Datenschutz newsbox

Ausgabe 3 2018

DATAKONTEXT

Editorial

„Wir brauchen endlich eine smarte Datenkultur vor allem für Unternehmen. Tatsächlich existiert in Deutschland aber ein Datenschutz wie im 18. Jahrhundert."
Dieser Satz der designierten Staatsministerin „für Digitales", Dorothee Bär (CSU), sorgte für einige kontroverse Diskussionen, insbesondere auf Twitter.

Und auch der ehemalige BfDI, Peter Schaar, zeigte sich verwundert über ein solches „Datenschutzverständnis" und stellte die Frage in den Raum, wie sich die GroKo -Partner letztlich hinsichtlich des Themas Datenschutz in der Legislaturperiode aufstellen werden.

Die Koalition will laut Vertrag Innovationen und neue Dienste „ermöglichen und gleichzeitig den hohen und weltweit angesehenen Datenschutzstandard Europas und Deutschlands halten".

Wie dieser Spagat gelingen könnte, versucht das „Forum Privatheit" in einem neuen Papier darzustellen.
Das wissenschaftliche Expertengremium hat die Aussagen des Koalitionsvertrags zur geplanten Gestaltung der Digitalisierung untersucht und seine Analyse in einem Policy Paper zusammengefasst: Datenschutz stärken, Innovationen ermöglichen – Wie man den Koalitionsvertrag ausgestalten sollte. Es erläutert, welche Maßnahmen nun folgen müssen, um die Ziele Innovationsförderung und Datenschutz zu verbinden.

Die nächsten Jahre werden zeigen, ob das Thema Datenschutz ein essenzieller Bestandteil einer Digitalstrategie für das 21. Jahrhundert bleiben wird.

Ihr Levent Ferik

Countdown: Weniger als 100 Tage bis zur Anwendung der DS-GVO

Das neue Datenschutzrecht kommt. Jetzt letzte Schritte zur Vorbereitung einleiten.

Nun sind es noch weniger als 100 Tage, bis die DS-GVO flächendeckend bei sämtlichen datenverarbeitenden Stellen Anwendung findet. Den Unternehmen in der EU bleibt daher nicht mehr viel Zeit, ihre Datenschutzorganisation an die neuen Anforderungen der DS-GVO anzupassen.
Dabei setzt die DS-GVO auf ein Datenschutzmanagementsystem, das unabhängig von der Bestellung eines Datenschutzbeauftragten in der eigenen Verantwortung des Unternehmens wirksam sein muss. Jan Philipp Albrecht, MdEP, stellt fest: „Es wird kein Pardon geben."

Rat können sich Verantwortliche mit Hilfe der GDD-Praxishilfen DS-GVO holen. Die mittlerweile vierzehn Ausgaben starke Veröffentlichungsreihe befasst sich z.B. mit den maßgeblichen Themen der DS-GVO-Implementierung.

Zu den neuesten Veröffentlichungen gehören die Praxishilfe VII zu Transparenzpflichten in zweiter Auflage, die Praxishilfe XII zur Auftragsverarbeitung und die Praxishilfe XIV zum spanischen Modell der Datenschutz-Folgenabschätzung. In Kürze erscheint ein weiterer Leitfaden zur Frage der datenschutzrechtlichen Einwilligung.

Quelle: GDD e.V.

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

Digitalen Nachlass regeln

Statistisch gesehen, verstirbt in Deutschland alle drei Minuten ein Facebook-Nutzer, ohne zu entscheiden, was mit geposteten Inhalten, Likes oder seinen hochgeladenen Fotos passieren soll. 57 Prozent der Deutschen nutzen lediglich ihr Gedächtnis, um sich ihre Online-Passwörter zu merken. Bei Flickr (und anderen Social-Media-Anbietern) können Freunde und Familie nicht auf die Fotos von Verstorben zugreifen. Mittlerweile existieren sogar diverse Anbieter auf dem Markt, die für die Hinterbliebenen einen „digitale Nachlassdienst" anbieten.

Hinterbliebene stehen vor vielen Herausforderungen, wenn sie an Vertragsinformationen gelangen müssen und Online-Konten von Verstorbenen verwalten sollen. Ohne Passwörter und Zugangsdaten haben Erben oft keinen Zugriff auf die Online-Konten. Sie können sich nicht um laufende Geschäfte wie Internetauktionen, Abos oder Bestellungen kümmern oder Verträge kündigen. Im schlimmsten Fall entstehen hohe laufende Kosten und finanzielle Schäden. Nur wenige Unternehmen stellen bislang Regeln auf, unter welchen Bedingungen ein Account aufgelöst werden kann und wer darüber entscheiden darf. Manche Regelungen sind zudem rechtlich fragwürdig. Neben der rechtlichen Seite geht es aber auch um einen selbstbestimmten Umgang mit dem eigenen Nachlass, etwa um den Umgang mit Profilen in sozialen Netzwerken.

In diesem Zusammenhang informiert die Verbraucherzentrale NRW über dieses Thema und weist darauf hin, dass es sinnvoll ist, eine Person des Vertrauens mit allen Aufgaben rund ums digitale Erbe zu betrauen. Dabei bewährt sich insbesondere eine Liste mit allen Benutzerkonten und Passwörtern, die an einem sicheren Ort hinterlegt werden sollte. Auch solle der Verbraucher genau festlegen, was mit seinen einzelnen Konten passieren soll. Wie gewünscht handeln könne die ausgewählte Person nur, wenn die Vollmacht „über den Tod hinaus" gilt.

Interessierte können sich auf den Seiten der Verbraucherzentrale NRW nicht nur eine Muster-Vollmacht zum digitalen Nachlass sowie eine Muster-Liste für Internet-Zugangsdaten runterladen, sondern sich auch detaillierter mit dem Thema beschäftigen.

Quelle: Verbraucherzentrale Nordrhein-Westfalen e.V.

DSK veröffentlicht Hinweise zum Verzeichnis von Verarbeitungstätigkeiten

Aus dem Verfahrensverzeichnis bzw. der Verarbeitungsübersicht gemäß der §§ 4e und 4g BDSG/Art. 18, 19 RL 95/46/EG wird künftig das Verzeichnis von Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DS-GVO.
Nach Erwägungsgrund 82 der DS-GVO soll der Verantwortliche „zum Nachweis der Einhaltung dieser Verordnung" das Verzeichnis von Verarbeitungstätigkeiten führen. Weiterhin kann die zuständige Aufsichtsbehörde die Vorlage verlangen, um die betreffenden Stellen hoheitlich zu kontrollieren. Bestehende Verarbeitungsübersichten nach den §§ 4e und 4g BDSG sind eine gute Grundlage für das VVT – müssen aber unter der DS-GVO angepasst werden.
Die Aufsichtsbehörden hatten bereits vor geraumer Zeit ein Kurzpapier zum Thema Verzeichnis von Verarbeitungstätigkeiten veröffentlicht.

Nun hat die sog. Datenschutzkonferenz (DSK) ihre Hinweise veröffentlicht, die sie zum Art. 30 DS-GVO erarbeitet hat. Gleichzeitig betrachten die veröffentlichten Musterverzeichnisse die Thematik jeweils aus der Perspektive des Verantwortlichen (gem. Art. 30 Abs. 1 DS-GVO) und des Auftragsverarbeiters (gem. Art. 30 Abs. 2 DS-GVO).

Downloads unter:

- Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DS-GVO als WinWord-Datei (docx)
- Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DS-GVO als PDF-Datei
- Muster Übersicht von Verarbeitungstätigkeiten Auftragsverarbeiter gem. Artikel 30 Abs. 2 DS-GVO als WinWord-Datei (docx)
- Muster Übersicht von Verarbeitungstätigkeiten Auftragsverarbeiter gem. Artikel 30 Abs. 2 DS-GVO als PDF-Datei

Artikel-29-Datenschutzgruppe veröffentlicht WP 261

Die Artikel-29-Datenschutzgruppe hat ihr Working Paper 261 veröffentlicht. Nach Art. 49 DS-GVO (Ausnahmen für bestimmte Fälle) sollen Datenübermittlungen in Drittländer unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre ausdrückliche Einwilligung erteilt hat, wenn die Übermittlung gelegentlich erfolgt und im Rahmen eines Vertrags oder zur Geltendmachung von Rechtsansprüchen, sei es vor Gericht oder auf dem Verwaltungswege oder in außergerichtlichen Verfahren, wozu auch Verfahren vor Regulierungsbehörden zählen, erforderlich ist.
Relevant wird Art. 49 DS-GVO, wenn weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 DS-GVO vorliegt noch geeignete Garantien nach Artikel 46 DS-GVO, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, auf die eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation gestützt werden könnten.
Im Working Paper 261 wird herausgearbeitet, wie die Ausnahmen des Artikel 49 DS-GVO zu interpretieren und anzuwenden sind. Das Working Paper steht bis zum 26.03.2018 für Kommentierungen offen. Diese können an JUST-ARTICLE29WP-SEC@ec.europa.eu übersendet werden.

Quelle: Artikel-29-Datenschutzgruppe

Verpflichtung auf die Vertraulichkeit nach DS-GVO

Das bisherige Datenschutzrecht sah in § 5 BDSG a.F. eine sog. „Verpflichtung auf das Datengeheimnis“ vor. Eine vergleichbar klare und eindeutige Regelung ist in der DS-GVO nicht mehr enthalten. Insoweit stellt sich datenverarbeitenden Unternehmen die Frage, ob die klassische Verpflichtung auf das Datengeheimnis weiterhin eine Zukunft hat und als "Verpflichtung auf die Vertraulichkeit" fortlebt.

Die GDD hatte sich bereits in ihrer Praxishilfe DS-GVO XI – Verpflichtung auf die Vertraulichkeit dahingehend positioniert, dass eine Verpflichtung auf die Vertraulichkeit auch unter dem Regime der DS-GVO ein probates Mittel sein wird, um unmissverständlich auf die Bedeutung und den Umfang datenschutzrechtlicher Regeln hinzuweisen und Mitarbeitern etwaige Risiken von Gesetzesverstößen vor Augen zu führen.

Auch das BayLDA vertritt die Ansicht, dass eine Belehrung und Verpflichtung der beschäftigten Personen zur Beachtung der datenschutzrechtlichen Anforderungen auch unter Geltung der DS-GVO als organisatorische Maßnahme geboten bleibt, um die Einhaltung des Datenschutzes so weit wie möglich sicherzustellen. Auf Grund der vielen Nachfragen nach einer Hilfestellung habe man nun einen Mustertext mit Erläuterungen für eine solche Belehrung und Verpflichtung von Beschäftigten veröffentlicht, so das BayLDA.
Das entsprechende Dokument ist für Interessierte ebenfalls auf der BayLDA-Homepage bei den Informationsblättern in der Infothek zu finden (www.lda.bayern.de/de/infoblaetter.html).

Ouelle: BayLDA

Hinweise zur datenschutzrechtlichen Einwilligung nach DS-GVO

Die Einwilligung ist einerseits Betroffenenrecht, da sie der betroffenen Person die Möglichkeit gibt, aktiv über die Verarbeitung, ihre Zwecke und näheren Umstände zu bestimmen. Andererseits ist sie aus Sicht des Verantwortlichen ein Erlaubnistatbestand im Sinne von Art. 6 Abs. 1 lit. a DS-GVO. Eine wirksame Einwilligung ist an strenge Voraussetzungen geknüpft, zudem werden gesteigerte Anforderungen an den Nachweis gestellt. Darüber hinaus kann die Einwilligung von der betroffenen Person widerrufen werden.

Die neue Praxishilfe des GDD-AK DS-GVO-Praxis befasst sich u.a. mit Fragen der Wirksamkeitsvoraussetzungen, des Nachweises und der Widerruflichkeit. Daneben werden konkrete Sonderfälle besprochen, wie z.B. der Umgang mit Alteinwilligungen, Werbeeinwilligungen und solchen im Beschäftigungsverhältnis.

Quelle: GDD-Praxishilfe DS-GVO XIII – Einwilligung, Version 1.0, Stand Februar 2018

Das neue Datenschutzrecht – Merkblatt für Zahnärzte

Wenn am 25.05.2018 die neue europäische Datenschutz-Grundverordnung wirksam wird, hat diese natürlich auch Relevanz für Zahnarztpraxen. Die Bundeszahnärztekammer hat die wichtigsten Neuerungen zusammengefasst und informiert in einem neuen Leitfaden über die neuen Vorgaben.

Die Verarbeitung von personenbezogenen Daten in der Zahnarztpraxis ist nur erlaubt mit Einwilligung der betroffenen Person oder aufgrund einer gesetzlichen Erlaubnis. Dieses Prinzip gilt nicht nur für Patientendaten, sondern für alle personenbezogenen Daten.

Auch Beschäftigtendaten und Lieferantendaten sind durch das Datenschutzrecht geschützt. Der Datenschutz ergänzt die zahnärztliche Schweigepflicht, die sich aus dem Berufsrecht und dem Strafrecht ergibt. Schweigepflichtig sind alle Mitarbeiter der Praxis, aber auch Dienstleister, die Kenntnis von Patientendaten erlangen. Nach dem jüngst geänderten § 203 Strafgesetzbuch (StGB) muss der Praxisinhaber jeden Dienstleister zur Geheimhaltung verpflichten.

Quelle: Bundeszahnärztekammer

ICO veröffentlicht Muster für Verzeichnis von Verarbeitungstätigkeiten

Aus dem Verfahrensverzeichnis bzw. der Verarbeitungsübersicht gemäß der §§ 4e und 4g BDSG/Artt. 18, 19 RL 95/46/EG wird künftig das Verzeichnis Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DS-GVO. Nach Erwägungsgrund 82 der DS-GVO soll der Verantwortliche „zum Nachweis der Einhaltung dieser Verordnung" das Verzeichnis von Verarbeitungstätigkeiten führen. Weiterhin kann die zuständige Aufsichtsbehörde die Vorlage verlangen, um die betreffenden Stellen hoheitlich zu kontrollieren. Bestehende Verarbeitungsübersichten nach den §§ 4e und 4g BDSG sind eine gute Grundlage für das VVT, müssen aber unter der DS-GVO angepasst werden.

In der Regel müssen alle Verantwortlichen (Unternehmen/Legaleinheiten/Behörden etc.) ein VVT führen. Gem. Art. 30 Abs. 5 DS-GVO ist diese Pflicht zwar beschränkt auf Unternehmen

- mit einer Größe ab 250 Mitarbeitern; oder
- mit einem besonderem Risiko bei der Verarbeitung; oder
- mit Verarbeitung von sensiblen Daten (Artt. 9 und 10 DS-GVO); oder
- einer nicht nur gelegentlichen Verarbeitung.

Der Information Commissioner (IC) ist der Datenschutzbeauftragte des Vereinigten Königreichs und leitet die britische Datenschutzbehörde, das Information Commissioner's Office (CIO). Der ICO hat nun auf seiner Seite eine umfangreiche Materialsammlung zum Thema Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO online gestellt. Es werden zwei Muster zur Dokumentation angeboten:
Das erste Muster betrachtet die Verarbeitungen aus der Perspektive der für die Verarbeitung Verantwortlichen gem. Art. 30 Abs. 1 DS-GVO.
Das zwei Muster richtet sich hingegen speziell an Auftragsverarbeiter und bemisst sich an Art. 30 Abs. 2 DS-GVO.

Quelle: The Information Commissioner`s Office (ICO)

DS-GVO: Umsetzungsbedarf für die Rechtsanwaltskanzlei

Auch der Deutsche Anwaltverein (DAV) stellt seinen Mitgliedern und auch allen anderen Interessierten hilfreiche Informationen und Muster für die Umsetzung der DS-GVO zur Verfügung.
Unter den angebotenen Materialien befinden sich das sog. DAV-Merkblatt zur DS-GVO, Hinweise zur Datenverarbeitung in der Kanzlei (zur Übergabe bei Mandatsbeginn) sowie eine Muster-Datenschutzerklärung für die Kanzlei-Webseite.

Abgerundet werden die Informationen um eine beispielhafte Zusammenstellung von technisch-organisatorischen Maßnahmen zur Datensicherheit, welche zur Dokumentation und zur Vorlage bei eventuellen Überprüfungen genutzt werden können.

Mit dabei ist auch ein Musterverzeichnis der Verarbeitungstätigkeiten im Excel-Format.

Quelle: Deutscher Anwaltverein

Kompass zur IT-Verschlüsselung

Eine Studie im Auftrag des BMWi, die am 26.02.2018 im BMWi vorgestellt wurde, kommt zu dem Ergebnis, dass insbesondere bei den kleinen und mittleren Unternehmen (KMU) noch großer Nachholbedarf herrscht, was das Thema Verschlüsselung angeht. Während Großunternehmen zu über 90 Prozent Verschlüsselungslösungen einsetzen, sei dies lediglich bei rund drei Viertel der KMU der Fall. Dabei ist der Einsatz von Verschlüsselungslösungen, zum Beispiel für E-Mails und Datenträger, ein wichtiger Faktor, um die IT-Sicherheit von Unternehmen zu erhöhen und Gefahren durch Angriffe zu minimieren.

Bundeswirtschaftsministerin Brigitte Zypries: „Informationen in einer unverschlüsselten E-Mail sind etwa genauso schlecht geschützt, als würde man sie auf einer Postkarte versenden. Die Notwendigkeit für elektronische Verschlüsselung wird zwar oftmals erkannt, die Umsetzung scheitert jedoch an dem scheinbar hohen Aufwand und der umständlichen Bedienung im Alltag. Deshalb haben wir die tieferliegenden Hemmnisse beim Einsatz von Verschlüsselung in einer Studie untersuchen lassen und in einem ersten Schritt einen Kompass zur IT-Verschlüsselung als Orientierungshilfe für Unternehmen erstellt. Denn es wird immer wichtiger, dass Unternehmen ihr geistiges Eigentum sowie Unternehmens- und Kundendaten vor den immer professionelleren Hackerangriffen schützen. Wir wollen sie dabei unterstützen."

Mit dem Kompass zur IT-Verschlüsselung können KMU herausfinden, an welchen Stellen eine Verschlüsselung sinnvoll ist und welche Verschlüsselungsmöglichkeiten zur Verfügung stehen. Anhand von Leitfragen hilft der Kompass außerdem bei der Entscheidungsfindung, welche Lösungen im eigenen Unternehmen zum Einsatz kommen sollen. Ein Glossar erklärt die zentralen Begriffe und Abkürzungen.

Der Kompass zur IT-Verschlüsselung wurde im Rahmen der Studie Einsatz von elektronischer Verschlüsselung – Hemmnisse für die Wirtschaft von den Projektpartnern Goldmedia GmbH, if(is) – Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen und IRNIK – Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) erstellt.

Die Ergebnisse der Studie können hier (PDF, 780KB) abgerufen werden. Den Kompass zur IT-Verschlüsselung finden Sie hier (PDF, 2MB).

Quelle: Bundesministerium für Wirtschaft und Energie

Ist Google ein Telekommunikationsdienst? – EuGH soll entscheiden

Der EuGH soll klären, ob E-Mail-Dienste, die über das offene Internet erbracht werden, ohne den Kunden selbst einen Internetzugang zu vermitteln (sog. Webmail-Dienste), Telekommunikationsdienste sind und damit den entsprechenden gesetzlichen Verpflichtungen unterliegen. Dies hat das Oberverwaltungsgericht am 26.02.2018 auf eine Klage des US-amerikanischen Unternehmens Google hin in einem Musterprozess entschieden.
Dem Verfahren liegt ein bereits seit mehreren Jahren geführter Rechtsstreit zwischen der für die Aufsicht über den Telekommunikationsmarkt in Deutschland zuständigen Bundesnetzagentur mit Sitz in Bonn und Google zugrunde. Die Behörde ist der Ansicht, dass der von Google betriebene E-Mail-Dienst Gmail (früher: Google Mail) ein Telekommunikationsdienst im Sinne des deutschen Telekommunikationsgesetzes ist und Google daher den dort für Anbieter von solchen Diensten geregelten Pflichten unterliegt, zum Beispiel Anforderungen des Datenschutzes oder der öffentlichen Sicherheit. Mit Bescheiden aus Juli 2012 und Dezember 2014 hatte die Bundesnetzagentur Google verpflichtet, Gmail bei ihr als Telekommunikationsdienst anzumelden. Dagegen klagte Google erfolglos vor dem Verwaltungsgericht Köln und legte anschließend Berufung ein.

Nach der zwischen den Beteiligten im Streit stehenden gesetzlichen Definition im Telekommunikationsgesetz sind Telekommunikationsdienste in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Google ist der Auffassung, dass diese Bestimmung für Webmail-Dienste wie Gmail nicht einschlägig ist, weil sie sich das Internet als bestehendes Telekommunikationsnetz zu Eigen machen, ohne es selbst zu betreiben, den Nutzern den Zugang hierzu zu vermitteln oder die Datenübertragung auf sonstige Weise zu kontrollieren. Außerdem würden Webmail-Dienste wie Gmail für die Nutzer vielfach kostenlos erbracht.

Der 13. Senat hat das Berufungsverfahren nun ausgesetzt und den EuGH um Vor-abentscheidung ersucht. Da die gesetzliche Definition im Telekommunikationsgesetz auf eine annähernd gleichlautende Bestimmung in der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste zurückgehe, komme es für den Senat bei seiner Entscheidung über die Berufung maßgeblich auf die Vorgaben des europäischen Rechts an. Der EuGH müsse klären, ob auch internetbasierte E-Mail-Dienste, die über das offene Internet bereitgestellt würden und selbst keinen Inter¬netzugang vermittelten, als Übertragung von Signalen über elektronische Kommunikationsnetze von der Richtlinie erfasst würden. Ferner müsse die Frage beantwortet werden, wie das Merkmal „gewöhnlich gegen Entgelt erbracht“ auszulegen sei.

Beschluss des OVG Münster: Aktenzeichen 13 A 17/16 (I. Instanz: VG Köln 21 K 450/15)

Skript Internetrecht – Stand März 2018

Alle (halbe) Jahre wieder: Die neue Fassung des bekannten und bewährten Skripts „Internetrecht" des Münsteraner Jura-Professors Dr. Thomas Hoeren wurde von ihm und seinem ITM-Team auf den Stand März 2018 gebracht und steht ab sofort auf der Website des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster zum Download als PDF-Datei bereit. Das E-Book umfasst 600 Seiten. Rechtsprechung und Literatur wurden in der neuesten Auflage aktualisiert. Kapitel 6 des Skripts befasst sich ausschließlich mit der DS-GVO, die ab dem 25.05.2018 wirksam werden wird. Das Skript geht insbesondere auf diese Themen ein:

- Die Datenschutzgrundverordnung (DS-GVO) – ein erster Überblick
- Anwendbarkeit
- Zweckbindungsgrundsatz
- Einwilligung
- Minderjährigenschutz
- Recht auf Löschung („Recht auf Vergessenwerden")
- Recht auf Datenportabilität
- Profiling und Scoring
- Auftragsdatenverarbeitung
- Drittstaaten
- Datenschutzbeauftragter
- Bußgelder
- Verarbeitung i. R. v. Arbeitsverhältnissen

Quelle: Institut für Informations-, Telekommunikations- und Medienrecht/Uni Münster