DataAgenda-Arbeitspapier 53, 10/2023

DataAgenda - das Informationsportal zum Datenschutzrecht

Präsentiert von DATAKONTEXT

www.DataAgenda.de

@dataagenda

Datenschutzrechtliche Rahmenbedingungen für eine gemeinwohlorientierte Datennutzung

I. Einleitung

In den letzten Jahren hat die Bedeutung von Daten und Informationen immer weiter zugenommen, insbesondere durch die verstärkten Diskussionen zur Verfügbarkeit von Gesundheitsdaten im Zusammenhang mit der globalen Corona-Pandemie. Die Frage nach der Verfügbarkeit und dem Zugang zu Daten verdeutlicht eindrucksvoll, dass Datennutzung genauso wie Datenschutz nicht mehr nur eine rechtliche oder technische Frage ist, sondern gleichermaßen auch ein gesellschaftspolitisches Thema geworden ist.

Die Europäische Union (EU) hat in diesem Zusammenhang ehrgeizige Ziele in der Digitalpolitik formuliert und strebt an, „Europa zum Daten-Kontinent Nummer eins auf der Welt zu machen“[1]. Dabei spielt der Data Governance Act eine Schlüsselrolle, indem er einen Rahmen schafft, der die gemeinsame Nutzung von Daten erleichtert und Grundlagen für ein europäisches Datenaustauschmodells normiert.

Jede gemeinwohlorientierte Datennutzung bewegt sich innerhalb datenschutzrechtlicher Rahmenbedingungen, die maßgeblich von der Datenschutz-Grundverordnung (DS-GVO) bestimmt werden und von nationalen Einzelvorschriften ergänzt werden. Im Folgenden werden die Chancen und Herausforderungen und mithin die datenschutzrechtlichen Anforderungen an das Datenteilen ausführlich diskutiert.

II. Die Digitalpolitik der EU

Die EU verfolgt entschlossen ihre Vision, im globalen Datenraum eine Führungsposition einzunehmen. Europäischen Unternehmen soll der Zugang zu Daten erleichtert und eine Europäischer Gesundheitsdatenraum soll neu geschaffen werden. Der Data Governance Act stellt eine strategische Weichenstellung dar, um diesen ehrgeizigen Zielen gerecht zu werden. Er legt nicht nur die rechtlichen Grundlagen für den Umgang mit Daten fest, sondern betont auch die grundlegende Bedeutung von Vertrauen und Grundrechtschutz im Zusammenhang mit Daten. Hierbei ist insbesondere dem auch in der Grundrechte-Charta (GR-Charta) der EU verankerten Schutz personenbezogener Daten Rechnung zu tragen.

1 SZ, EU vereinfacht den Datenaustausch, 1.12.2021, https://www.sueddeutsche.de/wirtschaft/data-governance-eu-datentreuhaender-niebel-breton-1.5477968#:~:text=Binnenmarkt%2DKommissar%20Thierry%20Breton%20sagt,auf%20der%20Welt%20zu%20machen%22.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

III. Die Digitalpolitik der Bundesrepublik Deutschland

Ende des Jahres 2019 hat die Bundesregierung Eckpunkte einer Datenstrategie beschlossen.[2] Danach sind eine verantwortungsvolle Datennutzung sowie das Recht auf Schutz personenbezogener Daten kein Widerspruch, sondern zwei Seiten derselben Medaille. In Anerkennung dessen will die Bundesregierung Datennutzung und Datenschutz gleichermaßen wahren, um so die Chancen der Digitalisierung zu realisieren, dabei aber gleichzeitig ihre Risiken adressieren und berücksichtigen. Die Datenstrategie soll deswegen auch im Handlungsfeld „Datenbereitstellung verbessern und Datenzugang sichern" entwickelt werden:

Um Gesellschaft, Wirtschaft und Wissenschaft einen chancenorientierten, verantwortungsvollen und barrierefreien Zugang zu Daten zu ermöglichen, muss die Bereitstellung von Daten verbessert und dazu die langfristige Verfügbarkeit von Daten technisch und rechtlich sichergestellt werden.

Dazu werden wir unter Beachtung der datenschutzrechtlichen Regelungen unter anderem:

- *Den Aufbau wettbewerbsfähiger und nachhaltiger Dateninfrastrukturen und - ökosysteme unterstützen.*
- *Die rechtlichen Rahmenbedingungen für die Bereitstellung von hochwertigen Daten klären und, u.a. Fragen der rechtlichen Anforderungen an die Anonymisierung und der Rolle von Intermediären überprüfen.*
- *Analysieren, welche Anreize für Unternehmen (insbesondere für den Mittelstand) und zivilgesellschaftliche Akteure und gemeinnützige Träger gesetzt, welche Voraussetzungen geschaffen werden müssen und welchen Beitrag vertrauenswürdige Datenräume und Strukturen von Datentreuhändern leisten können, um das freiwillige Teilen von Daten zu verstärken.*
- *Die Forschung befördern, unter anderem um die Entwicklung der nötigen Technologien und deren Transfer in die Anwendung zu gewährleisten. Dazu gehören auch neue und sichere Methoden zur Anonymisierung und Pseudonymisierung sowie zur praxistauglichen Datenportabilität.*
- *Herausarbeiten, welche weiteren unterstützenden Maßnahmen, Einrichtungen oder Werkzeuge auf infrastruktureller, institutioneller, rechtlicher und technischer Ebene in Deutschland und Europa notwendig sind.*
- *Prüfen, ob ein Anreizsystem zur Förderung genossenschaftlicher oder gemeinwohlorientierter Datennutzung geschaffen werden sollte und - wenn ja, wie der Zugang zu Daten entsprechend sichergestellt werden kann.*[3]

IV. Die Notwendigkeit neuer Datenteilungsmodelle

Inmitten der Bemühungen der Bundesregierung und der Europäischen Kommission, datenpolitische Strategien zu entwickeln, bleibt eine zentrale Frage bislang weitgehend ungelöst: Wie kann die Konfiguration des Datenaustauschs und des Datenzugangs gestaltet werden, um den größtmöglichen Nutzen für eine breite Palette von Akteuren zu gewährleisten? Dieses Ansinnen in Bezug auf Datenzugang und Datenteilung erweisen sich insbesondere im Zusammenhang mit dem Einsatz von „Künstlicher Intelligenz" als zunehmend bedeutsam und dringlich. Die Quantität und Qualität der verfügbaren Daten sind von entscheidender Bedeutung für die Leistungsfähigkeit eines algorithmischen Systems, was die Grundlage Künstlicher Intelligenz darstellt. Ebenso stark fließen diese Faktoren auf die Fähigkeit zur Bereitstellung nützlicher Analysen, die effektive Unterstützung von Entscheidungsprozessen sowie die Genauigkeit der Vorhersagen unter Zuhilfenahme Künstlicher Intelligenz. Die Qualität und Verfügbarkeit von Daten sind entscheidend für die Leistungsfähigkeit dieser Anwendungen. Daher ist es von grundlegender Bedeutung, neue Modelle für die Datenteilung zu entwickeln und zu erproben, um das volle Potenzial von Daten auszuschöpfen.

2 Bundesregierung, Eckpunkte einer Datenstrategie der Bundesregierung, 18.12.2019, Drs. 19/16075.
3 Ebd., 3.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

V. Chancen und Risiken des Datenteilens

Obwohl auf der gesamten Welt immer riesigere Datenmengen generiert werden, bleibt ein Großteil dieser Daten ungenutzt. Solange diese Daten nicht aktiv genutzt werden, bleiben auch das damit verbundene Potenzial, Daten zum Wohl der Gesellschaft einzusetzen, ungenutzt. Daten werden oft metaphorisch als das „Gold“ oder „Öl“ des 21. Jahrhunderts bezeichnet, doch ihr Wert sollte über ökonomische Interessen hinaus betrachtet werden. Das Teilen von Daten birgt zweifellos auch Risiken. Dabei sind der Datenschutz und das Vertrauen derjenigen, deren Daten geteilt werden, von entscheidender Bedeutung. Gleichzeitig bedarf es einer gesellschaftlichen Debatte über den vermehrten Datenzugang und die dafür verwendeten Modelle müssen weiterentwickelt und erprobt werden.

1. Datenschutzrechtliche Anforderungen

a) Rechtsgrundlage

Die zentralen Risiken und Herausforderungen bei der Bereitstellung von Daten für das Gemeinwohl sind insbesondere in den datenschutzrechtlichen Anforderungen sowie der Frage nach dem sicheren Umgang mit personenbezogenen Daten (Daten- und Informationssicherheit). Bei der Teilung personenbezogener Daten besteht grundsätzlich eine Gefahr für den grundrechtlichen Schutz der Datensubjekte (Nutzer bzw. Datenbereitsteller). Soweit der supranationale Gesetzgeber die DS-GVO nicht aufweichen möchte, ist die Beachtung der in Art. 5 DSGVO verankerten Grundprinzipien elementar.

Hiernach bedarf jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage (Art. 5 Abs. 1 lit. a, 6, 9 DS-GVO). Der Dateninhaber, der Daten zum Zwecke des Gemeinwohls teilen möchte, könnte sich für diese Übermittlung der Daten auf Art. 6 Abs. 1 lit. c DS-GVO berufen, aber nur sofern der Gesetzgeber eine solche Möglichkeit normenklar schafft. Sofern jedoch besondere Kategorien von Daten verarbeitet werden, müsste überdies eine Ausnahmeregelung nach Art. 9 Abs. 2 DS-GVO greifen und für den jeweiligen Zweck Garantien getroffen werden, die mit der korrekten Ausnahmeregelung in Art. 9 Abs. 2 DS-GVO korrespondieren. Der weitere Verantwortliche, der an dem Gemeinwohl teilhaben will und die personenbezogenen Daten verarbeiten will, muss ebenfalls eine Rechtsgrundlage nach Art. 6 DS-GVO vorweisen können.

Weiter sind im Zusammenhang mit Zugriffsberechtigungen die Grundsätze der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) und der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) von besonderer Bedeutung. Diesen Grundsätzen Rechnung zu tragen erscheint mindestens ambitioniert, solange das Gemeinwohl nicht als hinreichender Zwecke anerkannt wird. So gilt beispielsweise für die Verarbeitung für Zwecke der wissenschaftlichen Forschung, dass eine pauschale Bezugnahme auf Forschungszwecke nicht den Anforderungen an eine vom Gesetzgeber verlangte, eindeutige Zweckbestimmung genügt.[4] Diese rechtliche Bewertung erscheint auch für den Zweck des Gemeinwohls denkbar, wenn nicht sogar wahrscheinlich. Im Falle einer tatsächlichen Weiterarbeitung zu anderen Zwecken blieben die gesetzlichen Anforderungen des Art. 6 Abs. 4 DS-GVO zu erfüllen, was einer Einzelfallbetrachtung Bestand halten muss. Hierbei können Parameter wie die Verarbeitung personenbezogener Daten in großem Umfang oder die Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 DS-GVO (z.B. Gesundheitsdaten) diese Rechtsgrundlage als hinfällig und damit als nicht anwendbar erscheinen lassen.

4 Ehmann/Selmayr-*Heberlein*, DS-GVO, Art. 6, 2. Aufl. 2018, Rn. 9.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

b) Betroffenenrechte

An prominenter Stelle formuliert die EU innerhalb der Grundrechte-Charta mit dem Recht auf Auskunft[5] die Betroffenenrechte und kodifiziert sie zusätzlich sekundärrechtlich sehr umfänglich innerhalb der DS-GVO. Gerade in dem Zusammenspiel von mehreren Akteuren, die Zugriff auf die geteilten personenbezogenen Daten haben, ist Transparenz für betroffene Personen die basale Voraussetzung dafür, um überhaupt ihre Rechte ausüben zu können.

Maßgeblich wird in diesem Zusammenhang die Frage sein, ob im Zusammenhang mit der sekundären Nutzung betroffenen Personen eine Art Widerspruchsrecht (Opt-out) zugesprochen wird.

c) Pseudonymisierung als Schutzmaßnahme

Allein im Falle der Verarbeitung anonymisierter Daten ist der Anwendungsbereich des Datenschutzrechts nicht eröffnet. Wann aber der Personenbezug tatsächlich beseitigt ist und auch unter Zuhilfenahme vertretbarer technischer Mittel nicht wiederhergestellt werden kann, sodass von einer Anonymisierung gesprochen werden kann, ist bislang nicht gesetzlich geklärt. Es fehlen Standards zur Anonymisierung genauso wie zur Pseudonymisierung, wann Daten tatsächlich als anonymisiert bzw. pseudonymisiert gelten. Für pseudonymisierte Daten ist das Datenschutzrecht ohne jede Beschränkung weiter voll und ganz einzuhalten.[6] In Anbetracht der identifizierten Problembereiche forciert die Datenstrategie der EU die Schaffung entsprechender Voraussetzungen. Dies wird sie durch Normung, die Entwicklung von Instrumenten, das Sammeln bewährter Verfahren beim Umgang mit personenbezogenen Daten, insbesondere im Zusammenhang mit der Pseudonymisierung und den Ausbau von Datenverarbeitungsinfrastrukturen der nächsten Generation erreichen.[7] Dadurch soll u.a. auch eine Grundlage geschaffen werden, „damit Ökosysteme für Datenweitergabe und künstliche Intelligenz florieren können“.

Die angesprochene Pseudonymisierung birgt ein beträchtliches Potenzial Daten durch entsprechende Verfahren von ihrem Personenbezug zu befreien, um sie weiter datenschutz-konform nutzen zu können. Die Pseudonymisierung personenbezogener Daten schafft eine Möglichkeit, zwischen den entgegenstehenden Interessen von Betroffenen und Datenverarbeitern

zu vermitteln und Szenarien zu gestalten, bei denen eine Verwendung von Klardaten nicht mehr erforderlich ist. Unter Zuhilfenahme dieser Maßnahme ließe sich die Nutzung vorhandener Datenmengen für das Gemeinwohl weiter rechtlich zulässig ausgestalten.[8] Ebenso trägt diese Maßnahme sehr stark zur Akzeptanz aller betroffenen Personen bei, deren Daten dem Allgemeinwohl zur Verfügung gestellt werden sollen.

5 Art. 8 Abs. 2 Satz 2 GR-Charta.
6 EG. 26 DS-GVO.
7 Europäische Kommission, Eine europäische Datenstrategie, 19.2.2020, COM(2020) 66 final. So auch Datenethikkommission, Gutachten der Datenethikkommission der Bundesregierung, 2019, 4, 125, 129 f. Ausführlich hierzu auch: Schwartmann/Jaspers/Lepperhoff/Weiß, Praxisleitfaden zum Anonymisieren personenbezogener Daten, 2022.
8 Die praktische Umsetzung der Pseudonymisierung wird ausführlich behandelt in: Schwartmann/Weiß, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der DS-GVO, 2017.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

d) Pseudonymisierung schafft Vertrauen

Pseudonyme Daten schaffen aber auch Vertrauen, indem in möglichst transparenter Weise mithilfe technischer Aufwände eine „Codierung“ von persönlichen Informationen zugunsten vom Betroffenen erfolgt und er hierdurch das Interesse eines Verantwortlichen am Schutz dieser Daten erkennen kann. Dies ist ein maßgebliche Voraussetzung, da jede Form des Teilens von Daten – auch wenn diese aggregiert, anonymisiert oder pseudonymisiert wurden – ein gewisses Maß an Vertrauen derjenigen voraussetzt, deren Daten geteilt werden. Selbst eine umfassende Anonymisierung der Daten kann einen vollständigen Datenschutz keineswegs garantieren. Zudem ist es für Unternehmen fraglich, ob durch das Teilen der von ihnen gesammelten Daten ein wirtschaftlicher Nutzen für sie entsteht. Langfristig könnte dies zur Folge haben, dass weniger Daten gesammelt werden und schlussendlich so auch weniger Daten geteilt werden könnten.

VI. Konzept einer Datenteilungspflicht

Ein Konzept der Datenteilungspflicht wird zwar vereinzelt, wie zum Beispiel im Energiesektor in Großbritannien, bereits angewandt. Die Umsetzung einer allgemeinen Pflicht zur Datenbereitstellung durch öffentliche und private Stellen wäre jedoch ein Novum. Bei der Datenteilungspflicht würden alle oder ausgewählte Unternehmen, wie z.B. die, die einen datengetriebenen Markt beherrschen, dazu verpflichtet, einen Teil der von ihnen generierten oder verwalteten Daten Dritten zur Verfügung zu stellen. Potenzielle Nutzer könnten dann sowohl andere Firmen, die auf dem jeweiligen datengetriebenen Markt aktiv sind, aber auch öffentliche Stellen und zivilgesellschaftliche Organisationen sein. Die Befürworter einer Datenteilungspflicht streben in erster Linie die Schaffung von mehr Wettbewerb auf jenen digitalen Märkten an, die bislang von einigen wenigen Akteuren dominiert werden. Über das Teilen von Daten als zentraler Baustein für digitale Innovationen soll allen die Möglichkeit gegeben werden, am Marktgeschehen teilzunehmen. Wie die Weitergabe der Daten genau ablaufen könnte, welche Daten infrage kommen und welche Märkte als datengetrieben gelten, ist noch weitgehend unklar.

VII. Offene Daten

Als Open Data (Offene Daten), werden Daten bezeichnet, die nahezu ohne Einschränkungen von jedem genutzt und weiterverbreitet werden dürfen. Das Modell findet überwiegend Anwendung bei staatlichen Daten, um Transparenz, Innovation und Teilhabe zu fördern. Das liegt auch daran, dass sich dieses Modell zur Datenteilung grundsätzlich nur dann anbietet, wenn durch die öffentliche Bereitstellung weder der Datenschutz noch Geschäftsgeheimnisse oder andere sensible Informationen bedroht sind, da die Daten für alle zugänglich auf Online-Portalen o.Ä. bereitgestellt werden sollen. Aufgrund der offenen Gestaltung des Datenzugangs kann grundsätzlich jeder von der Datennutzung auf unterschiedliche Art und Weise profitieren, soweit die notwendige Infrastruktur geschaffen ist und entsprechende Expertise besteht. Auch die Datenbereitsteller haben einen Nutzen, indem sie zum Beispiel von den Nutzern der Daten Rückmeldungen zu fehlerhaften Datensätzen erhalten.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

VIII. Datentreuhänder

Datentreuhänder erhalten in aktuellen Debatten viel Aufmerksamkeit und werden unter anderem von der EU als Modell zur gerechten, fairen und sicheren Teilung personenbezogener Daten gesehen. Ob und inwiefern diese Erwartungen erfüllt werden, bleibt aufgrund fehlender Umsetzungserfahrung abzuwarten.

In Anlehnung an das rechtliche Konstrukt eines Treuhandverhältnisses übertragen die Mitglieder im Modell der Datentreuhänder die Entscheidung über Datenzugang- und Nutzungsrechte an einen oder mehrere Treuhänder. Es existiert bislang keine feststehende Definition für Datentreuhänder. Ähnlich wie im Fall von Data Commons und Datenkooperativen ist nicht festgelegt, wie Zugang und Nutzung der Daten technisch konkret ablaufen. Der Fokus liegt vielmehr auf der Idee, dass über eine treuhänderische Verwaltung der Daten, die einzelnen Mitglieder bei Fragen von Datenweitergabe an und -nutzung durch Dritte entlastet werden.

IX. Fazit

Neben bewährten technischen Schwierigkeiten bestehen die Herausforderungen beim Datenteilen insbesondere im Schutz personenbezogener Daten sowie in mangelndem Vertrauen bei denen, deren Daten gesammelt und (weiter) verarbeitet werden. Der faire Datenzugang für das Gemeinwohl führt zu Wettbewerb, Vergleichbarkeit, Transparenz und Qualität und damit letztendlich zum Nutzen für Alle. All das hängt nicht zuletzt auch davon ab, wer Daten sammelt, mit wem sie geteilt werden, welche Ziele bei der Datennutzung verfolgt und wie die enormen Mengen von Daten bei der Entwicklung algorithmischer Systeme genutzt werden. Die Bereitstellung von Daten für das Gemeinwohl in Form einer Datenteilung ist eine zutiefst gesellschaftspolitische Frage. Datenteilungsmodelle können dazu beitragen, den gesellschaftlichen Nutzen von Daten zu maximieren und dabei den Datenschutz zu wahren. Um die Potenziale von Daten für die Gemeinschaft voll auszuschöpfen und die Herausforderungen des Datenschutzes erfolgreich zu bewältigen, bedarf es jedoch klarer rechtlicher Vorgaben als Ergänzung und Konkretisierung des bestehenden datenschutzrechtlichen Rahmen sowie spezifizierender Vorgaben, wie insbesondere in Form von Standards für die Pseudonymisierung.

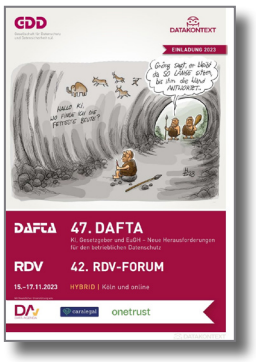
DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Seminartipp zum Arbeitspapier

47. DAFTA + 42. RDV-Forum

Die Debatte um GPT-Anwendungen ist in den Unternehmen angekommen. Aktuell wird der Einsatz Künstlicher Intelligenz (KI) auf der EU-Ebene im Trilog zwischen Parlament, Kommission und Mitgliedstaaten verhandelt. Das Ergebnis soll noch in diesem Jahr vorliegen. Im Unternehmensalltag sind Chatbots & Co. allerdings schon jetzt angekommen. Sie werden insbesondere auch unter Verarbeitung von Kundendaten eingesetzt. Das ruft Verbraucher- und Datenschützer auf den Plan, denn die Anforderungen der DS-GVO müssen jetzt und künftig ungeachtet der entstehenden KI-Regularien eingehalten werden. Offen sind Fragen auf allen Ebenen der DS-GVO, vom Anwendungsbereich, über die Zulässigkeit der Datenverarbeitung bis hin zu den Dokumentations- und Transparenzpflichten, der automatisierten Entscheidung und der Datenschutz-Folgenabschätzung.

Weitere Infos finden Sie hier.



DataAgenda
ist das Informationsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps rund um den Datenschutz.

Datakontext
ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.

Autoren

Prof. Dr. Rolf Schwartmann
Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V (GDD), Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln) und Mitglied der Datenethikkommission.

Dr. Tobias Jacquemain, LL.M. (GDD e.V.)
Promotion zum Schadensersatz für Datenschutzverstöße nach Art. 82 DS-GVO und Lehrbeauftragter an der Universität zu Köln, an der Technischen Hochschule (TH) Köln sowie an der TH Georg Agricola in Bochum.