-kuenstliche-intelligenz-in-der-oeffentlichen-verwaltung/, abgerufen am 29.2.2024.

[208] Ausarbeitung der Wissenschaftlichen Dienste des Deutschen Bundestages „Künstliche Intelligenz in der Justiz -Internationaler Überblick", WD 7 –3000 -017/21 vom März 2021.

[209] Siehe hierzu die Verordnung (EU) 524/2013 des Europäischen Parlaments und des Rates vom 21.5.2013 über die Online-Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der VO (EG) 2006/2004 und der RL 2009/22/EG (Verordnung über Online-Streitbeilegung in Verbraucherangelegenheiten – ODR-Verordnung).

[210] www.justiz.bayern.de/media/images/behoerden-und-gerichte/oberlandesgerichte/nuernberg/thesenpapier_der_arbeitsgruppe.pdf, abgerufen am 29.2.2024.

[211] Downloadbar unter https://www.fdp.de/koalitionsvertrag, abgerufen am 29.2.2024, S. 106.

[212] Zur Entwicklung und technischen Wirkungsweise KI basierter Chatbots Ory/Weth/Biallaß, jurisPK-ERV Band 1, 2. Aufl., Kapitel 8 (Stand: 23.11.2022) , Rn. 76 ff.

[213] Biallaß NJW-aktuell 34/2019, S. 15.

[214] Hartmann DRiZ 2020, 86 f.

mit Mandanten. Konkret sind Chatbots auf EU-Ebene zur Unterstützung der Nutzung des E-Justice-Portals vorgesehen.[215]

169 **b) Rechtliche Bewertung des KI-Einsatzes in der Justiz.** *aa) Verfassungsprinzipien.* Spezifische – einfachrechtliche – Normen zum Einsatz der KI in der Justiz fehlen bisher. Insbesondere gibt es keine dem § 35a VwVfG vergleichbare Norm für gerichtliche Verfahren, etwa für das – schon weitgehend automatisierte – Mahnverfahren. Der KI-Einsatz in der Justiz muss allerdings den Verfassungsprinzipien entsprechen, insbesondere dem Prinzip des (natürlichen) unabhängigen Richters gem. Art. 92 GG mit der Kontrolle über die eigene Entscheidung, die keiner selbstlernenden Maschine überlassen werden darf, wenn deren Ergebnis niemand vorhersehen und konkret auch nicht beeinflussen kann; dem Prinzip des gesetzlichen Richters, dessen Zuständigkeit vor Beginn der Streitigkeit klar bestimmt ist, dem Gebot des fairen Verfahrens, das auch den Prozessbeteiligten die Chance gibt, auf den Gang und das Ergebnis des Verfahrens Einfluss zu nehmen, was insbesondere bei einer selbstlernenden, unüberwachten KI kaum vorstellbar ist. Ferner muss der KI-Einsatz dem Prinzip des effektiven Rechtsschutzes und damit verbunden dem Gebot der Nachprüfbarkeit der Entscheidung entsprechen, was in Gefahr ist, wenn eine intransparent arbeitende Maschine entscheidet.

170 Auch Grundrechte, vor allem der Schutz vor Diskriminierung sind zu beachten; dieses Grundrecht ist tangiert, wenn Prognosesoftware (wie etwa die in den USA verwandte Software COMPAS[216]) eingesetzt wird, um die Rückfallgefahr von Verurteilten abzuschätzen, was wiederum bedeutsam für die Festlegung von Kautionen, die Bemessung von Strafhöhen oder die Entscheidung über eine frühere Haftentlassung auf Bewährung ist. Denn hier besteht die Gefahr, dass in die Programmierung Vorurteile der Programmierer in die KI eingeflossen sind. Richter müssen diese Herausforderungen kennen und bei ihren eigenen Entscheidungen damit sachgerecht umgehen. Ist der Richter nicht in der Lage, die von der Künstlichen Intelligenz beeinflusste Entscheidungsstruktur zu durchdringen („Black-Box-Systeme") und folgt er ungeprüft dem Entscheidungsvorschlag, trifft er keine unabhängige und allein am Gesetz orientierte Entscheidung. Insoweit können Richter auch durch eigenes Verhalten ihre richterliche Unabhängigkeit verletzen.[217]

171 Einige Verfahrensarten könnten für eine Öffnung für eine Automatisierung auch mithilfe des Einsatzes künstlicher Intelligenz auch ohne Verstoß etwa gegen die Justizgewährleistungspflicht in Erwägung gezogen werden, etwa das Kostenfestsetzungsverfahren.[218]

172 Die 73. Jahrestagung der Präsidentinnen und Präsidenten der Oberlandesgerichte, des Kammergerichts, des Bayerischen Obersten Landesgerichts und des Bundesgerichtshofs beschloss, unter Leitung der Oberlandesgerichte Nürnberg und Celle eine Arbeitsgruppe einzurichten, welche ein Grundlagenpapier zu den Zielen einer Nutzbarmachung von KI in der Justiz durch strukturierte Aufarbeitung von technischen Möglichkeiten, ihrem praktischen Nutzen und ihren verfassungsrechtlichen sowie ethischen Grenzen erstellen sollte. Das anschließend erarbeitete Grundlagenpapier („Einsatz von KI und algorithmischen Systemen in der Justiz") wurde sodann in der 74. Jahrestagung einstimmig beschlossen. Aus dem Anhang des Grundlagenpapiers sind die laufenden und geplanten Projekte zu Legal Tech und künstlicher Intelligenz aufgelistet.[219]

---

[215] Das ist vorgesehen im mehrjährigen Aktionsplan für E-Justrice 2019–2023, der im Dezember 2018 angenommen wurde (ABl. 2019/C96/05). Hierzu auch Bernhardt in Szostek/Zalucki (Hrsg.), Internet and New Technologies Law – Perpectives and Challenges –, 2021, S. 173, 186.

[216] Dazu Wahedi, Verfassungsrechtliche Anforderungen an die Automatisierung der Justiz, 2018, S. 25 ff.

[217] So auch der Abschlussbericht LAG Legal Tech, S. 57, www.schleswig-holstein.de/DE/Landesregierung/II/Minister/Justizministerkonferenz/Downloads/190605_beschluesse/TOPI_11_Abschlussbericht.html, abgerufen am 29.2.2024.

[218] Wahedi, Verfassungsrechtliche Anforderungen an die Automatisierung der Justiz, 2018, S. 94.

[219] Das Grundlagenpapier ist unter https://oberlandesgericht-celle.niedersachsen.de/startseite/aktuelles/ki_in_der_justiz/ergebnisse-der-74-jahrestagung-zum-einsatz-kunstlicher-intelligenz-in-der-justiz-u-a-212102.html abrufbar (abgerufen am 29.2.2024). Siehe auch sehr umfassende Darstellung zu den Projekten und zur den rechtlichen Fragen des Einsatzes künstlicher Intelligenz Biallaß in: Ory/Weth, jurisPK-ERV Band 1, 2. Aufl., Kapitel 8 (Stand: 23.11.2022).

bb) Supranationale Normen. Die Konzeption und der Einsatz von KI -Instrumenten müssen ferner mit den Menschenrechten vereinbar sein, wie sie in der Europäischen Menschenrechtskonvention (EMRK) und dem Übereinkommen des Europarates zum Schutz personenbezogener Daten festgelegt sind.[220] 173

Im Anwendungsbereich der europäischen DSGVO normiert mit europaweiter Geltung Art. 22 Abs. 1 DSGVO, dass eine betroffene Person ein Recht auf ein Handeln durch einen Menschen hat und eine Maschinenentscheidung nicht genügt – es sei denn, der Betroffene hat in eine solche automatische Entscheidung eingewilligt oder das nationale Recht sieht etwas anderes vor. 174

cc) Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über Künstliche Intelligenz- KI-Gesetz). Auf EU-Ebene setzt die Grundrechtecharta ebenfalls dem Einsatz der KI auch im Justizbereich Grenzen – wie auch bereits zu Zeiten des EWG-Vertrages das gerichtliche Verfahrensrecht im Sinne höherrangiger (Verfassungsrechts-) Prinzipien auszulegen war.[221] Am 21.4.2021 hatte die EU-Kommission auf der Grundlage des EU-Weißbuchs zur KI von Februar 2020 einen Verordnungsvorschlag für einen „Rechtsakt über Künstliche Intelligenz" vorgelegt.[222] Auf dieser Basis und nach fast dreijähriger Diskussion wurde am 2.2.2024 über die **Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über Künstliche Intelligenz- KI-Gesetz)** im Trilog ein Einigung erzielt und vom Ausschuss der Ständigen Vertreter (COREPER) einstimmig gebilligt.[223] Die Verkündung im Amtsblatt steht (Stand Februar 2024) bevor.[224] 175

Die Verordnung tritt am 20. Tag nach ihrer Veröffentlichung im EU-Amtsblatt in Kraft und wird im Wesentlichen nach 24 Monaten anwendbar, Art. 85 Abs. 1 und Abs. 2, mit Ausnahme der folgenden spezifischen Bestimmungen, die in Art. 85 Abs. 3 genannt sind.: Die Regelungen für verbotene KI-Systeme sind bereits nach 6 Monaten anzuwenden, die Verpflichtungen für sog. Foundation Models gelten nach 12 Monaten Verpflichtungen für KI-Systeme mit hohem Risiko im Sinne von Art. 6 Abs. 1 (also KI-Systeme, die als Sicherheitskomponente eines Produkts verwendet werden sollen, oder KI-Systeme, die in Anhang II aufgeführt sind) werden nach 36 Monaten gelten (Art. 85 Abs. 3b). 176

Das KI-Gesetz enthält Verpflichtungen für Anbieter, Betreiber, Importeure, Händler und Produkthersteller von KI-Systemen, die mit dem EU-Markt verbunden sind. Das KI-Gesetz gilt beispielsweise für Anbieter, die KI-Systeme auf dem EU-Markt in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle für allgemeine Zwecke („GPAI-Modelle") auf dem EU-Markt in Verkehr bringen; (2) Bereitsteller von KI-Systemen, die einen Niederlassungsort in der EU haben bzw. in der EU ansässig sind, sowie für Anbieter und Bereitsteller von KI-Systemen in Drittländern, wenn der von einem KI-System erzeugte Output in der EU verwendet wird (Art. 2 Abs. 1 KI-Gesetz). Der räumliche Anwendungsbereich erstreckt sich gemäß Art. 2 Abs. 1 lit.c dem Marktortprinzip entsprechend auch auf Anbieter von AI aus Drittländern mit einem „Output" in der EU. 177

Art. 3 **definiert ein KI-System** als „ein maschinengestütztes System, das so konzipiert ist, dass es mit einem unterschiedlichen Grad an Autonomie betrieben werden kann und das nach seiner Einführung Anpassungsfähigkeit zeigen kann und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebun- 178

---

[220] Zu den Vorgaben der EMRK und der Charta der CEPEJ ausführlich Bernhardt in Chibanguza/Kuß/Steege (Hrsg)., Künstliche Intelligenz, Recht und Praxis automatisierter und autonomer Systeme, 2021, S. 1076 f.

[221] Bernhardt, Verfassungsprinzipien. Verfassungsgerichtsfunktionen- Verfassungsprozessrecht im EWG-Vertrag, 1987, S. 41 ff.

[222] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence, abgerufen am 16.4.2022.

[223] https://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2024/0202_KI-VO.html?cms_mtm_campaign=linksFromNewsletter, abgerufen am 24.2.2024. Der im Folgenden dargestellte Text beruht auf einem geleakten Dokument, https://www.linkedin.com/posts/dr-laura-caroli-0a96a8a_ai-act-consolidated-version-activity-7155181240751374336-B3Ym/, abgerufen am 24.2.2024.

[224] Siehe Einzelheiten zum KI-Gesetz die Ausführungen von Bernhardt, Europäisches E-Government, → ■.

gen beeinflussen können".[225] Diese Definition stimmt weitgehend mit der Definition der OECD überein.

179 Die einzuhaltenden Pflichten richten sich nach der **Risikoklassifizierung** von KI-Systemen. Je höher das Risiko ist, desto strenger ist das einzuhaltende regulatorische Regime. Gemäß Erwägungsgrund 28a ist das Ausmaß der durch das KI-System verursachten negativen Auswirkungen auf die durch die Charta geschützten Grundrechte von besonderer Bedeutung für die Einstufung eines KI-Systems als hochriskant. Bezug genommen wird auf die Grundrechte der EU-Grundrechtecharta, etwa auf die Menschenwürde (Art. 1), die Achtung des Privat- und Familienlebens und den Schutz personenbezogener Daten (Art. 7 und 8), das Diskriminierungsverbot (Art. 21) und die Gleichstellung von Frauen und Männern (Art. 23). Verhindert werden soll eine Beeinträchtigung der Rechte auf freie Meinungsäußerung (Art. 11) und Versammlungsfreiheit (Art. 12). Zu den zu schützenden Rechten zählt der Erwägungsgrund auch das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht, die Unschuldsvermutung und das Verteidigungsrecht. Ein **unannehmbares Risiko** führt zur Konsequenz des Verbots bestimmter Anwendungen bzw. erheblicher Restriktionen (Art. 5 KI-Gesetz).

180 Die meisten durch die KI-Verordnung normierten Pflichten knüpfen an sogenannte **Hochrisikosysteme** (Art. 6) an. Als hochriskant eingestufte Systeme können nur dann zugelassen werden, wenn sie die Anforderungen für eine vertrauenswürdige KI erfüllen, die Anbieter eine Risikoeinschätzung und beabsichtigte Schutzmaßnahmen darlegen, wenn sie einen Prüfungsprozess mit Qualitätsmanagement- und Konformitätsbewertungsverfahren (Art. 17) durchlaufen haben, bevor sie auf dem Unionsmarkt in Verkehr gebracht werden können, und die Einrichtung, Durchführung und Aufrechterhaltung eines Systems zur Überwachung nach dem Inverkehrbringen sicherstellen. Anwender von Hochrisiko-KI müssen ein Risikomanagement einrichten sowie hohe Anforderungen an Datenqualität, Dokumentation, Transparenz und technischer Robustheit beachten. Weiters sind grundrechtliche Folgenabschätzungen (Human Rights Impact Assessments) zwingend durchzuführen.

181 Zu den Hochrisiko-Anwendungen zählen Systeme, die selbst Produkte oder Sicherheitskomponenten von Produkten sind, die im **Anhang II** der Harmonisierungsrechtsvorschriften der EU fallen und die einer Konformitätsprüfung unterzogen werden müssen. Daneben werden auch solche KI-Lösungen als Hochrisiko-Systeme definiert, die einem der Bereiche des **Anhang III der KI-Verordnung** unterfallen.

182 Generell sollen gemäß Art. 6 Abs. 2a KI-Gesetz die **Anwendungen von der Klassifizierung als Hochrisiko ausgenommen** werden, die kein signifikantes Risiko für die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen haben. Dies ist der Fall, wenn eines oder mehrere der folgenden Kriterien erfüllt sind: Das KI-System ist dazu bestimmt, eine eng begrenzte Verfahrensaufgabe auszuführen, das Ergebnis einer zuvor ausgeführten menschlichen Tätigkeit zu verbessern, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu bestimmt, die zuvor abgeschlossene menschliche Beurteilung zu ersetzen oder zu beeinflussen, ohne dass eine ordnungsgemäße menschliche Überprüfung stattfindet. Eine Ausnahme kommt auch in Betracht, wenn das KI-System eine vorbereitende Aufgabe für die in Anhang III aufgeführten Hochrisiko-Systeme wahrnehmen.

183 Genannt sind in Anhang III auch KI-Systeme, die dazu bestimmt sind, von einer Justizbehörde oder in deren Auftrag eingesetzt zu werden, um eine **Justizbehörde bei der Erforschung und Auslegung von Tatsachen und Gesetzen** sowie bei der **Anwendung des Rechts auf einen konkreten Sachverhalt** zu unterstützen, oder die in ähnlicher Weise **bei der alternativen Streitbeilegung eingesetzt** werden.

184 Kommt ein Anbieter zu der Auffassung, dass ein KI-System nach Anhang III kein hohes Risiko darstellt, muss er seine Einschätzung dokumentieren, bevor das System in Verkehr gebracht oder in Betrieb genommen wird, und muss das KI-System gemäß Art. 51 Abs. 1a

[225] Die hier und im Folgenden verwandten deutschsprachigen Zitate des KI-Gesetzes beruhen auf einer nicht amtlichen Übersetzung des bisher (Februar 2024) nur auf Englisch verfügbaren Textes.

registrieren. Auf Verlangen der zuständigen nationalen Behörden muss Anbieter die Dokumentation der Bewertung vorlegen.

185 **Erwägungsgrund 40** führt dazu aus, dass bestimmte KI-Systeme, die für die **Rechtspflege und demokratische Prozesse** bestimmt sind, als **risikoreich eingestuft** werden sollten, da sie potenziell erhebliche Auswirkungen auf Demokratie, Rechtsstaatlichkeit, individuelle Freiheiten sowie das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren haben. Um den Risiken potenzieller Voreingenommenheit, Fehler und Undurchsichtigkeit zu begegnen, sei es insbesondere angebracht, KI-Systeme, die von einer Justizbehörde oder in deren Auftrag eingesetzt werden sollen, um die Justizbehörden bei der Recherche und Auslegung von Fakten und Gesetzen sowie bei der Anwendung des Rechts auf einen konkreten Sachverhalt zu unterstützen, als hochriskant einzustufen. Allerdings wird auch die Nützlichkeit der KI-Instrumente für die Richterinnen und Richter hervorgehoben, denn der Einsatz von Werkzeugen der künstlichen Intelligenz könne die Entscheidungsfähigkeit oder die richterliche Unabhängigkeit unterstützen. Andererseits sollte die Künstliche Intelligenz Richterinnen und Richter nicht ersetzen, da die endgültige Entscheidungsfindung eine von Menschen gesteuerte Tätigkeit und Entscheidung bleiben müsse.

186 Schließlich erwähnt Erwgr.40, dass die Zuordnung zur Hochrisikoklasse sich nicht auf KI-Systeme erstrecken solle, die für rein verwaltungstechnische Nebentätigkeiten bestimmt sind, die sich nicht auf die eigentliche Rechtsprechung im Einzelfall auswirken, zB die Anonymisierung oder Pseudonymisierung gerichtlicher Entscheidungen bzw. die Kommunikation zwischen dem Personal, die Verwaltungsaufgaben oder die Zuweisung von Ressourcen.

187 Generell sollen gemäß Art. 6 Abs. 2a die Anwendungen **von der Klassifizierung als Hochrisiko ausgenommen** werden, die **kein signifikantes Risiko für die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen** haben. Dies ist der Fall, wenn eines oder mehrere der folgenden Kriterien erfüllt sind: Das KI-System ist dazu bestimmt, eine eng begrenzte Verfahrensaufgabe auszuführen, das Ergebnis einer zuvor ausgeführten menschlichen Tätigkeit zu verbessern, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu bestimmt, die zuvor abgeschlossene menschliche Beurteilung zu ersetzen oder zu beeinflussen, ohne dass eine ordnungsgemäße menschliche Überprüfung stattfindet. Eine Ausnahme kommt auch in Betracht, wenn das KI-System eine vorbereitende Aufgabe für die in Anhang III aufgeführten Hochrisiko-Systeme wahrnehmen.

188 Titel VIIIA enthält Sonderregelungen für KI-Modelle mit allgemeinem Verwendungszweck (sogenannte **General Purpose AI Models oder GPAI-Modelle**), Art. 52a ff. Ein GPAI-Modell ist gemäß Art. 3 Abs. 44b des KI-Gesetzes ein Modell, „das mit einer großen Datenmenge und in großem Maßstab unter Selbstüberwachung trainiert wurde, dass eine erhebliche Allgemeinheit aufweist und in der Lage ist, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, unabhängig davon, wie das Modell auf den Markt gebracht wird, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann. Das umfasst nicht KI-Modelle, die vor ihrer Veröffentlichung auf dem Markt für Forschungs-, Entwicklungs- und Prototyping-Aktivitäten verwendet werden." Hier gelten besondere Pflichten, wobei gemäß den Art. 52a ff. zwischen **einfachen GPAI-Modellen** und solchen mit **systemischem Risiko** (also einer Rechenleistung für das KI-Training mit mehr als 10^25 FLOPS) zu unterscheiden ist (Art. 52a Abs. 2). Für die Justiz kommt der Einsatz von GPAI-Modellen theoretisch in Betracht, der Einsatz (etwa „ChatGPT") müsste allerdings anhand der Vorgaben des KI-Gesetzes intensiv geprüft werden.

189 Der **Einsatz von KI-Systemen mit hohem Risiko** bedarf gem. Art. 14 stets einer **wirksamen „menschlichen Aufsicht".** Verwaltungsmitarbeiter dürfen sich also nicht auf den von einem KI-System mit hohem Risiko erzeugten Output zu verlassen bzw. müssen sich der Gefahren einer „automation bias" (die Neigung von Menschen, Vorschläge von automatisierten Entscheidungssystemen zu bevorzugen), insbesondere wenn KI dazu verwendet wird, Informationen oder Empfehlungen für Entscheidungen zu liefern. „Menschliche Aufsicht" bedeutet, dass „der Nutzer keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange dies nicht von mindestens zwei natürlichen Personen überprüft und bestätigt wurde" (Art. 14 Abs. 5). Der Verwaltungsangehörige als „Mensch" muss insoweit in der Lage sein, das AI-System für

hohe Risiken nicht zu verwenden oder die Ergebnisse des AI-Systems für hohe Risiken anderweitig zu ignorieren, außer Kraft zu setzen oder umzukehren.

9. Blockchain in der Justiz

190 Bei der Blockchain handelt sich um eine verteilte Datenbank, in der die Datenblöcke wie bei einer Kette (Chain) aneinandergereiht werden.[226] An den Ursprungsblock werden immer neue Datenblöcke chronologisch angehängt werden, nachdem sie überprüft und bestätigt wurden. Mittels peer-to-peer-Netzwerken und kollektiver Registrierung der Transaktionen („Distributed Ledger")wird sichergestellt, dass Transaktionen rückwirkend nicht geändert werden können. Jeder, der an dem Blockchain-System teilnimmt, speichert auf seinem Rechner eine vollständige Kopie der Datenhistorie. Dies beugt Manipulationen vor, da eine manipulierte Kopie nicht auf das ganze System durchschlägt. Es müsste, um Gefahren auszulösen, jeder einzelne teilnehmende Computer manipuliert werden. Das System ist gegen Angriffe und Netzausfällt geschützt. Die Reihenfolge der Blöcke ist noch zusätzlich durch eine Prüfsumme gesichert, so dass die Reihenfolge der Blöcke nicht nachträglich geändert werden kann. Es ist eine Verfolgung und Prüfung von Erweiterungen der Blockchain möglich. Die Blockchain wird algorithmisch gesteuert. Ihre Veränderung erfolgt nach ex ante definierten Regeln. Anwendungsfelder der Blockchain im Bereich E-Justice könnten perspektivisch vor allem die Justizregister sein, etwa Grundbücher, wobei auch insoweit die verfassungsrechtlichen Grenzen zu beachten sind.[227]

10. Legal Tech

191 Legal Technology (kurz Legal Tech) befasst sich mit der Automatisierung von juristischen Tätigkeiten mithilfe der Informationstechnologie. Üblich ist auf der Basis von Oliver R. Goodenough[228] die Beschreibung verschiedener Wirkungsphasen bzw. Entwicklungsstufen: von Legal Tech 1.0 mit einer computergestützten Büroorganisation und Kommunikation (etwa Dokumentenverwaltung, Buchhaltung und Onlinedienste) über Legal Tech 2.0 mit der Automatisierung standardisierter juristischer Tätigkeiten bis hin zu Legal Tech 3.0 und der Einbeziehung von Künstlicher Intelligenz in die juristische Tätigkeit.[229] Einsatzfelder von Legal Tech sind heute vor allem Internetplattformen, die Nutzerinnen und Nutzer in einfacher Weise bei der Ermittlung rechtsrelevanter Tatsachen unterstützen und daraus Erkenntnisse für die Geltendmachung von Rechtsansprüchen gewinnen lassen. Dies betrifft etwa die Berechnung von Ausgleichs- und Entschädigungsansprüchen bei der Annullierung und Verspätung von Flügen aufgrund der Art. 4 Abs. 3 und Art. 5 Abs. 1c Fluggastrechte-VO oder die Durchsetzung von Mietrückzahlungsansprüchen.[230] Vertragsgeneratoren helfen dabei, auf der Grundlage von Standardvertragsmustern individuelle Vertragstexte zu erstellen, eine Smart Contracts-Software führt selbständig Rechtshandlungen zur Erfüllung von Verträgen aus. Rechtlich geht es bei Lega-Tech-Dienstleistungen teilweise um Inkassodienstleistungen gemäß § 10 Abs. 1 Nr. 1 RDG. Der BGH hat Rechtsdienstleistungsportale in gewissen Grenzen als vereinbar mit dem RDG angesehen.[231] Von der Inkassodienstleistungsbefugnis eines nach § 10 Abs. 1 S. 1 Nr. 1 RDG registrierten Inkassodienstleisters sei es (noch) gedeckt, „wenn dieser auf seiner Internetseite einen ‚Mietpreisrechner' zur – zunächst unentgeltlichen – Berechnung der ortsüblichen Vergleichsmiete zur Verfügung stellt und im An-

[226] Siehe zur Funktionsweise der Blockchain Ory/Weth/Biallaß, jurisPK-ERV Band 1, 2. Aufl., Kapitel 8 (Stand: 23.11.2022), Rn. 84 ff ff.; Wahedi, Verfassungsrechtliche Anforderungen an die Automatisierung der Justiz, S. 103 ff. jeweils mwN.

[227] Wahedi, Verfassungsrechtliche Anforderungen an die Automatisierung der Justiz, S. 111 ff.

[228] Huffpost v. 2.4.2015, https://www.huffpost.com/entry/legal-technology-30_b_6603658, abgerufen am 29.2.2024.

[229] Leeb, Digitalisierung, Legal Technology und Innovation, 2019, S. 51 ff.; Hähnchen/Schrader/Weiler/Wischmeyer JuS 2020, 625. Zu den weiteren Definitionen: Ory/Weth/Biallaß, jurisPK-ERV Band 1, 2. Aufl., Kapitel 8 (Stand: 23.11.2022), Rn. 2.

[230] https://conny.de/abgerufen am 29.2.2024.

[231] BGH-27.11.2019 – VIII ZR 285/18, ZIP 2019, 2065 = BeckRS 2019, 30591. dazu Prütting 2020, 49; NJW 2020, 208, 213 ff. mwN.

schluss hieran dem Mieter die Möglichkeit gibt, ihn durch Anklicken eines Buttons mit der außergerichtlichen Durchsetzung von – näher bezeichneten – Forderungen und etwaigen Feststellungsbegehren gegen den Vermieter im Zusammenhang mit der „Mietpreisbremse" – unter Vereinbarung eines Erfolgshonorars in Höhe eines Drittels der jährlichen Mietersparnis (vier Monate) sowie einer Freihaltung des Mieters von sämtlichen Kosten – zu beauftragen und in diesem Zusammenhang die genannten Ansprüche zum Zweck der Durchsetzung treuhänderisch an den Inkassodienstleister abzutreten, der im Falle einer Erfolglosigkeit der eigenen außergerichtlichen Rechtsdienstleistungstätigkeit einen Vertragsanwalt mit der anwaltlichen und gegebenenfalls auch gerichtlichen Durchsetzung der Ansprüche beauftragen kann, zum Abschluss eines Vergleichs jedoch grundsätzlich nur mit Zustimmung des Mieters befugt ist." Bei der Auslegung des § 10 Abs. 1 S. 1 Nr. 1 RDG sei eine „großzügige Betrachtung" geboten.

11. Reformdiskussion und Modernisierungsbestrebungen in der Zivilgerichtsbarkeit

Es wurde bereits auf den Bericht der Arbeitsgruppe „Modernisierung des Zivilprozesses" im Auftrag der Präsidentinnen und Präsidenten der Oberlandesgerichte, des Kammergerichts, des Bayerischen Obersten Landesgerichts und des Bundesgerichtshofs hingewiesen.[232] Über die bereits erörterten Vorschläge hinaus hat die Arbeitsgruppe ua einen elektronischen Nachrichtenraum vorgeschlagen, in dem formlose Nachrichten insbesondere zur Organisation des Verfahrens, zB zur Terminabstimmung ausgetauscht werden können. Ferner soll ein bundesweiter einheitlicher elektronischer Bürgerzugang in Gestalt eines Online-Portals eingerichtet werden, der teilweise die Aufgaben der Rechtsantragstellen übernehmen und für Erklärungen im Rahmen eines neu einzuführenden Online-Verfahrens dienen soll. Schließlich schlägt die Arbeitsgruppe vor, anhand eines elektronischen Basisdokuments[233] den Prozessstoff zu sammeln und gegenüberzustellen. Dieses Basisdokument soll den Austausch von Schriftsätzen und auch den Tatbestand des Urteils ersetzen. Rn. **192**

Über diese Vorschläge werden inzwischen weitere Ideen erörtert, zB zur Idee einer gerichtlichen E-Akte in der Cloud und zum „gerichtlichen elektronischen Datenraum"[234] und zu einem ausgeweiteten strukturierten Parteivortrag.[235] **193**

Insgesamt fehlt es oft in den für die Justiz verantwortlichen Ländern an den erforderlichen Ressourcen. Deshalb hat die Ampel-Koalitionsvereinbarung angekündigt, mit den Ländern den Pakt für den Rechtsstaat zu verstetigen und ihn um einen „Digitalpakt für die Justiz" zu erweitern.[236] Bereits die große Koalition von CDU/CSU und SPD hatte in ihrem Koalitionsvertrag von 2018 einen „Pakt für den Rechtsstaat" vorgesehen,[237] der in einem Beschluss der Ministerpräsidentenkonferenz konkretisiert worden war. Zwar enthielt der Pakt auch einen Abschnitt „Digitalisierung". Darin ging es allerdings praktisch ausschließlich um den medienbruchfreien Austausch zwischen Polizei und Staatsanwaltschaft, die Schaffung einer Kommunikationsschnittstelle zwischen Justiz und Polizei und die Einrichtung eines Polizei-IT-Fonds.[238] Zuletzt ging es darum, insgesamt die Justizdigitalisierung in einer gemeinsamen Kraftanstrengung von Bund und Ländern zu forcieren. Nach langem Ringen zwischen Bund und Ländern wurde auf drei Bund-Länder-Digital-Gipfel zuletzt im Mai und im November 2023 Einigkeit über Finanzierungsfragen und die gemeinsam zu **194**

[232] https://www.justiz.bayern.de/media/images/behoerden-und-gerichte/oberlandesgerichte/nuernberg/diskussionspapier_ag_modernisierung.pdf, abgerufen am 29.2.2024.

[233] Siehe dazu Greger, NJW 2019, 3429, 3431 ff.

[234] Siehe zu weiterreichenden Reformvorschlägen Ory/Weth/Köbler, jurisPK-ERV Band 1, 2. Aufl., Kapitel 7 1. Überarbeitung (Stand: 16.1.2024).

[235] Zwickel, Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, Tagungsband zur 3. Tagung junger Prozessrechtswissenschaftler und -wissenschaftlerinnen 2017, Schriften zum Prozessrecht, Bd. 246 (2018), 179.

[236] https://fragdenstaat.de/dokumente/142083-koalitionsvertrag-2021–2025/ Rn. 3527 f.

[237] Koalitionsvertrag vom 18.3.2018, S. 123, https://www.bundesregierung.de/breg-de/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906, abgerufen am 29.2.2024.

[238] https://www.bundesregierung.de/breg-de/suche/bund-und-laender-einig-pakt-fuer-den-rechtsstaat-kommt-1556186, abgerufen am 29.2.2024.

verantworteten Projekten erzielt.[239] Es gibt ua Planungen (deren Realisierung teilweise schon begonnen wurde) für die Entwicklung und Erprobung eines zivilgerichtlichen Online-Verfahrens, für die Entwicklung einer digitalen Rechtsantragstelle sowie für die Entwicklung des Videoportals der Justiz sowie für die Konzeption einer bundeseinheitlichen Justizcloud und für die Erstellung eines Grobkonzepts für die Entwicklung einer Vollstreckungsdatenbank.

12. Justizregister

195 **a) Allgemein.** Es gibt in Deutschland über 350 verschiedene, über alle föderalen Ebenen hinweg verteilte Registertypen.[240] Die Datensätze dieser Register, die für verschiedene Verwaltungsvorgänge genutzt werden, sind nicht systematisch miteinander vernetzt. Behörden, die Anträge einer Bürgerin oder eines Bürgers bearbeiten, können und dürfen die erforderlichen Informationen und Nachweise aus datenschutzrechtlichen Gründen ohne entsprechende Einwilligung der betroffenen Bürgerinnen und Bürger nicht aus den Registern anderer Behörden heraussuchen, müssen diese vielmehr oft bei Bürgerinnen und Bürgern erneut erheben, obwohl die entsprechenden Dokumente schon mehrfach an anderer Stelle vorliegen. Zur Realisierung des europarechtlich vorgesehenen Once-Only-Prinzips,[241] bedarf es allerdings einer qualitätsgesicherten Verknüpfung der Datensätze in verschiedenen Registern mit dem jeweiligen Antragsteller anhand gemeinsamer Ordnungsmerkmale. Das Registermodernisierungsgesetz[242] zielt darauf ab, Verwaltungsdaten mithilfe eines veränderungsfesten Ordnungsmerkmals – nämlich der sogenannten Steuer-ID – zur richtigen Person zuzuordnen, um auf diese Weise ua das sogenannte „Once-Only-Prinzip"-des Onlinezugangsgesetz zu realisieren. Gespeicherte Daten und Nachweise können auf diese Weise mehrfach verwandt werden und müssen nicht immer wieder abgefragt werden. Die Justizregister sind nur teilweise vom Registermodernisierungsgesetz erfasst, etwa das Handelsregister. Das sogenannte Datenschutzcockpit, das schrittweise mit der Identifikationsnummer vorgesehen ist, soll den betroffenen Bürgerinnen und Bürger die Prüfung ermöglichen, welche ihrer Daten auf Grundlage der Steuer-ID zwischen öffentlichen Stellen ausgetauscht wurden.

196 Durch eine Novellierung des Onlinezugangsgesetzes, das der Deutsche Bundestag am 23.2.2024 beschlossen hat,[243] sollen die Strukturen der Bund-Länder-Zusammenarbeit verstetigt und ua auch Regelungen zu Digital-Only für Unternehmensleistungen eingeführt werden.

197 **b) Elektronisches Handelsregister und elektronisches Unternehmensregister.** Bereits seit 2007 wird das Handelsregister vollständig elektronisch geführt.[244] Sowohl die Übermittlung und Einreichung der Anmeldungen zur Eintragung als auch die Beauskunftung über den Inhalt der Eintragungen und der hinterlegten Dokumente erfolgen mittels elektronischer Informations- und Kommunikationssysteme (über das EGVP). Die rechtlichen und technischen Grundlagen sind in den §§ 8 bis 12 Handelsgesetzbuch (HGB) und in der Handelsregisterverordnung (HRV) geregelt. Bereits seit langer Zeit können die Daten der Handelsregister über das gemeinsame Registerportal der Länder www.handelsregister.de und www.unternehmensregister.de online abgerufen werden (vgl. die §§ 8, 8b HGB), wobei die Firmen-Recherche und der Abruf von Veröffentlichungen kostenfrei sind, die übrigen

[239] https://www.bmj.de/SharedDocs/Meldungen/DE/2023/1110_Digitalgipfel_PM.html.

[240] https://www.it-planungsrat.de/projekte/projekte-des-it-planungsrat/registermodernisierung, abgerufen am 29.2.2024.

[241] Art. 14 der EU-Verordnung vom 2.10.2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012.

[242] Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz) vom 28.3.2021 (BGBl. I S. 591), zuletzt geändert durch Artikel 11 des Gesetzes vom 9.7.2021 (BGBl. I S. 2467).

[243] BT-Drs. 20/8093.

[244] Einführung auf der Grundlage des Gesetzes über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG) vom 10.11.2006, BGBl. I, S. 2553, das wiederum die Richtlinien 2003/58/EG, 68/151/EWG, 2004/109/EG sowie 2001/34/EG umsetzte.

Abrufe nach erforderlicher Registrierung kostenpflichtig sind. Die Dokumente werden über das Elektronische Gerichts- und Verwaltungspostfach (EGVP) beim Handelsregister eingereicht. Gemäß § 12 Abs. 1 S. 1 HGB müssen die Anmeldungen zur Eintragung allerdings in öffentlich (durch einen Notar, § 129 BGB) beglaubigter Form eingereicht werden. Die Beglaubigung kann elektronisch erfolgen, indem das einzureichende elektronische Dokument von dem Notar mit einer qualifizierten elektronischen Signatur versehen wird, vgl. § 39a BeurkG. Mit dem Gesetz zur Umsetzung der Digitalisierungsrichtlinie (DiRUG)[245] wurden die Online-Gründung der GmbH sowie weitere Online-Verfahren für Registeranmeldungen ab dem 1.8.2022 ermöglicht. Die Digitalisierungsrichtlinie zielt darauf ab, europaweit grenzüberschreitend durch den Einsatz digitaler Instrumente und Verfahren die Gründung von Gesellschaften und die Errichtung von Zweigniederlassungen zu vereinfachen. Dies dient wiederum der Effizienz und Kosteneinsparung. Ua verpflichtet die Richtlinie zur Einführung der Online-Gründung der GmbH, zu Online-Verfahren bei Registeranmeldungen für Kapitalgesellschaften und Zweigniederlassungen, zur Einreichung und Offenlegung von Urkunden und Informationen im Handels- und Unternehmensregister sowie zum grenzüberschreitenden Informationsaustausch über das Europäische System der Registervernetzung. Von der Möglichkeit, die Umsetzungsfrist vom 1.8.2021 um ein Jahr hinauszuschieben, hat Deutschland Gebrauch gemacht.

198 Das deutsche Recht sieht traditionell die notariellen Mitwirkung bei der Gründung einer GmbH sowie bei der Eintragung und Einreichung von Urkunden und Informationen zum Handelsregister vor und hat sich bereits aus Anlass der Digitalisierung der Handelsregister dafür entschieden, anstelle einer – technisch möglichen und vorstellbaren – unmittelbaren elektronischen Anmeldung durch die Gesellschafter (wie in einigen EU-Mitgliedstaaten üblich) weiterhin die Einbindung der Notare in die Anmeldungen zu den Registern vorgesehen. Maßgebend hierfür sind die Wahrung der etablierten Grundsätze und Prinzipien des deutschen Handels- und Gesellschaftsrechts“,[246] die Wahrung der „Funktionsfähigkeit und Verlässlichkeit der Handels-, Genossenschafts- und Partnerschaftsregister“ sowie die Rolle der Notarinnen und Notare für den Rechts- und Geschäftsverkehr. Das zum 1.8.2022 in Kraft getretene „Gesetz zur Umsetzung der Digitalisierungsrichtlinie“ (DiRUG) beseitigt das Erfordernis, für eine GmbH-Gründung persönlich bei einem Notar zu erscheinen. Es hat die gesetzlichen Rahmenbedingungen für die Vornahme virtueller notarieller Beurkundungen und Beglaubigungen im Handels- und Gesellschaftsrecht geschaffen. Der Notar kann nun virtuell gemäß § 2 Abs. 3 GmbHG nF mithilfe eines besonders gesicherten Videokommunikationssystems einschließlich einer qualifizierten elektronischen Signatur eingebunden werden. § 2 Abs. 3 GmbHG verweist dabei auf die §§ 16a bis 16e BeurkG., die die genauere Durchführung regeln. Zur Identifikation der Gesellschafter wird ein elektronischer Identitätsnachweis wie beispielsweise ein Personalausweis mit eID-Funktion benötigt.

199 Ferner ist seitdem gem. § 12 Abs. 1 S. 2 HGB für die Anmeldung der GmbH die öffentliche Beglaubigung mittels Videokommunikation (§ 40a BeurkG.) zulässig. Demnach kann bei Einzelkaufleuten und Kapitalgesellschaften sowie deren Zweigniederlassungen die notarielle Beglaubigung von Handelsregisteranmeldungen mittels Videokommunikation stattfinden, so dass eine persönliche Anwesenheit beim Notar entbehrlich wird. Mit dem Gesetz zur Ergänzung der Regelungen zur Umsetzung der Digitalisierungsrichtlinie[247] wurden diese Vorschriften ergänzt: Die Zulässigkeit der Online-Beglaubigung von Handelsregisteranmeldungen ist seitdem nicht mehr auf bestimmte Rechtsträger beschränkt, sondern für sämtliche Rechtsträger möglich sein. Gleichzeitig wurden die Anmeldungen zum Partnerschafts-, Genossenschafts- und Vereinsregister ebenfalls in den Anwendungsbereich des notariellen

[245] vom 5.7.2021. Das Gesetz zur Umsetzung der Digitalisierungsrichtlinie (DiRUG) dient der Umsetzung der Richtlinie (EU) 2019/1151 des Europäischen Parlaments und des Rates vom 20.6.2019 zur Änderung der Richtlinie (EU) 2017/1132 im Hinblick auf den Einsatz digitaler Werkzeuge und Verfahren im Gesellschaftsrecht, ABl. L 186 vom 11.7.2019, S. 80.

[246] Begründung des Entwurfs eines Gesetzes zur Umsetzung der Digitalisierungsrichtlinie (BT-Drs. 19/28177).

[247] Gesetz zur Ergänzung der Regelungen zur Umsetzung der Digitalisierungsrichtlinie und zur Änderung weiterer Vorschriften vom 15.7.2022, BGBl. I 2021, BGBl. 2022, 1146.

Online-Beglaubigungsverfahrens einbezogen. Ferner wurden notariellen Beurkundungen von Willenserklärungen im Rahmen der Gründung von Gesellschaften mit beschränkter Haftung (GmbH) mittels Videokommunikation auf Sachgründungen erstreckt. Das Bundesjustizministerium plant ferner mit dem (Referenten-) Entwurf eines Gesetzes zur Einführung einer elektronischen Präsenzbeurkundung eine notarielle Beurkundung mithilfe des Einsatzes von Unterschriftenpads.[248]

200 **c) Elektronisches Genossenschaft- und Partnerschaftsregister, Elektronisches Vereinsregister und elektronisches Gesellschaftsregister.** Auf der Basis des Genossenschaftsgesetzes und der Verordnung über das Genossenschaftsregister wurde das **Genossenschaftsregister** in Deutschland als öffentliches Register beim Amtsgericht eingerichtet, aus dem sich die Rechtsverhältnisse einer eingetragenen Genossenschaft (eG) ersehen lassen. Bereits das Registerverfahrenbeschleunigungsgesetz von 1993 eröffnete die rechtliche Möglichkeit, das Genossenschaftsregister in elektronischer Form zu führen. Einzureichen sind ua der Gründungsvertrag und die rechtlich relevanten Änderungen. Das (öffentliche) Partnerschaftsregister wird beim Amtsgericht mit den Angaben über die wesentlichen Rechtsverhältnisse einer Partnerschaft als juristischer Person, zu der sich Angehörige freier Berufe zusammenschließen können, geführt, in der sich Angehörige freier Berufe zusammenschließen können. Das Gesetz zur Modernisierung des Personengesellschaftsrechts (MoPeG) vom 10.8.2021, das im Wesentlichen am 1.1.2024 in Kraft trat,[249] sieht vor, dass ein Gesellschaftsregister eingeführt, in dem sich eine GbR eintragen lassen kann (die sich dann als eGbR bezeichnen kann), wenn die Gesellschaft ihrerseits ein registriertes Recht, wie etwa ein Grundstück, erwerben will.

201 **d) Elektronisches Grundbuch.** *aa)Elektronische Führung des Grundbuchs und elektronischer Rechtsverkehr zum Grundbuch.* Bereits durch das Registerverfahrensbeschleunigungsgesetz vom 20.12.1993[250] wurden die Grundbuchordnung und die Grundbuchverfügung um Vorschriften für die maschinelle Grundbuchführung ergänzt (§§ 126 ff. GBO, §§ 61 ff. GBV). Seitdem können das Grundbuch und die Hilfsverzeichnisse nicht mehr nur auf Papier, sondern rechtswirksam auf elektronischen Datenträgern geführt werden, was in allen Ländern in Deutschland realisiert wurde. Ferner können die für eine Grundbucheintragung erforderlichen Dokumente als elektronische Dokumente übermittelt und vom Grundbuchamt in einer elektronischen Akte aufbewahrt werden.[251] Allerdings bedarf die für die Eintragung ins Grundbuch erforderliche Erklärung auch in den Fällen des elektronischen Rechtsverkehrs der notariellen Beurkundung oder Beglaubigung. Von der notariellen Urkunde wird dem Grundbuchamt vom Notar eine beglaubigte elektronische Abschrift übermittelt, die eine zuverlässige Prüfung der Authentizität und der Integrität des elektronischen Dokuments ermöglicht. Reformbestrebungen, diese Beurkundung auch online (virtuell) zu ermöglichen, sind bisher nicht bekannt. Die Notare können dabei zur Teilnahme am elektronischen Rechtsverkehr verpflichtet werden. Gemäß 133 GBO kann in das maschinell geführte Grundbuch im automatisierten Abrufverfahren Einsicht genommen werden, allerdings ist dies auf bestimmte Stellen und Personen beschränkt und nur mit Genehmigung der Landesjustizverwaltung zulässig, § 133 Abs. 2 S. 1, Abs. 4 Satz 2 GBO. Zu differenzieren ist zB in Berlin zwischen dem uneingeschränkten Abrufverfahren (Gerichte, Behörden, Notare, öffentlich bestellte Vermessungsingenieure), dem eingeschränkten Abrufverfahren (Personen und Stellen, die vom Eigentümer/Erbbauberechtigten zur Einsicht ermächtigt wurden, Personen oder Stellen, die die Zwangsvollstreckung betreiben, Inhaber von Rechten an einem Grundstück, einem grundstücksgleichen Recht oder an einem Recht an einem solchen Recht, Versorgungsunternehmen (für Elektrizität, Gas, Fernwärme, Wasser/Abwasser, Tele-

[248] https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2024_Praesenzbeurkundung_Einfuehrung.html, abgerufen am 29.2.2024.

[249] BGBl. 2021, 3436.

[250] BGBl. I 1993, 2182.

[251] Auf der Basis des Gesetzes zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Akte im Grundbuchverfahren sowie zur Änderung weiterer grundbuch-, register- und kostenrechtlicher Vorschriften (ERVGBG) und der entsprechenden Verordnungen der Länder.

kommunikation). Beim eingeschränkten Abrufverfahren müssen die Personen oder Stellen das Vorliegen der Voraussetzungen, die ihr berechtigtes Interesse begründen, beim einzelnen Abruf in codierter Form erklären (Darlegungserklärung). Sämtliche Abrufe werden aus datenschutzrechtlichen Gründen protokolliert.[252] Ferner besteht für Notare, die am automatisierten Abrufverfahren teilnehmen, die Möglichkeit, sich über durchgeführte Grundbucheintragungen per E-Mail benachrichtigen zu lassen.

bb) Elektronische Einsichtnahme. Gemäß § 133 Abs. 2 S. 3 GBO erfolgt die Einsicht- 202
nahme entweder über einen Bildschirm oder in Form eines Bildschirmabdrucks.

cc) Datenbankgrundbuch. Das bisherige elektronische Grundbuch erfüllt die Erwartun- 203
gen an ein modernes, recherchierbares elektronisches Register nicht. Mithilfe des Datenbankgrundbuch sollen zukünftig Grundbuchinhalte maschinenlesbar gestaltet werden. Inhalte werden strukturiert und sollen logisch verknüpft werden. Dadurch sollen neue Recherche- und Auskunftsmöglichkeiten entstehen. Ferner soll das Datenbankgrundbuch schnellere Informationen über Dienstbarkeiten ermöglichen, die sich über viele bzw. mehrere Grundstücke erstrecken. Mit dem Gesetz zur Einführung eines Datenbankgrundbuchs (DaBaGG) vom 1.10.2013[253] wurde die Rechtsgrundlage für die Einführung eines vollstrukturierten Datenbankgrundbuchs geschaffen. Mit dem Gesetz werden die Landesregierungen ermächtigt, Zeitpunkt und Umfang der Einführung des Datenbankgrundbuchs für das jeweilige Land zu bestimmen. Das Gesetz sieht neue, übersichtlichere und den jeweiligen Bedürfnissen angepasste Darstellungsformen des Grundbuchinhalts und neue Auskunfts- und Recherchemöglichkeiten neben den bisherigen Darstellungsformen vor. Da die Erstellung des digitalen Datenbankgrundbuchs mit der Überführung von 36 Millionen Grundbuchblättern in Strukturdaten (also etwa 400 Millionen Seiten)[254] einen erheblichen Umstellungsaufwand erfordert, wurde das (zunächst) 16-Länder-Projekt „Entwicklung eines bundeseinheitlichen Datenbankgrundbuchs (dabag)"begründet, mit dem die Realisierung eines bundesweit einheitlichen Softwaresystems zur Speicherung und Bearbeitung von maschinell geführten Grundbüchern in voll strukturierter Form sowie die Online-Beauskunftung der Grundbücher bundesweit erreicht werden sollte. Nach Beginn der Vorbereitungsarbeiten vor ca. 20 Jahren wurde am 4.1.2016 in diesem Zuge die Projektphase „Realisierung und Pilotierung" eingeleitet und am 6.3.2019 eine Vertragsänderung unterzeichnet, wonach die Projektlaufzeit um 26 Monate verlängert wurde.[255]

e) Zentrales Testamentsregister. Es wird seit dem 1.1.2012 von Bundesnotarkammer ge- 204
führt. Es enthält die Verwahrangaben zu sämtlichen erbfolgerelevanten Urkunden, die vom Notar errichtet werden oder in gerichtliche Verwahrung gelangen. Bei einem Sterbefall hat das zuständige Nachlassgericht das Register von Amts wegen auf dort vorhandene Testamente bzw. andere erbfolgerechtliche Urkunden zu überprüfen, worauf die Bundesnotarkammer als registerführende Stelle mitteilt, ob und welche Verfügungen von Todes wegen zu beachten sind.

f) Das Zentrale Vorsorgeregister (ZVR).[256] Die Bundesnotarkammer führt im gesetzlichen 205
Auftrag des Bundesministeriums der Justiz das elektronische Zentrale Vorsorgeregister, in dem private sowie notarielle Vorsorgevollmachten, Betreuungsverfügungen und Patientenverfügungen registriert sind. Deutschlandweit und rund um die Uhr können Betreuungsgerichte den Inhalt des Zentralen Vorsorgeregisters einsehen bzw. sind aufgrund des Amtsermittlungsgrundsatzes dazu verpflichtet, um Kontakt zu den Vertrauenspersonen aufzunehmen. So kann ein Arzt vor einer Operation beim Gericht eine Betreuerbestellung

[252] Siehe zu den einzelnen Bedingungen des Abrufverfahrens etwa Informationen der Berliner Gerichte, https://www.berlin.de/gerichte/was-moechten-sie-erledigen/ , abgerufen am 29.2.2024. Übersicht zu den einzelnen Landesregelungen https://www.elrv.info/elektronischer-rechtsverkehr/uebersicht-verordnungen, abgerufen am 29.2.2024.

[253] BGBl. I 2013. 3719.

[254] Büttner, JurPC Web-Dok. 117/2016, Abs. 72.

[255] https://www.grundbuch.eu/nachrichten/ , abgerufen am 29.2.2024.

[256] https://www.vorsorgeregister.de/, abgerufen am 29.2.2024.

beantragen und das Gericht kann durch Einsichtnahme in das Vorsorgeregister eine dort registrierte Vorsorgevollmacht mit dem Namen des Bevollmächtigten herausfinden.

206 **g) Zentrales Schutzschriftenregister (ZSSR).** Dieses zentrale, länderübergreifende elektronische Register[257] wird seit 1.1.2016 für alle Länder beim Oberlandesgericht Frankfurt am Main geführt. Registriert sind dort Schutzschriften im Sinne vorbeugender Verteidigungsschriftsätze gegen erwartete Anträge auf Arrest oder einstweilige Verfügung (§ 945a Abs. 1 S. 2 ZPO). Online-Formulare sind unter www.zssr.justiz.de abrufbar.[258] Sobald eine Schutzschrift in das zentrale elektronische Schutzschriftenregister (ZSSR) eingestellt ist, gilt sie als bei allen ordentlichen Gerichten der Länder (§ 945a Abs. 2 S. 1 ZPO) und allen Arbeitsgerichten der Länder (§§ 62 Abs. 2 S. 3, 85 Abs. 2 S. 3 ArbGG) eingereicht.

207 Um der Einreichungsfiktion Genüge zu tun, hat das Gericht nach Antragseingang zu recherchieren, ob eine Schutzschrift in dieser Sache im Register eingestellt ist; das Gericht muss selbst die erforderlichen organisatorischen Maßnahmen treffen, um die Beachtung einer eventuell im Schutzschriftenregister eingereichten Schutzschrift zu gewährleisten.[259] Die auf § 945b ZPO beruhende Verordnung über das elektronische Schutzschriftenregister v. 24.11.2015[260] konkretisiert in ihrem § 2 die Anforderungen an eine ordnungsgemäße Einreichung von Schutzschriften. Sechs Monate nach ihrer Einstellung sind die Schutzschriften zu löschen. Seit dem 1.1.2017 sind Rechtsanwältinnen und Rechtsanwälte verpflichtet, Schutzschriften ausschließlich zum Schutzschriftenregister einzureichen, § 49c BRAO.[261]

208 **h) Elektronisches Urkundenarchiv.** § 78h BNotO[262] verpflichtet die BNotK zum Betrieb des Elektronischen Urkundenarchivs. Dieses zentrale elektronische Archiv ermöglicht den Notaren die Führung der elektronischen Urkundensammlung, des Urkundenverzeichnisses und des Verwahrungsverzeichnisses. Das Elektronische Urkundenarchiv stellt den für die Verwahrung zuständigen Stellen (in der Regel den Notaren) nur die Infrastruktur für eine elektronische Verwahrung zur Verfügung, ohne dadurch selbst Verwahrstelle zu werden.[263] Zugangsberechtigt zum Urkundenarchiv ist gemäß § 78i BNOTO ausschließlich die für die Verwahrung zuständige Stelle, die die verwahrte Urkunde errichtet hat bzw. deren Amtsnachfolger. Seit dem 1.1.2022 sind ferner die § 55 BeurkG (Verzeichnis und Verwahrung der Urkunden), § 56 BeurkG (Übertragung der Papierdokumente in die elektronische Form; Einstellung der elektronischen Dokumente in die elektronische Urkundensammlung), § 59a BeurKG (Verwahrungsverzeichnis) sowie die auf der Basis von § 59 BeurKG erlassene Rechtsverordnung zu beachten. Seit dem 1.1.2022 ist ferner die im elektronischen Urkundenarchiv zu verwahrende elektronische Fassung mit der Papierurschrift gleichgestellt (§ 45 Abs. 2 BeurkG, § 56 Abs. 3 BeurkG).[264] Dazu muss der Notar gemäß § 56 Abs. 1 BeurkG mithilfe eines qualifizierten Medientransfer die inhaltliche und bildliche Übereinstimmung des elektronischen Dokuments mit der Papierurschrift sicherstellen und durch einen Vermerk bestätigen.

209 **i) Schuldnerverzeichnis.** In das Schuldnerverzeichnis, das vom Vollstreckungsgericht geführt wird, werden die Personen eingetragen, die eine eidesstattliche Versicherung nach §§ 807, 899 ff. ZPO oder nach § 284 Abgabenordnung abgegeben haben. Das Schuldnerverzeichnis enthält nach § 882b Abs. 2 und 3 ZPO die persönlichen Daten des Schuldners, das Datum der Eintragung und den Grund, weshalb die Eintragung erfolgt ist. In dem Gemeinsamen Vollstreckungsportal der Länder werden die bundesweiten Daten aus den

[257] https://schutzschriftenregister.hessen.de/, abgerufen am 29.2.2024.
[258] Abgerufen am 29.2.2024.
[259] Anders/Gehle ZPO, 82. Auflage 2024, § 945a Rn. 6.
[260] BGBl. I 2015, 2135.
[261] Das Inkrafttretensdatum ergibt sich aus Art. 26 Abs. 6 des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten. Zur Verortung kritisch: Wehlau/Kalbfus ZRP 2013, 101, 102; Weller DRiZ 2013, 290, 294 f.
[262] Durch das Gesetz zur Neuordnung der Aufbewahrung von Notariatsunterlagen und zur Einrichtung des Elektronischen Urkundenarchivs bei der Bundesnotarkammer sowie zur Änderung weiterer Gesetze vom 1.6.2017 (BGBl. 2017 I S. 1396) neu eingefügt.
[263] BeckOK BNotO/Sander, 9. Ed. 1.2.2024, BNotO § 20 Rn. 224.
[264] Einzelheiten bei BeckOK BNotO/Sander, 9. Ed 1.2.2024, BNotO § 20 Rn. 225 ff.

Schuldnerverzeichnissen nach §§ 882b ff. ZPO zum kostenpflichtigen Abruf bereitgestellt.[265] Der Einsichtnehmende erteilt gemäß § 6 Schuldnerverzeichnisführungsverordnung (SchuFV) mit der Nutzung der im Verzeichnis aufgeführten Daten das Einverständnis zur Speicherung seiner Daten. Jeder eingetragene Schuldner kann die für sechs Monate zu seiner Eintragung gespeicherten Protokolldaten einsehen.

210 j) **Rechtsdienstleistungsregister.** Das Rechtsdienstleistungsregister gemäß § 16 RDG ist ein öffentliches, elektronisch geführtes Register, in dem Personen registriert werden, denen Inkassodienstleistungen, Rentenberatung oder Rechtsdienstleistungen nach ausländischem Recht erlaubt. Ferner sind ersichtlich die Personen oder Vereinigungen, denen die Erbringung von Rechtsdienstleistungen nach § 9 Abs. 1 bestandskräftig untersagt worden ist.

211 k) **Bundeszentralregister.** Unter der Aufsicht des Bundesamts für Justiz wird gemäß § 1 Bundeszentralregistergesetz (BZRG) das Bundeszentralregister (seit 1975 ausschließlich) als elektronisches Register geführt. In das Register werden gemäß § 3 BZRG strafgerichtliche Verurteilungen mit den Personendaten des Verurteilten, bestimmte Entscheidungen von Verwaltungsbehörden und anderen Gerichten, Vermerke über die Schuldunfähigkeit, gerichtliche Feststellungen zur Betäubungsmittelabhängigkeit und zum Verbot der Ausübung eines Gewerbes, nachträgliche Entscheidungen wie Straferlass, Strafaussetzung, Führungsaufsicht, Bewährungshilfe, die vorzeitige Aufhebung einer Sperre der Fahrerlaubnis, der Tag des Ablaufs des Verlustes der Wählbarkeit, Amtsfähigkeit oder des Wahl- und Stimmrechts, nachträgliche Entscheidungen der Beseitigung des Strafmakels, der Abkürzung oder Verlängerung der Bewährungszeit. Bei Vorliegen der entsprechenden Voraussetzungen werden außerdem ausländische strafrechtliche Verurteilungen gegen Deutsche, in Deutschland geborene oder wohnhafte Personen in das Register eingetragen. Auskünfte über Eintragungen können beantragt werden im Rahmen von Führungszeugnissen (§§ 30 ff. BZRG), unbeschränkten Auskünften aus dem Zentralregister (§ 41 BZRG). Ferner kann gemäß § 42 BZRG Auskunft an die betroffene Person erteilt werden. Unbeschränkt sind auch anonymisierte Auskünfte für wissenschaftliche Forschungsvorhaben möglich. Verurteilungen werden dann nicht mehr in Führungszeugnisse aufgenommen (§§ 33 ff. BZRG), wenn die im BZRG definierte Frist abgelaufen ist. Allerdings können bestimmten in § 41 BZRG genannten Institutionen weiterhin solche Verurteilungen mitgeteilt werden. Nach Ablauf einer weiteren Frist, die sich nach Art der Verurteilung bzw. nach der Strafhöhe richtet (§§ 45 ff. BZRG) wird die Verurteilung im Register getilgt.

212 l) **Zentrales Staatsanwaltschaftliches Verfahrensregister (ZStV).** Auf der Basis von § 492 StPO wurde das elektronische Register 1999 eingerichtet und steht seit 1.1.2007 unter der Aufsicht des Bundesamts für Justiz. In das Register werden eingetragen: die Personendaten von Beschuldigten sowie andere zur Identifizierung geeignete Merkmale, die zuständige Stelle und das Aktenzeichen, die nähere Bezeichnung der Straftaten, insbesondere die Tatzeiten, die Tatorte und die Höhe etwaiger Schäden, die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften, die Einleitung des Verfahrens sowie die Verfahrenserledigungen bei der Staatsanwaltschaft und bei Gericht nebst Angabe der gesetzlichen Vorschriften. Einzelheiten ergeben sich aus der Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters (ZStVBetrV). Die Eintragungen werden den Ermittlungsbehörden automatisch oder auf Anfrage mitgeteilt. Auf diese Weise soll den Strafermittlungsbehörden eine Koordinierung der Strafverfolgungsmaßnahmen ermöglicht, insbesondere erforderliche Informationen über denselben Beschuldigten in verschiedenen Ermittlungsverfahren zur Verfügung gestellt werden, somit Mehrfachtäter ermittelt und Doppelverfahren vermieden werden.

13. Open Justice

213 Der vornehmlich im Common Law verankerte Open Justice-Grundsatz[266] beinhaltet ua, dass gerichtliche Verfahren – einschließlich der Inhalte der gerichtlichen Dokumente – offen

[265] https://www.vollstreckungsportal.de/zponf/allg/willkommen.jsf, abgerufen am 29.2.2024.
[266] Siehe dazu Bernhardt NJW 2015, 2779.

für die Öffentlichkeit sein sollten. Das BVerfG hat den Grundsatz der öffentlichen Verhandlung – auch unter Hinweis auf Art. 6 Abs. 1 EMRK – hervorgehoben und die beiden Zielsetzungen betont: die Verfahrensgarantie zum Schutze der an der Verhandlung Beteiligten sowie die Möglichkeit des Volkes, von den Geschehnissen im Verlauf einer Gerichtsverhandlung Kenntnis zu nehmen und die durch die Gerichte handelnde Staatsgewalt einer Kontrolle in Gestalt des Einblicks der Öffentlichkeit zu unterziehen. § 169 GVG hat den Open-Justice-Grundsatz für das gerichtliche Verfahren konkretisiert. Zwar wird der Grundsatz festgelegt, dass die Verhandlung vor dem erkennenden Gericht einschließlich der Verkündung der Urteile und Beschlüsse öffentlich ist. Allerdings sind Ton- und Fernseh-Rundfunkaufnahmen sowie Ton- und Filmaufnahmen zum Zwecke der öffentlichen Vorführung oder Veröffentlichung ihres Inhalts unzulässig. Hiervon gibt es allerdings Ausnahmen: Es kann eine Tonübertragung in einen Arbeitsraum für Personen, die für Presse, Hörfunk, Fernsehen oder für andere Medien berichten, von dem Gericht zugelassen werden, wobei wiederum eine Tonübertragung zur Wahrung schutzwürdiger Interessen der Beteiligten oder Dritter oder zur Wahrung eines ordnungsgemäßen Ablaufs des Verfahrens teilweise untersagt werden kann. Bei Verfahren „von herausragender zeitgeschichtlicher Bedeutung für die Bundesrepublik Deutschland" können Tonaufnahmen der Verhandlung einschließlich der Verkündung der Urteile und Beschlüsse zu wissenschaftlichen und historischen Zwecken von dem Gericht zugelassen werden. Aber auch das kann zur Wahrung schutzwürdiger Interessen der Beteiligten oder Dritter oder zur Wahrung eines ordnungsgemäßen Ablaufs des Verfahrens untersagt werden. Schließlich können Ton- und Fernseh-Rundfunkaufnahmen von der Verkündung von Entscheidungen des Bundesgerichtshofs ausnahmsweise zugelassen werden.

214 Das Prinzip Open Justice und das Recht auf informationelle Selbstbestimmung müssen im digitalen Zeitalter einem neuen Ausgleich zugeführt werden: Die aus der Öffentlichkeitsmaxime abzuleitende Information über Zeit und Ort der Verhandlung, die in der Vergangenheit regelmäßig durch Aushang im Gericht praktiziert wurde, gehört im digitalen Zeitalter ins Internet – ebenso wie alle anderen bisherigen Papierbekanntmachungen. Die entsprechenden Instrumentarien sind bereitzustellen. In den Zeiten der digitalen Transformationen dürften die derzeitigen Möglichkeiten der Öffentlichkeitsbeteiligung, die noch auf das Prinzip der Saalöffentlichkeit bezogen sind, nicht mehr ausreichend sein.

215 Dies gilt insbesondere dann, wenn –wie von der Bundesregierung geplant und nun im Gesetzesbeschluss des Deutschen Bundestages vorgesehen- der Einsatz der Videokonferenzsysteme ausgeweitet wird. So sieht das vom Deutschen Bundestag am 17.11.2023 beschlossene Gesetz zur Förderung des Einsatzes von Videokonferenztechnik in der Zivilgerichtsbarkeit und den Fachgerichtsbarkeiten[267] gemäß 128 Abs. 2 ZPO – neu – vor, dass der Vorsitzende die Teilnahme an der mündlichen Verhandlung per Bild- und Tonübertragung für einen Verfahrensbeteiligten, mehrere oder alle Verfahrensbeteiligte gestatten oder anordnen kann. Beantragt ein Verfahrensbeteiligter die Teilnahme per Bild- und Tonübertragung, soll der Vorsitzende diese anordnen, wobei die Ablehnung eines Antrags auf Teilnahme per Bild- und Tonübertragung unter Berücksichtigung der Umstände des Einzelfalls zu begründen ist. Gegen eine Anordnung der Videokonferenz kann der Adressat Einspruch einlegen. „Wird der Einspruch fristgerecht eingelegt, so hebt der Vorsitzende die Anordnung für alle Verfahrensbeteiligten auf. In diesem Fall soll der Vorsitzende den Verfahrensbeteiligten, die keinen Einspruch eingelegt haben, die Teilnahme per Bild- und Tonübertragung gestatten. Im Übrigen sind Entscheidungen nach dieser Vorschrift unanfechtbar."

216 Der ferner neu vorgesehene§ 128a Abs. 3 S. 2 ZPO sieht auch die Möglichkeit der virtuellen Teilnahme von Mitgliedern des Gerichts vor, wobei der Vorsitzende die Videoverhandlung von der Gerichtsstelle aus leitet. Allerdings kann gemäß § 128a Abs. 6 ZPO der Vorsitzende die Videoverhandlung auch von einem anderen Ort als der Gerichtsstelle aus leiten,

[267] BR-Drs. 604/23. Allerdings hat hierzu der Bundesrat den Vermittlungsausschuss angerufen, weil er insbesondere Gefahren für die Wahrheitsfindung und Beeinträchtigung des Opferschutzes, aber auch Verfahrensverzögerungen und einen zum Verhältnis von personellem, technischen, organisatorischen und finanziellen Aufwand nicht ausreichenden Mehrwert befürchtet, BR-Drs. 604/23 (Beschluss).

wenn alle Verfahrensbeteiligten und alle Mitglieder des Gerichts an der mündlichen Verhandlung per Bild- und Tonübertragung teilnehmen. Für die beobachtende Öffentlichkeit ist die Übertragung in einen anderen Saal im Gerichtsgebäude zur Beteiligung der Öffentlichkeit vorgesehen. Es erscheint aber wenig zeitgemäß, allein die Öffentlichkeit noch bei einem ansonsten vollvirtuellen Verfahren zum Gang in das Gerichtsgebäude zu veranlassen. § 16 des Gesetzes betreffend die Einführung der Zivilprozessordnung soll daher gemäß Gesetzesbeschluss des Deutschen Bundestages so geändert werden, dass Bundesregierung und die Landesregierungen per Rechtsverordnung ohne Zustimmung des Bundesrates für ihre jeweiligen Zuständigkeitsbereiche zum Zwecke der Erprobung zulassen können, dass die Gerichte zur Herstellung der Öffentlichkeit bei Videoverhandlungen gemäß § 128a Abs. 6 S. 1 der Zivilprozessordnung auch „die unmittelbare Teilnahme der Öffentlichkeit an der Videoverhandlung ermöglichen". Dabei kann die Zulassung der Erprobung auf einzelne Gerichte oder Verfahren beschränkt werden. Der Gesetzesbeschluss sieht vor, die Geltungsdauer einer solchen Rechtsverordnung längstens bis zum Ablauf des 31.12.2033 zu befristen. Zu der ermöglichten Erprobung sind auch Evaluierungen gesetzlich vorgesehen. Ferner ist vier und acht Jahre nach dem Inkrafttreten eine Evaluierung der Erkenntnisse aus der Erprobung vorgesehen.

Seit den 1990er Jahren gab es viele Fortschritte bei dem Bemühen, Justiz mit den Mitteln **217** der Informationstechnologie transparenter zu gestalten. Getreu dem Motto des Eröffnungsvortrags von Berkemann auf dem 8. EDV-Gerichtstag 1999[268] gab es verschiedene Aktivitäten, Gesetze und Rechtsprechung – wenn auch teilweise in eingeschränkt recherchierbarer Form – kostenlos für die Allgemeinheit verfügbar zu machen. Gesetze und Rechtsverordnungen können in ihrer geltenden, also durch die Dokumentationsstelle im Bundesamt für Justiz fortlaufend konsolidierten Fassung abgerufen werden. Die Entscheidungen des BVerfG und der obersten Gerichtshöfe des Bundes und viele Entscheidungen der Gerichte der Länder können kostenlos eingesehen werden.[269]

Gerichtsentscheidungen gelten gem. Art. 4 Nr. 1 DSDVO als personenbezogene Daten, die **218** Veröffentlichung bedarf daher einer Rechtsgrundlage. Eine Rechtfertigung nach Artikel 6 DSGVO für die Veröffentlichung von Gerichtsentscheidungen ergibt sich ua aus dem presserechtlichen Auskunftsanspruch von Medienvertretern. Der „Ampel-Koalitionsvertrag" für die Jahre 2021–2025 sieht darüberhinausgehend vor, Gerichtsentscheidungen grundsätzlich in anonymisierter Form in einer Datenbank öffentlich und maschinenlesbar verfügbar zu machen.[270] Dies umfasst offenbar auch die Veröffentlichung der Entscheidungen erstinstanzlicher Gerichte. Mit dieser Frage hat sich auch die Arbeitsgruppe zur Modernisierung des Zivilprozesses[271] befasst und angeregt, zunächst bundesrechtlich vorzuschreiben, gerichtliche Entscheidungen mit grundsätzlicher Bedeutung (nach klaren Kriterien) zu veröffentlichen. Wenn dagegen eine (mithilfe von KI) zuverlässige Anonymisierung von Gerichtsentscheidungen möglich ist, könnten alle Gerichtsentscheidungen unmittelbar aus der E-Akte heraus bereitgestellt werden.

Entsprechend dem Open-Justice-Prinzip sind die Möglichkeiten der Justiznutzer und **219** Rechtsinteressierten, in komfortabler Weise alle wichtigen Informationen im Internet aufzurufen, zu verbessern. Zwar verfügt das Justizportal des Bundes und der Länder mittlerweile über ein reichhaltiges Informationsangebot, etwa ein Orts- und Gerichtsverzeichnis, Bekanntmachungen, Online-Dienste, Abrufbarkeit von Formularen, Rechtstexten und Ge-

[268] JurPC Web-Dok. 188/1999, Abs. 1 – 79; https://www.jurpc.de/jurpc/show?id=19990188.

[269] https://www.bundesverfassungsgericht.de/SiteGlobals/Forms/Suche/Entscheidungensuche_Formular.html?language_=de; abgerufen am 29.2.2024; https://www.bundesgerichtshof.de/DE/Entscheidungen/entscheidungen_node.html;jsessionid=E151326F4E083861558EC96A6F19EC7D.2_cid368; https://www.bverwg.de/suche?lim=10&start=1&db=e&q=*&dt=; https://www.bundesarbeitsgericht.de/entscheidungen/; abgerufen am 29.2.2024; https://www.bundesfinanzhof.de/de/entscheidungen/entscheidungen-online/; abgerufen am 29.2.2024. https://www.bsg.bund.de/DE/Entscheidungen/Entscheidungen-ab-2018/entscheidungen-ab-2018_node.html, abgerufen am 29.2.2024.

[270] https://fragdenstaat.de/dokumente/142083-koalitionsvertrag-2021–2025/, Rn. 3562.

[271] S. 70, downloadbar unter https://www.justiz.bayern.de/gerichte-und-behoerden/oberlandesgerichte/nuernberg/aktuelles.php, abgerufen am 29.2.2024.

richtsentscheidungen bis hin zu Verlinkungen mit E-Justice-Angeboten auf der EU-Ebene. Nicht ausreichend ist demgegenüber das bisherige Angebot, sich etwa schnell und komfortabel über Rechtsfragen im Zusammenhang mit den geltenden Pandemieregeln oder Gerichtsentscheidungen zu den Freiheitseinschränkungen aufgrund der Pandemie informieren können oder Informationen zu den rechtspolitischen Planungen auf Bundes- und Landesebene aufzurufen oder aktuelle Diskussionen und Beschlüsse des E-Justice-Rats und der Bund-Länder-Kommission für Informationstechnik in der Justiz detaillierter nachzuvollziehen.

220 Auch auf europäischer Ebene ist das Open-Justice-Prinzip aus der Festlegung der Werte des Art. 2 Abs. 2 EUV abzuleiten (Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte einschließlich der Rechte der Personen, die Minderheiten angehören). Ferner sieht Art. 1 Abs. 2 EUV vor, dass „dieser Vertrag eine neue Stufe bei der Verwirklichung einer immer engeren Union der Völker Europas darstellt, in der die Entscheidungen möglichst offen und möglichst bürgernah getroffen werden". Art. 15 AEUV konkretisiert das Prinzip der Offenheit. Dies betrifft auch den EuGH, denn die Veröffentlichung ist ein Akt der Gerichtsverwaltung, die gem. Abs. 4 den Pflichten des Art. 15 unterfällt. Ferner hebt der EuGH[272] den Grundsatz der Offenheit hervor und verweist insoweit auch auf Art. 10 Abs. 3 S. 2 EUV („Die Entscheidungen werden so offen und bürgernah wie möglich getroffen) und die Verbürgung des Rechts auf Zugang zu Dokumenten in Art. 42 der EU-Grundrechtecharta. Schließlich sieht auch die vom Rat der EU beschlossene Europäische Strategie für die E-Justiz und den Aktionsplan 2024–2028[273] als ein Ziel die Förderung der Zugänglichmachung von Justizdaten („datenorientierte Justiz") vor – unter Beachtung der Datenschutzvorschiften – die Transparenz; sie ermögliche die Entstehung neuer Geschäftsmodelle; auch die Entwicklung von KI- Systemen hänge von der Verfügbarkeit umfangreicher, strukturierter und maschinenlesbarer Datensätze ab. Das Risiko einer unbeabsichtigten Diskriminierung sei zu vermeiden. Sie erleichtere die Interoperabilität, trage zu einer fundierteren Entscheidungsfindung und zu besserer Priorisierung bei.

14. Europäisches E-Justice

221 **a) Allgemein und europäische Grundlagen.** Bereits 2007 wurden während der deutschen EU-Ratspräsidentschaft erste wichtige Weichenstellungen auf europäischer Ebene für eine stärker europäisch ausgerichtete Digitalisierung der Justiz gestellt. So wurde nicht nur eine eigene Ratsarbeitsgruppe E-Justice begründet, sondern auch das europäische Justizportal initiiert, das zum Fundament für eine europäische Zusammenarbeit bei der digitalen Justiz wurde.[274] Auch zukünftig geht es vor allem darum, das Europäische Justizportal weiterzuentwickeln des mehrjährigen Aktionsplans *2024–2028*[275] umzusetzen. Das gilt auch für die fortentwickelte Nutzung der Ergebnisse von e-CODEX (e-Justice Communication via Online Data Exchange) für die Justizkommunikation und den Dokumentenaustausch, die Verknüpfung der Justizregister, den Einsatz für strafprozessuale Zwecke, etwa die Umsetzung der Vorgaben für die Europäische Ermittlungsanordnung sowie bei der elektronischen Übermittlung von elektronischen Beweismitteln entsprechend der E-Evidence-VO.[276]

222 **b) E-Justiz-Portal.** Das Europäische Justizportal[277] wurde während von der deutschen EU-Ratspräsidentschaft 2007 initiiert und dessen Aufbau auf den Weg gebracht. Nach mehre-

[272] EuGH 22.1.2020 – C-178/18 P.

[273] https://data.consilium.europa.eu/doc/document/ST-15509-2023-INIT/de/pdf., abgerufen am 29.2.2024.

[274] Bernhardt, JurPC Web-Dok. 75/2007, Abs. 1–43, https://e-justice.europa.eu/home.do?plang=de&action=home., abgerufen am 16.4.2022.

[275] Ratsdokument vom 17.11.2023, 15509/23, S. 22 ff.

[276] Siehe dazu Bernhardt, in: Chibanguza/Kuß/Steege (Hrsg)., Künstliche Intelligenz, Recht und Praxis automatisierter und autonomer Systeme, 2021, S. 1089 ff.

[277] https://e-justice.europa.eu/home?plang=de&action=home, abgerufen am 29.2.2024. Siehe zu den Inhalten Bernhardt, in : Chibanguza/Kuß/Steege (Hrsg)., Künstliche Intelligenz, Recht und Praxis automatisierter und autonomer Systeme, 2021, S. 1076.

ren Ausbaustufen zielt das in allen 24 Amtssprachen verfügbare Portal im Schwerpunkt darauf ab, den (kostenlosen) Zugang zum Unionsrecht und zum nationalen Recht der EU zu ermöglichen sowie nationale Register miteinander zu vernetzen. Zum einen können Werkzeuge für grenzüberschreitende Recherchen genutzt (zB Tools für die Suche nach Angehörigen der Rechtsberufe in EU-Ländern -etwa Rechtsanwälte und Notare-) und Auskünfte erlangt werden etwa über die Prozesskostenhilfe, die Mediation, Rechte der Beschuldigten in Strafverfahren in den EU-Mitgliedstaaten oder rechtliche Informationen über familienrechtliche Angelegenheiten mit grenzüberschreitenden Aspekten in der EU. Aktuell und hilfreich war zuletzt der Überblick über Maßnahmen, die in der Europäischen Union in Bezug auf die COVID-19-Pandemie ergriffen wurden und die sich auf die Justiz, nationale Behörden und Angehörige der Rechtsberufe, aber auch Unternehmen und Bürger auswirken. Angehörige der Rechtsberufe erlangen Zugang zu allgemeinen Informationen über die justizielle Aus- und Fortbildung zum EU-Recht sowie über das Schulungsmaterial. Das Portal bietet einen Zugang zu diversen nationalen Justizregistern (Handels- und Unternehmensregister, Grundbücher, Insolvenzregister) und den Zugang zu gerichtlichen und außergerichtlichen Verfahren bei grenzüberschreitenden Sachverhalten. Die Entwicklung von effizienten Mitteln (semantisches Web) soll schließlich für einen erleichterten Zugang zu europäischer und nationaler Rechtsprechung sorgen. In diesem Zusammenhang ist insbesondere auf den **European Case Law Identifier (ECLI)**[278] hinzuweisen, der seit 4.5.2016 verfügbar ist und mittlerweile von einigen Mitgliedstaaten (in Deutschland beim BVerfG, BGH, BVerwG, BFH, BAG, BSG und einigen Gerichten der Länder), dem EuGH, dem EGMR und der Beschwerdekammer des Europäischen Parlaments angewandt wird. ECLI soll die korrekte und eindeutige Angabe von Fundstellen in den Gerichtsentscheidungen und damit auch eine grenzüberschreitende Suche nach bestimmten, möglicherweise einschlägigen Entscheidungen aufgrund eines Bestands von einheitlichen Metadaten über eine Suchschnittstelle erleichtern. Während vormals Rechtssachen in verschiedenen nationalen und grenzüberschreitenden Urteilsdatenbanken nach unterschiedlichen Regeln und unterschiedlichen Identifikatoren registriert wurden, können seither aufgrund eines Bestands von einheitlichen Metadaten über eine Suchschnittstelle mit dem festgelegten Identifikator thematisch passende Entscheidungen in den nationalen Datenbanken leichter aufgefunden werden. Für ein besseres Verständnis der unterschiedlichen Rechtssysteme der EU soll der **European Legislation Identifier (RLI)** und das **Projekt Legivoc** mit einem interoperablen Rechtsvokabular sorgen.

223 **c) Europäische Strafregistervernetzung.** Aufbauend auf einer ursprünglich von Deutschland und Frankreich pilotierten Vernetzung ihrer beiden Strafregister (seit 2004) und einer schrittweisen Ausdehnung auf andere EU-Mitgliedstaaten (zum NJR – Network of Judicial Registers) ist seit April 2012 das computergestützte Europäische Strafregisterinformationssystem (ECRIS – European Criminal Records Information System) im Echtbetrieb. Durch die Vernetzung der Strafregisterdatenbanken aller EU-Mitgliedstaaten können somit die Informationen über Strafurteile in einem elektronisch leicht übermittelbaren Standardformat ausgetauscht werden. ECRIS erlaubt es Richtern, Staatsanwälten und sonstigen zuständigen Behörden, in einfacher Weise auf das Vorstrafenregister eines jeden Unionsbürgers zuzugreifen, wobei unerheblich ist, in welchen EU-Ländern die betreffende Person bisher schon verurteilt worden ist.

224 Ferner wurde mit der Verordnung (EU) 2019/816 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Nicht-EU-Staatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, ein System mit dem Namen „Europäisches Strafregisterinformationssystem für Drittstaatsangehörige" („ECRIS-TCN") zur Ermittlung der Mitgliedstaaten eingerichtet, in denen Informationen zu früheren Verurteilungen von „Drittstaatsangehörigen" (dh Nicht-EU-Staatsangehörigen) vorliegen. Die nationalen Behörden, die Europäische Staatsanwaltschaft, Eurojust und Europol dürfen das System unter jeweils festgelegten Bedingungen verwenden. Durch weitere

[278] https://e-justice.europa.eu/content_european_case_law_identifier_ecli-175-de.do (abgerufen am 29.2. 2024). Dort sind auch die Staaten vermerkt, die am ECLI-System teilnehmen.

Änderungen der Verordnung[279] wurden ein Interoperabilitätsrahmen für die polizeiliche und justizielle Zusammenarbeit sowie weitere Zugangsmöglichkeiten zum System festgelegt.

225 **d) Europäisches Mahnverfahren.** Seit dem 12.12.2008 ist auf der Grundlage der EU-Verordnung (EG) Nr. 1896/2006 zur Einführung eines Europäischen Mahnverfahrens Gläubigern in den EU-Mitgliedsstaaten (mit Ausnahme von Dänemark)[280] die Möglichkeit eröffnet, unbestrittene Forderungen in Zivil- und Handelssachen nach einem einheitlichen Verfahren auf der Grundlage von Formblättern und ohne eine persönliche Anwesenheit der Antragssteller und ohne mündliche Verhandlung grenzüberschreitend gerichtlich geltend zu machen. Europäische Zahlungsbefehle werden – außer in Ungarn (dort fällt das Mahnverfahren in die Zuständigkeit der Notare) – von Gerichten ausgestellt. Zusammen mit der österreichischen Justizverwaltung wurde vom Amtsgericht Wedding, das auch als zentrales deutsches EU-Mahngericht fungiert, ein elektronisches Verfahren pilotiert, das mittlerweile auf viele EU-Mitgliedstaaten ausgedehnt wurde. Im Unterschied zum innerdeutschen Mahnverfahren erteilt das Gericht beim europäischen Mahnverfahren einen sofortigen Zahlungsbefehl, der dem Antragsgegner zugestellt und ohne weiteren Antrag für vollstreckbar erklärt werden kann, §§ 1093 ff. ZPO. Wie im deutschen Mahnverfahren prüft das Mahngericht die Angaben lediglich auf Vollständigkeit, jedoch nicht auf Richtigkeit, was eine Digitalisierung des Verfahrens erleichtert.

226 Für den Europäischen Zahlungsbefehl stehen elektronische Formblätter in allen EU-Sprachen zur Verfügung, die elektronisch über das Europäische Justizportal abgerufen und ausgefüllt werden können. Die dabei in die Felder einzusetzenden Angaben zu den Parteien und zur Art und Höhe der Forderungen könnten mithilfe von Codes (die im Formblatt erläutert werden) „automatisch" in die Sprache des zuständigen Gerichts übersetzt werden. Sodann kann das ausgefüllte Formblatt entweder ausgedruckt und als Papierexemplar an das zu-ständige Mahngericht des anderen EU-Mitgliedstaats versandt oder auf elektronischem Weg eingereicht werden. Für eine elektronische Einreichung ist es gemäß Artikel 2 Nr. 2 der Richtlinie 1999/93/EG in einer Form zu unterzeichnen, die im Mitgliedstaat, in dem der Europäische Zahlungsbefehl erlassen wird, anerkannt wird. Sofern im Ursprungsmitgliedstaat alternative, sichere elektronische Kommunikationssysteme den autorisierten Nutzern zur Verfügung stehen und die Europäische Kommission über diese Systeme unterrichtet wurde, dann muss keine qualifizierte elektronische Signatur angebracht werden. Dies gilt etwa in Deutschland für die Übersendung über das beA. Im Rahmen des E-CODEX-Systems sind seit dem 25.7.2013 elektronische Übermittlungen von Anträgen im EU-Mahnverfahren zwischen einzelnen EU-Mitgliedstaaten möglich. Welche Form der Übersendung in Betracht kommt, ergibt sich aus den entsprechenden Informationen über das E-Justice-Portal.[281] Das Gericht prüft den Antrag und erlässt innerhalb von 30 Tagen den Europäischen Zahlungsbefehl, wenn das Formblatt korrekt ausgefüllt ist. Der Europäische Zahlungsbefehl muss dem Antragsgegner dann vom Gericht zugestellt werden. Der Antragsgegner kann dann den Forderungsbetrag entrichten oder aber innerhalb von 30 Tagen Einspruch gegen den Europäischen Zahlungsbefehl einlegen. Bei einem Einspruch kann das Mahnverfahren in ein „normales" Verfahren gemäß den Regeln eines ordentlichen Zivilprozesses überführt werden.

227 Eine rein digitale – automatische – Abwicklung des EU-Mahnverfahrens mit durchgängig elektronischer Beantragung, automatischer gerichtlicher Überprüfung der Antragsvoraussetzungen sowie elektronischen gerichtlichen Verfügungen und Entscheidungen sowie elektronischer Übermittlung an die Verfahrensbeteiligten wäre zwar wegen der streng formalisier-

[279] Verordnung (EU) 2019/818, mit der ein Rahmen für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) errichtet wird; Verordnung (EU) 2021/1133, in der die Voraussetzungen für den Zugang zu den in ECRIS-TCN gespeicherten Daten für Zwecke des Visa-Informationssystems, das mit der Verordnung (EG) Nr. 767/2008 eingerichtet wurde; Verordnung (EU) 2021/1151, in der die Bedingungen für den Zugang zu den in ECRIS-TCN gespeicherten Daten für Zwecke des Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) festgelegt wurden.

[280] Verordnung vom 12.12.2006 zur Einführung eines Europäischen Mahnverfahrens, ABl. L 399 vom 30.12.2006, S. 1.

[281] https://e-justice.europa.eu/dynform_intro_member_state_action.do, abgerufen am 29.2.2024.

ten Verfahren in den EU-Mitgliedstaaten vorstellbar, ist aber noch nicht realisiert. Auch im EU-Mahnverfahren ist dabei – ähnlich wie im nationalen Mahnverfahren – zu prüfen, ob eine Rechtsnorm für automatische Gerichtsentscheidungen ohne Prüfung durch einen Richter geschaffen werden kann. Art. 22 ESGVO dürfte hierbei kein Hindernis sein, da das Mahnverfahren ohne besondere Herausforderungen in ein normales streitiges Zivilstreitverfahren vor „menschlichen" Richtern überführt werden kann.

e) Europäisches Small Claims Verfahren. Wenn der Antragssteller es im Formblatt für den Europäischen Zahlungsbefehl vermerkt hat, wird das Verfahren nach Maßgabe eines Europäischen Verfahrens für geringfügige Forderungen weitergeführt (sofern die dafür erforderlichen Voraussetzungen erfüllt sind, insbesondere die Forderungssumme 5.000 EUR nicht übersteigt). 228

Das Small-Claims-Verfahren kommt aber auch als Alternative für den Europäischen Zahlungsbefehl in Betracht. Auf der Grundlage der Verordnung (EG) Nr. 861/2007 vom 11.7.2007[282] kann ein Verfahren für geringfügige Forderungen in Zivil- und Handelssachen stattfinden, deren Streitwert unter 5000 EUR liegt. Das auf Formularen basierende Verfahren findet in allen Mitgliedstaaten der Europäischen Union – mit Ausnahme von Dänemark –Anwendung. Wenn das Gericht keine Anhörung für erforderlich hält, findet das Verfahren schriftlich unter vom Gericht festgelegten Fristen statt. Gemäß Art.l 4 Abs. 1 der Verordnung können die Formulare Forderung auf dem Postweg übersendet oder auf anderem Wege übermittelt werden, der in dem Mitgliedstaat, in dem das Verfahren eingeleitet wird, zulässig ist, beispielsweise per Fax oder elektronisch. Entsprechende Informationen zur jeweiligen Zulässigkeit des Übermittlungsverfahrens sind über das Europäische Justizportal abrufbar.[283] 229

f) E-CODEX (e-Justice Communication via Online Data Exchange). Im Rahmen des von der Europäischen Kommission kofinanzierten Projekts „e-CODEX" wurden von 2010 bis 2016 unter der Leitung des Justizministeriums Nordrhein-Westfalen technische Lösungen für den sicheren Austausch justizieller Daten entwickelt. Das Projekt sollte den europäischen Bürgerinnen und Bürgern sowie den Unternehmen einen verbesserten grenzüberschreitenden elektronischen Zugang zum Recht ermöglichen und die elektronische Zusammenarbeit von Justizeinrichtungen innerhalb von Europa zu fördern, ohne dem Subsidiaritätsprinzip zuwiderzuhandeln. Dementsprechend wurde E-CODEX ohne einen zentralen Hub bzw. eine zentrale Datenspeicherung entwickelt. Bei E-CODEX handelt es sich daher um eine Kollaborationslösung mit Softwareelementen, einer einheitlichen Semantik und gemeinsamen Standards für den Austausch von Dokumenten und Daten, ohne dass die nationalen Lösungen dadurch ersetzt werden. Die Nutzer identifizieren und authentifizieren sich über ihre nationalen Systeme. E-Codex funktioniert mit sogenannten Konnektoren, die jeweils auf nationaler Ebene die Verbindung des Nutzers und dessen Nachricht über Gateways zu den Konnektoren der anderen Mitgliedstaaten sicherstellen. Sendet das System des Nutzers die Nachricht an den nationalen Konnektor, so wird das mitgeschickte XML-Dokument vom nationalen Format in das EU-Format umgewandelt und die Signatur auf dem PDF-Dokument validiert. Sodann wird ein Trust-OK-Token (PDF und XML) erstellt, um dem Empfänger im anderen Land eine Prüfung zu ermöglichen, ob die Signatur des PDF-Dokuments zum Zeitpunkt des Versands gültig war. Der Konnektor übermittelt die Nachricht an das Gateway verschlüsselt (SSL) an das Partnergateway des anderen Mitgliedstaates, das dann die Signatur der Nachricht prüft, die Anhänge entschlüsselt und die Nachricht an den Konnektor des Partnerlands weiterleitet. Die Empfangsbestätigungen werden auf demselben Weg zurückgeschickt. 230

[282] Verordnung (EG) Nr. 861/2007 des Europäischen Parlaments und des Rates vom 11.7.2007 zur Einführung eines europäischen Verfahrens für geringfügige Forderungen, ABl L 199 vom 31.7.2007, S. 1–22.

[283] https://e-justice.europa.eu/dynform_intro_form_action.do?idTaxonomy=177&formSelectiondynform_sc_a_2_action, abgerufen am 29.2.2024.

231 Mittlerweile gibt es EU-kofinanzierte Nachfolgeprojekte Me-CODEX („Maintenance of e-CODEX") und Me-CODEX II,[284] mit denen die e-CODEX-Lösungen weiter ausgebaut und neue Anwendungen ermöglicht werden. Bisher wurde der Betrieb von e-CODEX von den Mitgliedstaaten sichergestellt.

232 Auf der Grundlage der **e-CODEX-Verordnung**[285] soll nun das Instrumentarium dauerhaft für den elektronischen Rechtsverkehr genutzt und durch die Agentur eu-LISA betrieben und fortentwickelt werden. Eu-LISA ist die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, die – neben der Verantwortung für den Betrieb von ECRIS-TCN – bisher vor allem für europäische IT-Systeme der Inneren Sicherheit zuständig ist.

233 **Die e-CODEX-Verordnung (EU) 2022/850 vom 30.5.2022** regelt auf der Grundlage von Art. 81 und Art. 82 AEUV die Funktionsweisen, die Entwicklung von e-CODEX, die Komponenten des e-CODEX-Systems, die Zuständigkeiten und Aufgaben von eu-LISA, der EU-Kommission und der Mitgliedstaaten bei der Unterhaltung von e-CODEX-Zugangspunkten und den Zeitplan für die Übernahme des e-CODEX-Systems durch eu-LISA fest. Die Verordnung sieht einen Übergang der Zuständigkeit für das e-CODEX-System zwischen dem 1.7.2023 und dem 31.12.2023 vor. Schließlich ist die Einsetzung einer e-CODEX-Beratergruppe (Art. 12) und eines Programmverwaltungsrats (Art. 13) vorgesehen. Mit den Projekten Me-CODEX II und III sollte die Übergabe von e-CODEX an eu-LISA vorbereitet und die weitere Verwaltung, Entwicklung und Pflege des Systems sichergestellt werden.[286]

234 Ausdrücklich werden in Art. 14 Verordnung auch die Prinzipien betont, die für die Unabhängigkeit der Justiz stehen: „Bei der Wahrnehmung ihrer Zuständigkeiten gemäß dieser Verordnung achten alle Stellen den Grundsatz der Unabhängigkeit der Justiz im Einklang mit dem Grundsatz der Gewaltenteilung."

235 E-CODEX – Instrumente werden bereits genutzt bei der Verknüpfung der Handelsregister (BRIS=Business Register Interconnection System), teilweise bei der elektronischen Abwicklung des europäischen Mahnverfahrens und beim grenzüberschreitenden Verfahren für geringfügige Forderungen („Small Claims") sowie bei der Durchsetzung grenzüberschreitender Unterhaltsansprüche („iSupport"). In Betracht kommt aber auch die Nutzung im Bereich des Strafprozessrechts, etwa beim Austausch von Rechtshilfeersuchen in bilateralen Pilotprojekten, bei der Umsetzung europäischer Verpflichtungen aus dem Europäischen Haftbefehl, der Vollstreckungshilfe hinsichtlich Geldstrafen und Freiheitstrafe, der Umsetzung der Vorgaben für die Europäische Ermittlungsanordnung sowie bei der elektronischen Übermittlung von elektronischen Beweismitteln, sofern die E-Evidence-VO (Dienstleister) dieses vorsieht.

236 Die Verordnung (EU) 2023/2844 des Europäischen Parlaments und des Rates vom 13.12.2023 **über die Digitalisierung der justiziellen Zusammenarbeit und des Zugangs zur Justiz in grenzüberschreitenden Zivil-, Handels- und Strafsachen** und zur Änderung bestimmter Rechtsakte im Bereich der justiziellen Zusammenarbeit[287] gilt ab 1.5.2025 (Art. 26).

237 Die Verordnung will die Effizienz und die Wirksamkeit von Gerichtsverfahren verbessern und den Zugang zur Justiz zu vereinfachen. Die Verordnung setzt **rechtliche Regeln für die elektronische Kommunikation zwischen den zuständigen Behörden/Gerichten** in Verfahren der justiziellen Zusammenarbeit (Art. 3) und für die **elektronische Kommunikation zwi-**

[284] Siehe Beschreibungen unter https://www.justiz.nrw.de/JM/doorpage_online_verfahren_projekte/projekte_d_justiz/ecodex/index.php, abgerufen am 29.2.2024.

[285] Verordnung (EU) 2022/850 vom 30.5.2022 über ein EDV-System für den grenzüberschreitenden elektronischen Datenaustausch im Bereich der justiziellen Zusammenarbeit in Zivil- und Strafsachen (e-CODEX-System) und zur Änderung der Verordnung (EU) 2018/1726 (e-CODEX-Verordnung), ABl. vom 1.6.2022, L 150/1.

[286] http://elf-fae.eu/me-codex-2/ (abgerufen am 18.2.2024).

[287] Verordnung (EU) 2023/2844 des Europäischen Parlaments und des Rates vom 13.12.2023über die Digitalisierung der justiziellen Zusammenarbeit und des Zugangs zur Justiz in grenzüberschreitenden Zivil-, Handels- und Strafsachen und zur Änderung bestimmter Rechtsakte im Bereich der justiziellen Zusammenarbeit, ABl. L, 2023/2844, 27.12.2023.

schen natürlichen oder juristischen Personen und den zuständigen Behörden/Gerichten (Art. 4) in gerichtlichen Zivil- und Handelssachen und in Strafsachen. Vorgesehen ist die elektronische Einleitung von in der Verordnung namentlich genannten gerichtlichen Verfahren gegen eine Partei aus einem anderen Mitgliedstaat über einen elektronischen Zugangspunkt auf dem Europäischen Justizportal. Ersuchen, Dokumente und Daten zwischen nationalen Behörden und Gerichten sollen im Grundsatz digital übermittelt werden. Ferner trifft die Verordnung Regelungen über die Nutzung von Videokonferenzen bei mündlichen Verhandlungen in grenzüberschreitenden Zivil-, Handels- und Strafsachen. Gebühren sollen grenzüberschreitend elektronisch über den elektronischen Zugangspunkt im Rahmen des europäischen E-Justiz-Portals bezahlt werden können (Art. 9). Elektronische Dokumente in Justizangelegenheiten sollen auf der Grundlage eines dezentralen Systems grenzüberschreitend über den elektronischen Zugangspunkt oder über nationale IT-Portale ausgetauscht werden können.

Ergänzend soll eine **Richtlinie**[288] im Wesentlichen dafür sorgen, dass die Rahmenbeschlüsse und Richtlinien im Bereich der Zivil- und Strafsachen mit den Bestimmungen des Vorschlags für eine Digitalisierungsverordnung in Einklang gebracht und widersprüchliche Rechtsvorschriften geändert werden. Außerdem wird damit dafür gesorgt, dass Mitgliedstaaten, die nicht an die Digitalisierungsverordnung gebunden sind (Irland), zumindest durch die Richtlinie auf gemeinsame Ziele verpflichtet werden. **238**

15. Medienkompetenz/E-Justice-Kompetenz

Ohne ein Basiswissen der Zusammenhänge von Technik, Recht und Organisation (E-Justice-Kompetenz) ist angesichts der immer stärker voranschreitenden Digitalisierung und der Transformationsprozesse der Rechtspflege und der Rechtspraxis eine verantwortliche Ausübung juristischer Berufe in Zukunft kaum vorstellbar. Die Vermittlung der entsprechenden Kompetenz in der Juristenausbildung bedarf zukünftig einer Ausweitung.[289] Zwar dürften die Inhalte der Lehrveranstaltungen zum Zivil-, Straf- und Öffentlichen Recht sowie zum Verfahrensrecht immer stärker auch die digitalen Fragen erfassen, die auch in der Rechtssetzung eine immer größere Rolle spielen. Sinnvoll erscheint es aber, digitale Querschnittsfragen, die das Zivil-, Straf- und Öffentliche Recht und das Verfahrensrecht gemeinsam betreffen, auch in eigenen Lehrveranstaltungen zu vermitteln. Das betrifft beispielsweise die Möglichkeiten und Funktionsweise der elektronischen Gerichtsakte im Sinne einer medienbruchfreien Kenntnisnahme und Weiterverarbeitung digitaler Dokumente, die Nutzung elektronischer Register, die Informations- und Auskunftssysteme, die mobilen Anwendungen, die Softwareunterstützung für fachbezogenes methodisches Arbeiten, die Anwaltssoftware oder die Programme und Recherchewerkzeuge und die bei der Strafverfolgung zum Einsatz kommen. Darüber hinaus sind Möglichkeiten und Grenzen des Einsatzes künstlicher Intelligenz oder der Blockchain darzustellen. Insoweit wäre es hilfreich, die E-Justice -Themen in die durch § 5a DRiG definierten zwingenden Ausbildungsinhalte aufzunehmen. Baden-Württemberg hat in vorbildlicher Weise in § 3 Abs. 2 S. 2, Juristenausbildungs- und Prüfungsordnung (JAPrO) vom 2.5.2019 ausdrücklich bei der Beschreibung der Studieninhalte „auch die zunehmende Bedeutung der Digitalisierung“ und in Abs. 5 S. 1 die „digitalen Kompetenzen“ erwähnt. **239**

[288] Richtlinie (EU) 2023/2843 vom 13.12.2023 zur Änderung der Richtlinien 2011/99/EU und 2014/41/EU des Europäischen Parlaments und des Rates, der Richtlinie 2003/8/EG des Rates und der Rahmenbeschlüsse 2002/584/JI, 2003/577/JI, 2005/214/JI, 2006/783/JI, 2008/909/JI, 2008/947/JI, 2009/829/JI und 2009/948/JI des Rates im Hinblick auf die Digitalisierung der justiziellen Zusammenarbeit, ABl. L vom 27.12.2023.

[289] Bernhardt/Leeb in: Kramer/Kuhn/Putzke, Was muss Juristenausbildung heute leisten? 84 ff. Bernhardt jM 2022, 96; Herberger: ejustice-Kompetenz – Plädoyer für ein Ausbildungskonzept, in: Thomas Gottwald (Hrsg.) e-Justice in Österreich. Erfahrungsberichte und europäischer Kontext, FS Martin Schneider, 2013, S. 391–402.