Institut für Europäisches Medienrecht
Institute of European Media Law
Institut du droit européen des médias

Das aktuelle Stichwort

Datenschutz ohne Grenzen?

Zum Verhältnis von Datenschutz-Grundverordnung der EU zur Novelle des Datenschutzrechts des Europarates

Von Dr. Jörg Ukrow

Geschäftsführendes Vorstandsmitglied des EMR

I. Einleitung

Seit dem 25. Mai 2018 gilt innerhalb der Europäischen Union die am 24. Mai 2016 in Kraft getretene Datenschutzgrundverordnung. Diese fast zweijährige Übergangsphase konnte nicht nur von den Mitgliedstaaten der EU genutzt werden, um bestehendes nationales Datenschutzrecht anzupassen und Abweichungs- und Ausnahmemöglichkeiten, die die DSGVO nicht zuletzt auch mit Blick auf das in deren Art. 85 adressierte sog. Medienprivileg eröffnet, auszuschöpfen. Sie konnte auch von diesen Mitgliedstaaten der EU wie den übrigen Vertragsparteien des Europarates genutzt werden, um Friktionen im auf zwei Säulen beruhenden europäischen datenschutzrechtlichen Regulierungssystem soweit möglich zu vermeiden. Gemeinsames europäisches[1] Fundament dieses europäischen, aus den Säulen von EU- und Europaratsrecht aufgebauten Datenschutzsystems ist der Grundrechtsschutz der EMRK, der für die Säule des Datenschutzrechts der EU eine Ergänzung in der Grundrechtscharta der EU gefunden hat.

Beim derzeitigen Stand des Datenschutzrechts des Europarats ergänzen sich Art. 8 EMRK einerseits und die (Datenschutz-) Konvention 108 des Europarates aus 1981,[2] das

---

1 International hat der Datenschutz eine Anerkennung im Ansatz bereits in Art. Art. 12 der Allgemeinen Erklärung der Menschenrechte der Generalversammlung der Vereinten Nationen aus 1948 gefunden, wonach „(n)iemand ... willkürlichen Eingriffen in sein Privatleben, ... seine Wohnung und seinen Schriftverkehr .... ausgesetzt werden (darf)“ und „(j)eder ... Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen (hat)“. An diese völkerrechtlich nicht verbindliche Verbotsnorm knüpfen datenschutzrechtlich relevante und völkerrechtlich die Unterzeichnerstaaten bindende Verankerungen des Rechts auf Privatheit in Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte aus 1966 (999 UNTS 171), Art. 16 des Übereinkommen über die Rechte des Kindes aus 1989 (1577 UNTS 3) und Art. 14 der Internationalen Konvention zum Schutz der Rechte aller Wanderarbeitnehmer und ihrer Familienangehörigen aus 1990 (2220 UNTS 3) und an.

2 Bereits 2001 wurde zur Anpassung an die Entwicklung innerhalb der EU wurde ein Zusatzprotokoll betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (European Treaty Series No. 181) verabschiedet, das 2004 in Kraft trat. Es verpflichtet die beitretenden Staaten zur Einrichtung unabhängiger Kontrollstellen und zur Einführung von Regeln für den Transfer von Daten in Staaten, die keine Parteien des Übereinkommens sind.

„Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“[3] andererseits gegenseitig.[4] Dem grundrechtlichen Schutz durch Art. 8 EMRK kommt dabei nicht zuletzt deshalb eigenständige Bedeutung zu, weil die Konvention ausschließlich die automatisierte Datenverarbeitung, nicht die Datenverarbeitung im Übrigen erfasst und nur über eine Verletzung des Art. 8 EMRK die Möglichkeit einer auf Verletzung von Datenschutzrecht gestützten Individualbeschwerde eines Bürgers gegen seinen Staat nach Art. 34 EMRK besteht. Auf der anderen Seite reicht die Konvention insofern weiter, als sie schon nach ihrer derzeitigen Fassung in Art. 3 ausdrücklich auch die Datenverarbeitung im nicht-öffentlichen Bereich erfasst.[5] Diese Datenverarbeitung kann unter EMRK-Blickwinkel im Kern nur mit Blick auf eine etwaige Verletzung datenschutzrechtlicher Schutz- und Gewährleistungspflichten bedeutsam sein.[6]

Kurz vor dem Beginn der Geltung der DSGVO hat das Ministerkomitee des Europarates am 18. Mai 2018 – auch zur Vermeidung der genannten Widersprüche - ein Änderungsprotokoll zur Aktualisierung seiner Datenschutzkonvention aus 1981 verabschiedet. Dieses Änderungsprotokoll,[7] bei dem es sich um einen völkerrechtlichen Vertrag handelt, wird am 25. Juni 2018 in Straßburg zur Zeichnung aufgelegt, dem ersten Tag der Sommersitzung der Parlamentarischen Versammlung des Europarates[8] und gleichzeitig genau ein Monat nach Beginn der Geltung der DSGVO. Die Datenschutzkonvention des Europarates soll über dieses Protokoll stärker als bisher als globales Instrument "vermarktet" werden, um Mindeststandards für grenzüberschreitende Datenströme auch außerhalb des Rahmens des Europarates zu gewährleisten.[9]

---

3 Abrufbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/rms/0900001680078b38

4 Bei dieser Konvention handelt es sich um das erste internationale rechtsverbindliche Übereinkommen zum Schutz personenbezogener Daten; zu datenschutzbezogenen Regulierungsansätzen im außereuropäischen Raum vgl. *Malanczuk*, Data, Transboundary Flow, International Protection, in: Wolfrum (ed.), Max Planck Encyclopedia of Public International Law, Vol. II 2010, S. 1033 ff. Tz. 9 ff., 12, 25.

Kapitel II der Konvention der Afrikanischen Union über Cybersicherheit und den Schutz persönlicher Daten, das dem Schutz persönlicher Daten gewidmet ist, orientiert sich deutlich an dieser Konvention. Diese am 27. Juni 2014 von der Versammlung der Afrikanischen Union verabschiedete Konvention vom 27. Juni 2014 (online abrufbar unter https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.) ist allerdings bislang (Stand: 10. Mai 2018) nur von 10 Mitgliedstaaten der Afrikanischen Union signiert und lediglich von Mauritius und dem Senegal ratifiziert; vgl. https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf.

5 Vgl. *Hornung*, Fortentwicklung des datenschutzrechtlichen Regelungssystems des Europarats, DuD 28 (2004), 719 (721)

6 Zu Schutz- und Gewährleistungspflichten des Staates nach der EMRK vgl. z.B. *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, 5. Aufl. 2012, § 19; *Krieger*, Positive Verpflichtungen unter der EMRK: Unentbehrliches Element einer gemeineuropäischen Grundrechtsdogmatik, leeres Versprechen oder Grenze der Justiziabilität?, ZaöRV 74 (20149, S. 187 ff.

7 Eine konsolidierte Fassung des Übereinkommens unter Berücksichtigung dieses Protokolls ist abrufbar unter https://rm.coe.int/16808ade9d.

8 Vgl. https://www.coe.int/de/web/portal/-/enhancing-data-protection-globally-council-of-europe-updates-its-landmark-convention

9 Vgl. https://www.heise.de/newsticker/meldung/Europarat-will-Datenschutzkonvention-zum-globalen-Minimialstandard-machen-1389776.html

Der nachfolgende Beitrag untersucht unter besonderer Berücksichtigung von geographischem, personellem, sachlichem und funktionalem Anwendungs- und Geltungsbereich der DSGVO einerseits, der Konvention 108 in der Fassung des Änderungsprotokolls andererseits, inwieweit die gewünschte Widerspruchsfreiheit dieser beiden Rechtsinstrumente erreicht wurde. Vergleichende Bezugnahmen zur Situation auf dem Feld der Regulierung audiovisueller Mediendienste zeigen auf, inwieweit ein aufsichtsrechtlicher Gleichklang zwischen EU- und Europaratsrecht auf dem Feld der datenschutzrechtlichen Durchsetzung von Gemeinwohlinteressen über die Ansätze dieser Durchsetzung auf dem Feld der audiovisuellen Regulierung hinaus erreicht wurde. Abschließend wird erörtert, inwieweit der globale Orientierungsanspruch des Protokolls auf dem Feld des Datenschutzes auch mit Blick auf den anstehenden Brexit bedeutsam sein kann.

II. Der Anwendungsbereich der Regelungswerke

1. Der personelle Anwendungsbereich

Wie die DS-GVO[10] hat auch die Datenschutzkonvention[11] in der Fassung des Änderungsprotokolls den Datenschutz von Personen unabhängig von ihrer Staatsangehörigkeit oder ihrem Sitz im Blick.

2. Der geographische Geltungsanspruch der Regelungswerke

Die DSGVO gilt gemäß Art. 288 Abs. 2 Satz 2 AEUV unmittelbar in jedem Mitgliedstaat. Es bedurfte für deren Geltung mithin keines weiteren Umsetzungsaktes eines Mitgliedstaates der EU zur Transformation der DS-GVO in innerstaatliches Recht. Die EU-Mitgliedstaaten waren und sind verpflichtet, nationale Vorschriften, die durch die Verordnung ersetzt werden, aufzuheben.

Zur Wahrung einer fortdauernden Homogenität des Datenschutzrechts auch innerhalb des Europäischen Wirtschaftsraums (EWR)[12] ist es für die EFTA-Staaten Norwegen, Island und Lichtenstein erforderlich die DS-GVO in das EWR-Abkommen aufzunehmen und so die Anwendbarkeit des Regelwerkes auch für außerhalb des Rahmens der EU zu begründen: Über den Mechanismus der Art. 92 ff., 102 Abs. 1 bis Abs. 6 EWR-Abkommen i.V.m. der Verordnung (EG) Nr. 2894/94 kann die DSGVO auch innerhalb des Europäischen Wirtschaftsraums, der neben den Mitgliedstaaten der EU auch die EFTA-Staaten Norwegen, Island und Lichtenstein umfasst, Geltung beanspruchen. Im Interesse eines unbegrenzten EWR-weiten-Informations-Binnenmarktes erscheint ein rascher Abschluss des laufenden Übernahmeverfahrens sinnvoll und zugleich machbar.[13]

---

10 Für die EU folgt dieser weite personelle Anwendungsbereich nicht zuletzt auch aus Art. 8 Abs. 1 der Grundrechtecharta der EU und Art. 16 Abs. 1 AEUV.

11 Vgl. Art. 1 der Konvention

12 Die Vorgängerregelung der DS-GVO, die Datenschutzrichtlinie der EG 1995/46/EG, war in ihrer ursprünglichen Fassung Bestandteil des EWR-acquis; vgl. Beschluss des Gemeinsamen EWR-Ausschusses Nr. 83/1999 vom 25. Juni 1999 zur Änderung des Protokolls 37 und des Anhangs IX (Telekommunikationsdienste) zum EWR-Abkommens, ABl. EU 200 Nr. L 296/41.

13 Derzeit befindet sich der entsprechende Übernahmebeschluss des Joint Committee des EWR und der EFTA bei der EU-Kommission. Nach Auskunft Liechtensteins wird die DSGVO vor-aussichtlich "Anfang Juli" 2018 auch für die drei dem EWR angehörenden EFTA-Staaten in Kraft treten; vgl. http://datenrecht.ch/liechtenstein-anwendbarkeit-der-dsgvo-voraussichtlich-ab-anfang-juli-2018/.

Die Schweiz, die kein Mitglied des EWR ist, bereitet zudem eine Novelle ihres Datenschutzrechts vor, die sich eng an der DS-GVO orientieren soll. Von staatlicher schweizerischer Seite wird betont, dass Firmen, die sich schon auf die DSGVO eingestellt haben, dann, wenn die Schweizer Version fertig ist, bei deren Umsetzung eine erhebliche Zeitersparnis haben dürften.[14]

Das Protokoll zur Änderung der Datenschutzkonvention des Europarates ist in seinem Geltungsanspruch im Vergleich zur DSGVO einerseits zeitlich aufgeschoben, andererseits geographisch potentiell deutlich weiter reichend.

Nach seinem Art. 37 Abs. 1 tritt dieses Protokoll am ersten Tag des Monats in Kraft, der auf den Ablauf von drei Monaten nach dem Tag folgt, an dem alle Vertragsparteien des Übereinkommens ihre Zustimmung zu einer Bindung an das Protokoll gemäß Art. 36 Abs. 1 dieses Protokolls[15] abgegeben haben. Ist dieses Protokoll danach nicht in Kraft getreten, so tritt es gemäß seinem Art. 37 Abs. 2 am 25. Juni 2023 für die Staaten in Kraft, die ihre Zustimmung erklärt, an das Protokoll gebunden zu sein, sofern mindestens achtunddreißig Parteien dem Protokoll angehören. Bis zum Inkrafttreten dieses Protokolls und unbeschadet der Bestimmungen über das Inkrafttreten und den Beitritt durch Nichtmitgliedstaaten oder internationale Organisationen kann eine Vertragspartei des Übereinkommens gemäß Art. 37 Abs. 3 des Protokolls zum Zeitpunkt der Unterzeichnung dieses Protokolls oder zu einem beliebigen späteren Zeitpunkt erklären, dass sie die Bestimmungen dieses Protokolls vorläufig anwenden wird. In diesen Fällen gelten die Bestimmungen dieses Protokolls nur für die anderen Vertragsparteien des Übereinkommens, die eine entsprechende Erklärung abgegeben haben.

Die Mitgliedschaft an der Datenschutz-Konvention des Europarates ist auch unter dem Regime des Änderungsprotokolls nicht auf die Vertragsstaaten des Europarates beschränkt: Nach Art. 27 Abs. 1 der Konvention kann das Ministerkomitee des Europarats bei einstimmiger Zustimmung der Vertragsparteien dieses Übereinkommens jeden Staat, der kein Mitglied des Europarats ist, oder eine internationale Organisation einladen, diesem Übereinkommen beizutreten.[16] Damit erhebt die Datenschutz-Konvention des Europarates auch weiterhin einen potentiell globalen Geltungsanspruch.

Die Datenschutzkonvention des Europarates ist von sämtlichen derzeit noch 28 Mitgliedstaaten der EU sowie den weiteren 19 Mitgliedstaaten des Europarates unterzeichnet und ratifiziert. Als Nichtmitgliedstaaten des Europarates haben zudem Mauritius, Senegal, Tunesien und Uruguay die Konvention ratifiziert.[17]

---

14 Vgl. https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/e-commerce/eu-regelung-zum-datenschutz.html

Vgl. im Übrigen auch Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz (Stand: Mai 2018), abrufbar über https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/rechtliche-grundlagen/Datenschutz%20-%20International/DSGVO.html

15 Nach Satz 2 dieser Regelung bedarf das Protokoll der Ratifikation, Annahme oder Genehmigung. Die Herstellung der Zustimmung zur Bindung richtet sich mithin nach dem Verfassungsrecht des jeweiligen Signatarstaates.

16 Der Beitrittsbeschluss muss mit der Mehrheit nach Artikel 20 Buchstabe d des Statuts des Europarats und einstimmig von den Vertretern der Vertragsstaaten, die berechtigt sind, im Ministerkomitee zu sitzen, getroffen werden.

17 Eine Einladung zur Mitgliedschaft besteht zudem immer noch gegenüber Argentinien, Burkina Faso, den Kapverden und Mexiko; vgl. zum Ganzen https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=aTKfOVNZ.

3. Der sachlich-funktionale Anwendungsbereich der Regelungswerke

Der sachliche Anwendungsbereich der Regelungswerke ist im Grundsatz nach In-Kraft-Treten des Änderungsprotokolls identisch: Vom Geltungsbereich der Regelungswerke erfasst sind danach in beiden Regelwerken die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[18] Erfasst sind Datenverarbeitungen im öffentlichen wie im privaten Bereich. Betroffen sind von beiden Regelungswerken alle, die personenbezogene Daten verarbeiten, also vor allem Unternehmen und Selbstständige – aber auch das elektronische Mitgliederverzeichnis eines Vereins fällt schon in den Anwendungsbereich beider Regelungswerke. Ob mit Blick auf den mit den nunmehr erforderlichen Datenschutzvorkehrungen Betroffener verbundenen finanziellen und organisatorischen Aufwand nicht eine differenzierende Herangehensweise – z.B. in Form von *de-minimis*-Regeln – sinnvoll gewesen wäre, ist eine aktuell im Zusammenhang mit der DS-GVO diskutierte Frage, die indessen in gleicher Weise auch mit Blick auf die Datenschutzkonvention gestellt werden kann. Rechtspolitisch wäre für beide Regelungswerke überlegenswert gewesen, das datenschutzrechtliche Anforderungsprofil für Unternehmen mit einem bedeutsamen Umsatz und/oder mit einer erheblichen Anzahl von Kontakten umfassender auszugestalten als für KMU oder gar mitgliederschwache Vereine. Anknüpfungspunkte für einen solchen differenzierenden, am Verhältnismäßigkeitsgrundsatz ausgerichteten Regelungsansatz finden sich jüngst z.B. in Bezug auf Anbieter sozialer Netzwerke in § 1 Abs. 2 NetzDG[19] sowie – an diesen Ansatz anknüpfend – in § 68a Saarländisches Mediengesetz.[20]

Ausgenommen vom Anwendungsbereich sind nach DS-GVO wie Datenschutzkonvention Privatpersonen, wenn diese Daten ausschließlich für persönliche oder familiäre Zwecke verwenden.[21]

Der Katalog der Ausnahmetatbestände vom sachlichen Anwendungsbereich ist im Übrigen bei der DS-GVO weiter gefasst als bei der Datenschutzkonvention. Er umfasst im Rahmen der DS-GVO nach deren Art. 2 Abs. 2 Buchst. a), b) und d) auch die Verarbeitung personenbezogener Daten

- im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,
- durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich der Gemeinsamen Außen- und Sicherheitspolitik (GASP) der EU nach Titel V Kapitel 2 EUV fallen, sowie
- durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

---

18 Vgl. Art. 2 Abs. 1 DS-GVO; Art. 3 der Konvention

19 Danach ist der Anbieter eines sozialen Netzwerks ist von den Berichts- und Beschwerdemanagement-Pflichten nach den §§ 2 und 3 NetzDG (BGBl. 2017 I S. 3352) befreit, wenn das soziale Netzwerk im Inland weniger als zwei Millionen registrierte Nutzer hat.

20 Nach dem am 25. Mai 2018 in Kraft getretenen § 68a Abs. 4 Saarländisches Mediengesetz (SMG) (Amtsblatt des Saarlandes 2017, Teil I, S. 268) gilt die Pflicht des Anbieters eines sozialen Netzwerks, dessen Angebot sich auch an das Saarland richtet, zur Bestellung eines inländischen Zustellungsbevollmächtigten zur Effektuierung der Aufsichtstätigkeit der Landesmedienanstalt Saarland im Bereich des Vollzugs des SMG, des RStV und des JMStV nicht, wenn das soziale Netzwerk im Saarland weniger als 50.000 registrierte Nutzer hat.

21 Vgl. Art. 2 Abs. 2 Buchst. c) DS-GVO; Art. 3 Abs. 2 Datenschutzkonvention

Bei Tätigkeiten eines EU-Mitgliedstaates, die nicht in den Anwendungsbereich des Unionsrechts fallen oder innerhalb der GASP erfolgen, greift für die betreffenden Mitgliedstaaten allerdings grundsätzlich die Datenschutzkonvention. In Bezug auf GASP-Tätigkeiten wie auch mit Blick auf strafprozess- und strafvollstreckungsrechtliche Schranken der Datenverarbeitung[22] greift im Rahmen des Europarates-Regimes allerdings ggf. die Ausnahmemöglichkeit nach Art. 11 Abs. 1 Buchst. a) der Datenschutzkonvention.

Während die DS-GVO im Grundsatz eine abschließende Regelung für den Datenschutz innerhalb der EU begründet, die prinzipiell Abweichungen weder zu Gunsten noch zu Lasten des durch die Verordnung erreichten Datenschutzniveaus gestattet, ist die Datenschutzkonvention auch in der Fassung des Änderungsprotokolls offener in Form bloßer datenschutzrechtlicher Mindeststandards ausgestaltet: Nach Art. 13 der Konvention ist keine der Bestimmungen des Kapitels II der Konvention, die „Grundprinzipien für den Schutz personenbezogener Daten" zum Gegenstand hat, dahin auszulegen, dass die Möglichkeit einer Vertragspartei, den betroffenen Personen ein größeres Maß an Schutz zu gewähren als in diesem Übereinkommen vorgesehen, eingeschränkt oder anderweitig beeinträchtigt wird.

Dieser generellen Abweichungsmöglichkeit der Konvention zu Gunsten eines umfassenderen Datenschutzes stehen vereinzelte Öffnungsklauseln der DS-GVO gegenüber: Die Mitgliedstaaten der EU sind danach ermächtigt, die Regelungen der Verordnung – wie z.B. beim Beschäftigtendatenschutz nach Art. 88 DS-GVO – zu konkretisieren oder – wie z.B. bei der Ausgestaltung des sog. Medienprivilegs nach Art. 85 DS-GVO oder bei der Gewährung des Verbandsklagerechts nach Art. 80 Abs. 2 DS-GVO – zu ergänzen. In einzelnen Bereichen, wie z.B. bei der Frage der Altersgrenze für eine rechtswirksame Einwilligung in eine Datenverarbeitung, besteht im Rahmen solcher Öffnungsklauseln zudem die Möglichkeit, von Regelungsansätzen der DS-GVO auch in einer den Datenschutz faktisch verkürzenden Weise abzuweichen.[23]

III. Grundsätze für die Bearbeitung personenbezogener Daten nach den beiden Regelungswerken

Die Grundsätze für die Bearbeitung personenbezogener Daten nach den beiden Regelungswerken sind im Wesentlichen deckungsgleich, wie aus nachfolgender Tabelle ersichtlich ist:

Grundsatz	DS-GVO	Datenschutzkonvention
„Rechtmäßigkeit"[24]	Art. 5 Abs. 1 Buchst. a)	Art. 5 Abs. 3

22 Für die EU.-Mitgliedstaaten ist insoweit die Richtlinie (EU) 2016/680 vom 27. April 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 (Amtsbl. EU 2016 Nr. L 119/89) bedeutsam.

23 Die Einwilligung eines Kindes zur Datenverarbeitung rechtfertigt nach Art. 8 Abs. 1 Satz 1 DS-GVO bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, die Verarbeitung der personenbezogenen Daten des Kindes nur, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Die Mitgliedstaaten können nach Satz 3 der Regelung allerdings eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

24 Personenbezogene Daten müssen nach diesem Grundsatz auf rechtmäßige Weise verarbeitet werden.

„Fairness“[25]	Art. 5 Abs. 1 Buchst. a)	Art. 5 Abs. 4 Buchst. a)
„Transparenz“[26]	Art. 5 Abs. 1 Buchst. a)	Art. 5 Abs. 4 Buchst. a)
„Zweckbindung“[27]	Art. 5 Abs. 1 Buchst. b)	Art. 5 Abs. 4 Buchst. b)
„Datenminimierung“[28]	Art. 5 Abs. 1 Buchst. c)	Art. 5 Abs. 4 Buchst. c)
„Richtigkeit“[29]	Art. 5 Abs. 1 Buchst. d)	Art. 5 Abs. 4 Buchst. d)
„Speicherbegrenzung“[30]	Art. 5 Abs. 1 Buchst. e)	Art. 5 Abs. 4 Buchst. e)
„Integrität und Vertraulichkeit“[31]	Art. 5 Abs. 1 Buchst. f)	
„Rechenschaftspflicht“[32]	Art. 5 Abs. 2	Art. 10 Abs. 1
Grundsätzliches Verbot der Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen	Art. 9	Art. 6 Abs. 1 4. Spiegelstrich
Grundsätzliches Verbot der Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten	Art. 9	Art. 6 Abs. 1 1., 3. und 4. Spiegelstrich

25 Personenbezogene Daten müssen nach diesem Grundsatz nach Treu und Glauben verarbeitet werden.

26 Personenbezogene Daten müssen nach diesem Grundsatz in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

27 Personenbezogene Daten müssen nach diesem Grundsatz für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke bleibt hiervon unberührt.

28 Personenbezogene Daten müssen nach diesem Grundsatz dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

29 Personenbezogene Daten müssen nach diesem Grundsatz sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

30 Personenbezogene Daten müssen nach diesem Grundsatz in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

31 Personenbezogene Daten müssen nach diesem Grundsatz in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

32 Nach diesem Grundsatz ist der Verantwortliche für die Einhaltung der vorbezeichneten Grundsätze verantwortlich und muss deren Einhaltung nachweisen können.

zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person		
Begrenzung der Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten	Art. 10	Art. 6 Abs. 1 2. Spiegelstrich

Während allerdings im Rahmen der GS-DVO Abweichungen vom Grundsatz der Speicherbegrenzung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke ausdrücklich ermöglicht sind, sieht der Wortlaut der Datenschutzkonvention solche Abweichungen nicht ausdrücklich vor. Gegebenenfalls lassen sich solche Abweichungen zwar auch unter dem Datenschutzrecht des Europarates über die generelle Abweichungsmöglichkeit nach Art. 11 der Konvention rechtfertigen. Bei systematischer Auslegung der Konvention spricht dagegen allerdings, dass diese Zweckerreichungs-Tatbestände in Art. 11 Abs. 2 der Konvention nur in Bezug auf die Transparenzregelungen des Art. 8 und die Rechte des Datensubjektes nach Art. 9 der Konvention adressiert sind, während die in Art. 5 der Konvention geregelten Grundsätze der Datenverarbeitung nicht angesprochen werden.

Der Katalog von Ausnahmegründen, der in Art. 9 Abs. 2 DS-GVO mit Blick auf Abweichungen vom grundsätzlichen Verbot der Verarbeitung besonders sensibler, namentlich auch das Risiko von Diskriminierungen auslösenden[33] personenbezogener Daten enthalten ist, dürfte zwar vollumfänglich mit der Ausnahmeklausel in Art. 6 Abs. 1 und 2 der Datenschutzkonvention in Einklang stehen, wonach die Datenverarbeitung nur erlaubt ist, wenn geeignete Garantien gesetzlich verankert sind und die Bestimmungen dieses Übereinkommens ergänzen, mittels derer vor den Risiken geschützt wird, die die Verarbeitung dieser sensiblen Daten für die Interessen, Rechte und grundlegende Freiheiten des Datensubjektes darstellen kann. Allerdings ist diese Ausnahmeklausel der Datenschutzkonvention im Lichte ihres offenen und weiten Wortlauts nicht auf die Ausnahmetatbestände der DS-GVO begrenzt. Die Mitgliedstaten der EU können sich indessen nicht auf die Konvention stützen, um das Verbot der Verarbeitung der sensiblen Daten über die Ausnahmebestimmungen der DS-GVO selbst auszuhöhlen.

IV. Insbesondere: Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Während die DS-GVO generelle Bedingungen für die Rechtmäßigkeit der Datenverarbeitung regelt, ist die Datenschutzkonvention enger gefasst. Den die Konvention hat in Kapitel III nur grenzüberschreitende Flüsse persönlicher Daten im Zusammenhang mit dem in Art. 1 der Konvention umfassend definierten Ziel und Zweck der Konvention, dem Schutz jedes Einzelnen im Hinblick auf die Verarbeitung seiner persönlichen Daten, zum Gegenstand.

Auch in Bezug auf die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gibt es zudem lediglich im Ansatz, nicht in der Ausformung einen Gleichklang zwischen den beiden Regelungswerken:

Rechtfertigungsgrund für die Verarbeitung	DS-GVO	Datenschutzkonvention

[33] Vgl. hierzu Art. 6 Abs. 2 der Datenschutzkonvention

Einwilligung der betroffenen Person zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke	Art. 6 Abs. 1 Unterabs. 1 Buchst. a), Art. 7, 8	Art. 14 Abs. 4 Buchst. a)
Erforderlichkeit zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen	Art. 6 Abs. 1 Unterabs. 1 Buchst. b)	Art. 14 Abs. 4 Buchst. b)
Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt[34]	Art. 6 Abs. 1 Unterabs. 1 Buchst. c)	Art. 14 Abs. 4 Buchst. b)
Erforderlichkeit zum Schutz lebenswichtiger Interessen einer natürlichen Person[35]	Art. 6 Abs. 1 Unterabs. 1 Buchst. d)	Art. 14 Abs. 4 Buchst. b)
Erforderlichkeit für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde	Art. 6 Abs. 1 Unterabs. 1 Buchst. e)	Art. 14 Abs. 4 Buchst. c)
Erforderlichkeit zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen	Art. 6 Abs. 1 Unterabs. 1 Buchst. f)	Art. 14 Abs. 4 Buchst. c)
sog. Medienprivileg	Art. 85	Art. 14 Abs. 4 Buchst. d)

Gemeinsam ist beiden Regelungswerken die Berücksichtigung des Verhältnismäßigkeitsgrundsatzes und der Referenzrahmen einer demokratischen Gesellschaft bei der Frage der Legalität der Datenverarbeitung.[36]

Während in Art. 7 DS-GVO die Anforderungen an eine rechtlich beachtliche Einwilligung in die Datenverarbeitung im Detail ausgeführt sind, beschränkt sich die Konvention in Art. 14 Abs. 4

34 Ein typischer diesbezüglicher Fall dürfte die Aufbewahrung von Daten im Hinblick auf die Erfüllung einer steuerrechtlichen Erklärungs- und Abgabepflicht sein.

35 Ein entsprechender Fall ist z.B. die Ermittlung der Blutgruppe eines an einem Unfall beteiligten oder von einem Terroranschlag betroffenen Opfers, das in Lebensgefahr schwebt.

36 Vgl. Art. 23 DS-GVO, Art. 14 Abs. 4 Buchst. c) Datenschutzkonvention

Buchst. a) darauf, dass das Datensubjekt für den Datenfluss eine ausdrückliche, spezifische und freie Einwilligung erteilt hat, nachdem es über Risiken informiert wurde, die bei Fehlen geeigneter Schutzmaßnahmen auftreten.

Auch das in Art. 14 Abs. 4 Buchst. b) der Konvention für die Zulässigkeit des Datenflusses genannte Kriterium, dass spezifische Interessen des Datensubjekts den Datentransfer im besonderen Fall erfordern, erfasst erkennbar nicht nur die in Art. 6 Abs. 1 Unterabs. 1 Buchst. b) und c) DS-GVO erfassten Sachverhalte.

Bemerkenswert ist, dass dem sog. Medienprivileg nach der geänderten Datenschutzkonvention wie nach der DS-GVO Bedeutung nicht nur im Zusammenhang mit dem Datentransfer bei klassischen Medien wie Presse und Rundfunk zukommen kann, sondern auch mit Blick auf neue Medienakteure wie audiovisuelle Mediendienste auf Abruf, Plattformen (namentlich Videosharing-Plattformen) und Informationsintermediäre relevant sein kann, soweit diese Akteure im massenkommunikativen Gefüge als neuartige Faktoren und Mittler der Meinungsbildung bedeutsam sind.

V. Rechte des Betroffenen

Der Betroffene hat auch nach In-Kraft-Treten des Protokolls innerhalb der EU umfassendere Rechte auf der Grundlage der DS-GVO, wie nachfolgende Tabelle unterstreicht:

Recht ...	DS-GVO	Datenschutzkonvention
„ auf Information	Art. 12 Abs. 1, 4, 5 und 7 i.V.m. Art. 13 und 14	Art. 8
... auf Auskunft	Art. 12 Abs. 1 bis 6 i.V.m. Art. 15	Art. 9 Abs. 1 Buchst. b)
... auf Berichtigung	Art. 12 Abs. 1 bis 6 i.V.m. Art. 16, Art. 19	Art. 9 Abs. 1 Buchst. e)
„ auf Löschung	Art. 12 Abs. 1 bis 6 i.V.m. Art. 17, Art. 19	Art. 9 Abs. 1 Buchst. e)
... auf „Vergessenwerden“	Art. 12 Abs. 1 bis 6 i.V.m. Art. 17, Art. 19	./.
... auf Einschränkung der Verarbeitung	Art. 12 Abs. 1 bis 6 i.V.m. Art. 18, Art. 19	Art. 9 Abs. 1 Buchst. d)
... auf Datenübertragbarkeit	Art. 12 Abs. 1 bis 6 i.V.m. Art. 20	./.
... zum Widerspruch gegen die Verarbeitung	Art. 12 Abs. 1 bis 6 i.V.m. Art. 21	Art. 9 Abs. 1 Buchst. d)
... nicht auf der Basis von automatisierten Verarbeitungen beurteilt zu werden (inkl. Profiling)	Art. 12 Abs. 1 bis 6 i.V.m. Art. 22	Art. 9 Abs. 1 Buchst. a)

Namentlich enthält die Konvention auch weiterhin weder ein Recht auf Datenübertragbarkeit noch ein Recht auf „Vergessenwerden“. Diese beiden durch die DS-GVO eingeräumten Rechte werden lediglich in dem Erläuternden Bericht zur neugefassten Datenschutzkonvention adressiert – dort allerdings ohne hinreichende juristische Substanz.

So befasst sich der Erläuternde Bericht mit der Frage der Datenübertragbarkeit lediglich bei den Erläuterungen zu Art. 10 Abs. 3 der Konvention, wonach die für die Verarbeitung Verantwortlichen und gegebenenfalls die Verarbeiter technische und organisatorische Maßnahmen einsetzen, die die Auswirkungen des Rechts auf Schutz der persönlichen Daten in allen Stadien der Datenverarbeitung berücksichtigen. Im Zusammenhang mit dem damit angesprochenen Datenschutz durch Design plädiert der Erläuternde Bericht u.a. auch für Datenportabilitätstools, d.h. einfach zu verwendende Tools, die es den betroffenen Personen ermöglichen, ihre Daten an einen anderen Anbieter ihrer Wahl zu übertragen oder die Daten selbst zu behalten. [37]

Desweiteren sieht der Erläuternde Bericht zur neugefassten Datenschutzkonvention in einer für ein Recht auf „Vergessenwerden" relevanten Weise zwar vor, dass im Falle von Berichtigungen und Löschungen, die gemäß den Rechten des Betroffenen vorgenommen werden, diese den Empfängern der ursprünglichen Informationen möglichst zur Kenntnis gebracht werden. Allerdings besteht diese Empfehlung nach dem Bericht bereits dann nicht, wenn mit diesem Verfahren unverhältnismäßige Anstrengungen verbunden wären.[38] Zudem ist eine Verletzung dieser Empfehlung ebenso wenig sanktioniert wie ein Ausbleiben einer Reaktion der Empfänger der ursprünglichen Informationen auf ein solches In-Kenntnis-setzen..

Allerdings ist die Ausformung der Rechte der Betroffenen in der DS-GVO deutlich detaillierter und damit eine Verletzung der Rechte im Streitfall leichter nachweisbar als im Rahmen der Datenschutzkonvention.

VI. Zum Dialog zwischen DS-GVO und Datenschutzkonvention

1. Wechselseitige Bezüge in den Regelungswerken

DS-GVO und Datenschutzkonvention sind in nicht unerheblicher Weise aufeinander bezogen. Sie tragen dabei – in unterschiedlicher Weise – dem Umstand Rechnung, dass der Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig ist.[39].

Für die EU ist in der DS-GVO zunächst klargestellt, dass das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen bei der Übermittlung personenbezogener Daten aus der EU an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden sollte und dass derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig sind. [40].

Nach Art. 45 Abs. 1 Satz 1 DS-GVO darf eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erst dann vorgenommen werden, wenn die Kommission der EU beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale

---

37 Vgl. Council of Europe, Explanatory Report tot he Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal , Strasbourg, 25.VI.2018, Tz. 89 (abrufbar unter https://rm.coe.int/16808ac91a)

38 Vgl. Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal , Strasbourg, 25.VI.2018, Tz. 81 (abrufbar unter https://rm.coe.int/16808ac91a)

39 Vgl. Satz 1 des 101. Erwägungsgrund der DS-GVO

40 Vgl. Sätze 3 und 4 des 101. Erwägungsgrund der DS-GVO

Organisation ein angemessenes Schutzniveau bietet. Die hierbei zu berücksichtigenden Faktoren sind (nicht abschließend) im Katalog des Art. 45 Abs. 2 DS-GVO aufgeführt und umfassen u.a. Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten, Existenz und Effektivität unabhängiger Datenschutz-Aufsichtsbehörden sowie eingegangene internationale Verpflichtungen. In Bezug auf letzteres verweist der 105. Erwägungsgrund der DS-GVO ausdrücklich auf den Beitritt eines Drittlandes zur Datenschutzkonvention des Europarates aus1981.

Die Datenschutzkonvention nimmt zwar ebenso wenig wie die DS-GVO in ihrem Text auf den zweiten Pfeiler des europäischen Datenschutzrechts Bezug. Allerdings unterstricht der Erläuternde Bericht zum Protokoll zur Datenschutzkonvention, dass die Modernisierungsarbeiten an der Konvention im breiteren Kontext verschiedener paralleler Reformen der internationalen Datenschutzinstrumente durchgeführt wurden und hebt dabei insbesondere die Parallelität zum EU-Datenschutzreformpaket hervor, wobei der Bericht betont, dass größte Sorgfalt darauf verwendet wurde, die Kohärenz zwischen den beiden Rechtsrahmen sicherzustellen. [41]

2. Zum Fehlen einer ausdrücklichen Kollisionsregel

Während das Europäische Fernsehübereinkommen des Europarates (FsÜ) in seinem Art. 27 Abs. 1 eine ausdrückliche Kollisionsregel zum Verhältnis zwischen Konventions- und EU-Recht enthält, fehlt eine solche Regelung im Bereich der Datenschutz-Konvention des Europarates auch nach deren vorgesehener Änderung durch das Protokoll. Art. 27 Abs. 1 FsÜ regelt, dass die Vertragsparteien, die Mitglieder der Europäischen Gemeinschaft (nunmehr: der EU) sind, in ihren gegenseitigen Beziehungen Gemeinschaftsvorschriften (nunmehr: Vorschriften der EU) anwenden und daher die sich aus diesem Übereinkommen ergebenden Bestimmungen nur insoweit an, als es zu einem bestimmten Regelungsgegenstand keine Gemeinschaftsvorschrift (nunmehr: Unionsvorschrift) gibt. Letztere Auffangklausel für eine subsidiäre Anwendung des FsÜ im Verhältnis der EU-Mitgliedstaaten zueinander griff bereits bislang unter der Geltung der AVMD-Richtlinie ins Leere und wird nach deren vorgesehener Novelle erst recht gegenstandslos geworden sein.

Aus dem Fehlen einer entsprechenden datenschutzrechtlichen Kollisionsnorm ergibt sich indessen keine praktisch bedeutsame Unsicherheit im Verhältnis der Vertragsparteien der Datenschutz-Konvention zueinander:

- Die Vertragsstaaten, die Mitgliedstaaten der EU sind, sind durch die Konvention auch in einer durch das Protokoll geänderten Fassung völkervertragsrechtlich nicht gehindert, untereinander die DS-GVO anzuwenden.
- Für das Verhältnis von Vertragsparteien der Datenschutz-Konvention, die nicht beide EU-Mitgliedstaaten sind, zueinander, gilt zwar nicht die DS-GVO, sondern die Konvention. Diese hindert wiederum EU-Mitgliedstaaten allerdings nicht daran, auch in einem solchen Verhältnis das Marktortprinzip anzuwenden.

[41] Vgl. Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal , Strasbourg, 25.VI.2018, Tz. 3

VII. Brexit und Datenschutz

Auch in Bezug auf den Datenverkehr zwischen der EU und dem Vereinigten Königreich sind die Auswirkungen des Brexits noch nicht umfassend abschätzbar. Aktuell ist das Vereinigte Königreich als Mitglied der EU zwar an die DS-GVO gebunden. Nach dem Brexit wird die DSGVO im Vereinigten Königreich aber nicht mehr unmittelbar gelten – indessen gemäß Art. 3 DS-GVO weiterhin für im Vereinigten Königreich ansässige Unternehmen rechtlich relevant sein, die Waren oder Dienstleistungen in die EU-27 verkaufen oder erbringen oder das Verhalten betroffener Personen beobachten, soweit ihr Verhalten in der EU erfolgt. Auch nach dem Brexit müssen sich damit z.B. die Datenverarbeitung durch im Vereinigten Königreich ansässige Unternehmen im Zusammenhang mit der Mediennutzung EU-Ansässiger oder die Vorbereitung individualisierter/adressierter/personalisierter Werbung für Bewohner der EU seitens im Vereinigten Königreich ansässiger Unternehmen am Maßstab der DS-GVO messen lassen.

Nach dem Brexit ist es dem Vereinigten Königreich zwar rechtlich möglich, seinen eigenen Datenschutzstandard festzulegen, solange dieser mit den Vorgaben der Art. 8 EMRK in Einklang steht, sofern das Vereinigte Königreich nicht auch aus dem Europarat ausscheidet. In der Praxis dürfte diese datenschutzrechtliche Gestaltungsfreiheit des Vereinigten Königreichs allerdings durch das in der DS-GVO verankerte Verbot der Übertragung personenbezogener Daten aus der EU in Staaten, denen es an einem „angemessenen Schutzniveau" des Datenschutzes mangelt, eingeschränkt sein. Denn EU-Regulierungsbehörden und Gerichte haben zunehmend eine strenge Auslegung des Kriteriums „angemessen" vorgenommen, die im Ergebnis eine wesentliche Gleichwertigkeit des Datenschutzes erfordert.

Das Vereinigte Königreich steht daher vor einer Entscheidung. Es könnte sich entscheiden, insbesondere auch durch eine rasche eigene Ratifikation des Änderungsprotokolls zur Datenschutzkonvention und in der Erwartung von dessen baldigem In-Kraft-Treten auf eine Anerkennung des Datenschutzniveaus als „angemessen" durch die EU-Kommission zu setzen, um eine fortdauernde freie Übertragbarkeit persönlicher Daten aus der EU-27 ins Vereinigte Königreich zu ermöglichen.

Oder das Vereinigte Königreich könnte Gesetze erlassen, die aus berechtigter Sicht der Europäischen Kommission kein angemessenes, dem der EU im Wesentlichen gleichwertiges Datenschutzniveau sicherstellen. Dann wären Unternehmen, die Daten aus der EU-27 nach dem Vereinigten Königreich übertragen wollen, einer kostspieligen Einzelfallprüfung unterworfen, ob z.B. über Verwendung der EU-Standardvertragsklauseln, verbindliche Unternehmensregeln oder eine bilaterale Vereinbarung ein hinreichender Datenschutz bei dem die Daten empfangenden Unternehmen im Vereinigten Königreich besteht.

VIII. Ein kurzer Ausblick

Mit dem Protokoll zur Änderung der Datenschutzkonvention des Europarates wird wie mit der DS-GVO den Herausforderungen, die die Verwendung neuer Informations- und Kommunikationstechnologien für den Schutz der Privatsphäre mit sich bringt, ebenso wie der Aufgabe, Datenschutzrecht auch im Vollzug effektiver zu gestalten, in einer den jeweiligen Spezifika der beiden – miteinander verwobenen - Rechtskreise EU und Europarat angemessenen Weise Rechnung getragen.

Mit dem Änderungsprotokoll erhält die „Konvention 108" dabei ein beachtliches neues Momentum, um dem globalen Orientierungsanspruch der Konvention, der sich in entsprechende Ansätze des Europarates z.B. auch auf dem Feld der Bekämpfung von Cyberkriminalität

einfügt,[42] auch in den 20er Jahren des 21. Jahrhunderts zu genügen. Sie kann eine Brücke in eine sich entwickelnde Weltinnenpolitik[43] bilden, die ungeachtet jüngster Rückschläge durch nationalistische Tendenzen im transatlantischen Raum fortdauernd im Werden sein dürfte und bei der gemeinsame Datenschutzstandards ein unverzichtbarer Baustein eines menschenrechtsorientierten Regulierungsrahmens sind.

42 Die Cybercrime-Konvention des Europarates (SEV Nr. 185) ist inzwischen (Stand: 3. Juni 2018) auch von 14 Nichtmitgliedstaaten des Europarates ratifiziert, darunter u.a. den USA, Kanada, Japan, den Philippinen und Australien sowie weiteren afrikanischen, amerikanischen und asiatischen Staaten; vgl. https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cT9nEUjX.

43 Vgl. hierzu z.B. *Bartosch/Ganszyk* (Hrsg.), Weltinnenpolitik für das 21. Jahrhundert, 3. Aufl. 2009; *Beck*, Nachrichten aus der Weltinnenpolitik, 2010