[et_pb_section bb_built="1"][et_pb_row][et_pb_column type="4_4"][et_pb_text]

Das Datenschutzrecht umfasst nach deutschem und europäischem Verständnis die Rechtsnormen, die den Umgang (im europäischen Rechtskontext ist „Verarbeitung" der Oberbegriff) mit personenbezogenen Daten regeln. In der deutschen Verfassungsordnung findet es seine Grundlage in dem vom Bundesverfassungsgericht im „Volkszählungsurteil" von 1983 entwickelten Grundrecht auf informationelle Selbstbestimmung, das eine spezielle Ausprägung des Allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz) darstellt.

Explizit ist das Grundrecht auf Datenschutz inzwischen in zahlreichen Verfassungen der Länder sowie – auf europäischer Ebene – in der Charta der Grundrechte der EU (Art. 8, neben dem allgemeineren Recht auf Privatleben in Art. 7) enthalten. In der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte ergibt sich der Schutz personenbezogener Daten aus dem Recht auf Privatsphäre (Art. 8 der Europäischen Menschenrechtskonvention).

Die Einzelheiten dieses Grund- und Menschenrechts sind innerhalb der EU mittlerweile vor allem durch die Datenschutzrichtlinie (RL 95/46/EG) geregelt, die im Mai 2018 durch die dann in Kraft tretende Datenschutz-Grundverordnung (EU 2016/679) abgelöst wird. Abgesehen von bestimmten Öffnungsklauseln, die national divergierende Regelungen ermöglichen, gelten die in der DS-GVO aufgestellten Rechte und Pflichten unmittelbar und einheitlich in allen Mitgliedstaaten. Hinsichtlich der Öffnungsklauseln finden das Bundesdatenschutzgesetz und vielfältige spezialgesetzliche Regelungen Anwendung.

Die Verarbeitung personenbezogener Daten ist nach den vorgenannten Regelungen und Entscheidungen grundsätzlich nur zweckgebunden zulässig (sog. Zweckbindungsgrundsatz). Die Wahrung der aufgestellten Grundsätze in den Mitgliedstaaten sollen unabhängige Datenschutzbehörden und die Einführung eines Marktort-Prinzips sicherstellen.

Mit der Reform des Rechtsrahmens für elektronische Kommunikation 2009 wurden weiter durch die Richtlinie 2009/136/EG u. a. Informationspflichten für Dienstanbieter im Falle von Datenlecks und eine Zustimmungspflicht des Betroffenen für die Speicherung von Browser-„Cookies" in die RL 2002/58/EG eingefügt. 2018 sollen diese Bereiche einheitlich von der E-Privacy-Verordnung geregelt werden. Diese stellt eine Lex specialis zur DS-GVO dar und wird sie im Hinblick auf elektronische Kommunikationsdaten, die als personenbezogene Daten einzustufen sind, präzisieren und ergänzen.

Den Ausgleich mit dem Grundrecht auf Meinungsfreiheit stellen Vorschriften zum Datenschutz im Rahmen von journalistisch-redaktionellen Tätigkeiten (sog. Redaktionsdatenschutz) her, die sich für den Rundfunk im Rundfunkstaatsvertrag (RStV) sowie in weiteren Staatsverträgen und Landesmediengesetzen finden. Eine gesetzliche Regulierung für die Presse hat bisher nur rudimentär in den Pressegesetzen einiger Länder stattgefunden; überwiegend wird der Schutz personenbezogener Daten dort durch Mechanismen der freiwilligen Selbstkontrolle, vor allem den Pressekodex des Presserates, sichergestellt. Auf Telemedien finden die speziellen Vorschriften des Telemediengesetzes (TMG) Anwendung.

Mit der DS-GVO wird das Medienprivileg für die Datenverarbeitung in Art. 85 an die Mitgliedsstaaten übertragen. Hiermit werden die Mitgliedstaaten verpflichtet, durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang zu bringen.

Neben dem Datenschutz gewinnt auch die Datensicherheit mit steigendem Digitalisierungsgrad an Bedeutung. Auch wenn die Datensicherheit Schnittmengen zum Datenschutz aufweist, zielt sie zum einen weniger auf die Persönlichkeitsrechte eines Betroffenen, als vielmehr auf wirtschaftliche Interessen und Bedrohungen unmittelbar für Unternehmen, mittelbar für die Gesellschaft ab. Zum anderen ist Schutzziel nicht das Datum des Einzelnen, sondern die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität der IT-Systeme. In der Praxis finden sich vielfältige Regularien und Normierungen, um die Datensicherheit sicherstellen zu können. Dies sind beispielsweise der IT-Grundschutz des BSI oder ISO/IEC-27000.

Auf europäischer Ebene stehen Maßnahmen und Regularien unter dem Banner der European Cybersecurity Strategy (EU-CSS), die 2013 von der Kommission herausgegeben und deren Notwendigkeit vor allem mit der alarmierenden Zunahme von Sicherheitsvorfällen im Cyberraum – ob nun kriminell oder politisch motiviert, terroristisch oder staatlich veranlasst, beabsichtigt oder unbeabsichtigt -, die die Inanspruchnahme solcher Dienste, die für die Bürger selbstverständlich sind, erheblich stören (können) begründet wurde. In der EU-CSS werden allgemeine Ziele und Vorstellungen von einer Cybersicherheitspolitik dargestellt, die sich auf die drei EU-Politikbereiche Digitale Agenda, Inneres und Außen- und Sicherheitspolitik verteilen. Im Fokus steht dabei unter anderem die Widerstandsfähigkeit („resilience“) gegenüber Cyberangriffen, die durch die Richtlinie zur Netz- und Informationssicherheit (NIS-RL) von 2016 im Bereich kritischer Infrastrukturen hergestellt werden soll.

Auf nationaler Ebene tritt die IT-Sicherheit vor allem aus der Nationalen Strategie zum Schutz Kritischer Infrastrukturen, die sich mit Infrastrukturen im Allgemeinen und Kritischen Infrastrukturen im Besonderen als unverzichtbare Lebensadern moderner, leistungsfähiger Gesellschaften befasst, und der Cyber-Sicherheitsstrategie für Deutschland aus dem Jahre 2016, die sich auf den Bereich der Informationstechnik beschränkt, hervor. Aus diesen resultiert schließlich auch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, dessen Regulierungsziel vorrangig die Gewährleistung der Verfügbarkeit und Sicherheit der IT-Systeme insbesondere im Bereich der Kritischen Infrastrukturen durch die bewirkten Änderungen im BSI-Gesetz ist. Allerdings gab es auch Änderungen in anderen Bereichen, wobei vor allem die Änderung des Telemediengesetzes für den Medienbereich eine entscheidende Rolle spielt, da sie die Medien als Anbieter (auch) von Online-Inhalten regelmäßig adressiert.

Für Medienunternehmen, die sich in Bezug auf Cyberattacken in einer potentiellen Gefährdungslage befinden, ist der Rechtsrahmen insoweit relevant, als sie von dem großen Rahmen in Form der Strategien (EU-CSS und KRITIS-Strategie) angesprochen werden. Auf Regulierungsebene (NIS-RL und ITSiG) sind die Medien als solche aber offensichtlich nicht – auch nicht analog – angesprochen. Im interoperativen Bereich, also im Bereich der Zusammenarbeit auf Plattformen sind sie wiederum – mehr oder weniger ausdrücklich – zur Beteiligung und Herstellung von IT-Sicherheit aufgerufen.

[/et_pb_text][et_pb_blog _builder_version=“3.0.64″ show_thumbnail=“on“ show_more=“off“ show_author=“off“ show_date=“on“ show_categories=“off“ show_comments=“off“ show_pagination=“off“ include_categories=“23″ show_content=“off“ offset_number=“0″ use_overlay=“off“ fullwidth=“off“ use_dropshadow=“off“ background_layout=“light“ border_style=“solid“ /][/et_pb_column][/et_pb_row][/et_pb_section]