forum
<privatheit>
selbstbestimmtes_leben_
in_der_digitalen_welt

Interdisziplinäre Konferenz

„Die Fortentwicklung des Datenschutzes“

am 02. und 03. November 2017

in Berlin

Programm

Veranstalter
Forum Privatheit

Kontakt
Michael Friedewald
Geschäftsfeldleiter Informations-
und Kommunikationstechniken
Telefon +49 721 6809–146
Fax +49 721 6809–315
info@forum-privatheit.de

Veranstaltungsort
Tagungswerk
Lindenstr. 85
10969 Berlin

Weitere Informationen auf:
www.forum-privatheit.de

Interdisziplinäre Konferenz

„Die Fortentwicklung des Datenschutzes“

02. und 03. November 2017

Tagungswerk | Lindenstr. 85 | 10969 Berlin

Inhalt

„Forum Privatheit“ – Selbstbestimmtes Leben in der digitalen Welt

Im Zuge der fortschreitenden Digitalisierung fast aller Lebensbereiche werden Fragen zu Privatheit immer wichtiger und drängender. Die Suche nach einem adäquaten und modernen Datenschutz, der Grundrechte wie die informationelle Selbstbestimmung bewahrt und dabei gleichzeitig auch die der Digitalisierung innewohnenden Chancen fördert, ist eine Herausforderung, der sich der Forschungsverbund „Forum Privatheit“ seit 2014 stellt.

Das vom Bundesministerium für Bildung und Forschung geförderte „Forum Privatheit“ bündelt die Expertise von sieben Institutionen aus Wissenschaft und Praxis:

- Universität Kassel/Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG)
  Prof. Dr. Alexander Roßnagel, Recht; Prof. Dr. Jörn Lamla, Soziologie
- Eberhard Karls Universität Tübingen/Internationales Zentrum für Ethik in den Wissenschaften (IZEW)
  Prof. Dr. Regina Ammicht Quinn; PD Dr. Jessica Heesen, Philosophie
- Universität Duisburg-Essen
  Prof. Dr. Nicole Krämer, Psychologie
- Fraunhofer-Institut für System- und Innovationsforschung ISI
  Dr. Michael Friedewald, Technikfolgenabschätzung
- Fraunhofer-Institut für Sichere Informationstechnologie SIT
  Prof. Dr. Michael Waidner, Informatik
- Ludwig-Maximilians-Universität München
  Prof. Dr. Thomas Hess, Wirtschaftsinformatik
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
  Marit Hansen, Datenschutz

Das „Forum Privatheit“

» betrachtet die Fragen zu Privatheit und Datenschutz aus einer interdisziplinären Sicht und erarbeitet Lösungsvorschläge auf einer wissenschaftlich fundierten Basis. Dies ermöglicht einen sachlichen, auf Fakten beruhenden Dialog zwischen Forschung, Politik, Wirtschaft und Gesellschaft.

» stellt praxisorientierte Publikationen wie White Paper und Policy Paper bereit, die Gestaltern aus Politik, Wirtschaft und Zivilgesellschaft als Entscheidungs-, Handlungs- und Diskussionsgrundlage dienen.

» entwickelt Stellungnahmen und Positionen, die angesichts der komplexen Thematik von Technikentwicklung, Techniknutzung, Privatheit und Datenschutz Orientierung bieten.

» sieht sich als Plattform, die durch Veranstaltungen wie Diskussionsrunden, Tagungen und Workshops zu aktuellen Themen Stellung nimmt und Vorschläge für eine praxisgerechte Datenschutzpolitik entwickelt.

» ist eine wichtige Schnittstelle zwischen Forschung, Politik, Wirtschaft und Gesellschaft zu allen Fragen rund um Privatheit und Datenschutz.

» steht für einen intensiven Gedankenaustausch zur Verfügung und fördert den Dialog zwischen allen, die die Themen Privatheit und Datenschutz für wichtig halten.

Wir freuen uns auf den konstruktiven Diskurs mit Ihnen!

Ihr Forschungsverbund
„Forum Privatheit“

Die Fortentwicklung des Datenschutzes – Zwischen Systemgestaltung und Selbstregulierung

Vielfältige *Innovationen* der Informationstechnik stellen den Schutz von Grundrechten und Freiheiten vor fundamentale *Herausforderungen*: Allgegenwärtige Datenverarbeitung im Internet der Dinge mit Anwendungen in der Industrie 4.0, im Smart Home, im Smart Car oder im Rahmen von Smart Health erfassen Handlungen unzähliger Menschen und bewirken damit eine explosionsartige Zunahme personenbezogener Daten. Das Rückgrat der digitalen Gesellschaft bilden Infrastrukturen wie Suchmaschinen, Social Networks, Kommunikations- und Logistikdienste, deren wirtschaftliche Grundlage die Nutzung von Persönlichkeitsprofilen ist. Big Data-Analysen ermöglichen die Auswertung großer Datenmengen aus unterschiedlichen Quellen in Echtzeit. Dies eröffnet Chancen, birgt aber auch Risiken.

Herausforderungen meistern, ohne Chancen für Innovationen zu vergeben

Durch die allgegenwärtige Vernetzung werden moderne Basiskonzepte demokratischer Gesellschaften, wie etwa informationelle Selbstbestimmung, grundlegend in Frage gestellt. Datensparsamkeit und Zweckbindung der Datenverarbeitung passen nicht in eine Welt, in der Datenverarbeitung für vielfältige und nicht vorhersehbare Zwecke genutzt werden soll. Doch weder der europäische noch der deutsche Gesetzgeber haben bisher ein Konzept entwickelt, wie diesen *Herausforderungen* begegnet werden kann, ohne dabei die Chancen, die in den absehbaren Entwicklungen liegen, zu vergeben. Datenschutz bedarf hierfür sowohl einer neuen konzeptionellen Konturierung als auch neuer oder fortentwickelter Institutionen und Instrumente.

Kritischer und konstruktiver Diskurs

Soviel ist klar: Rein rechtliche Lösungen reichen nicht aus. Gefordert ist eine zukunftsadäquate Konzeption der Datenschutz-Governance. Auf der diesjährigen Konferenz des BMBF-geförderten „Forum Privatheit“ wollen wir daher konstruktiv und gestaltungsorientiert, aber auch kritisch und richtungsoffen über die Zukunft des Datenschutzes diskutieren. Es soll geklärt werden, inwieweit die *innovativen* Ansätze der Datenschutz-Grundverordnung wie das Gebot einer datenschutzgerechten Systemgestaltung, das Erfordernis einer Datenschutz-Folgenabschätzung, die Möglichkeit einer freiwilligen Datenschutz-Zertifizierung oder die Selbstregulierung durch Verhaltensregeln genutzt werden können, um den absehbaren *Herausforderungen* zu begegnen.

Mitgliedstaaten im Wettbewerb um geeignete Lösungen

Zu klären ist auch, was die Mitgliedstaaten im Rahmen ihrer Öffnungsklauseln zur Evolution des Datenschutzrechts beitragen können. Von einem Wettbewerb der Mitgliedstaaten um geeignete Lösungen könnte die Weiterentwicklung des Datenschutzrechts profitieren. Schließlich ist zu besprechen, welche Rolle inter- und transnationale Formen der Regulierung spielen, etwa im Rahmen der Vereinten Nationen. Welche Aspekte des Datenschutzes jenseits von rechtlicher Regulierung gestärkt oder gefördert werden können, ist ein weiterer wesentlicher Schwerpunkt der Konferenz.

Besserer Datenschutz durch einen interdisziplinären Dialog

Nur im interdisziplinären Dialog kann es gelingen, den *Herausforderungen* der digitalen Welt für einen modernen Datenschutz wirksam zu begegnen und dabei gleichzeitig die *Innovationschancen* der Digitalisierung zu nutzen. Die diesjährige Jahreskonferenz „Die Fortentwicklung des Datenschutzes“ des Forschungsverbunds „Forum Privatheit“ gibt allen beteiligten Fachdisziplinen und allen Interessierten die Gelegenheit, normative, institutionelle und instrumentelle Konzepte von Datenschutz zu diskutieren.

Programmübersicht 02. November 2017

10:00 **Registrierung**

11:00 **Eröffnung und Begrüßung – Saal**
Vertreter/in des BMBF
Alexander Roßnagel

Keynotes – Saal
▶ Datenschutz in Zeiten alles durchdringender Vernetzung – Herausforderungen für das Zusammenspiel von Technik und Regulierung
Frank Pallas

▶ Sind neue Technologien datenschutzrechtlich regulierbar?
Gerrit Hornung

▶ Datenschutz unter Druck: Fehlender Wettbewerb auf Plattformmärkten als Risiko für den Verbraucherschutz
Katharina Nocun

12:45 **Mittagspause**

14:00 **Track 1 Herausforderungen – Saal**
1.1 Probleme und Paradoxien des Datenschutzes

Track 2 Innovationen – Seminar 7
2.1 Umsetzung von Privacy by Design

16:00 **Kaffeepause**

16:30 **Track 1 Herausforderungen – Saal**
1.2 Zertifizierung

Track 2 Innovationen – Seminar 7
2.2 Gewährleistung von Transparenz

18:15 **Podiumsdiskussion: Umsetzung der Datenschutz-Grundverordnung im institutionellen Kontext – Saal**

Impulsvorträge:
▶ Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich
Philip Schütz

▶ Eine Vision für die Rolle der betrieblichen Datenschutzbeauftragten
Barbara Stoeferle

Weitere Diskutanten:
Thilo Weichert, Johannes Caspar, Achim Klabunde

Track 1 Herausforderungen

Saal

1.1 Probleme und Paradoxien des Datenschutzes

Fachliche Leitung: Marit Hansen

▶ Übersehene Probleme des Konzepts der Privacy Literacy
Thilo Hagendorff
▶ Was meint „Risiko“ im Datenschutz?
Martin Rost
▶ Das Einwilligungsparadox im Datenschutz: Eine Debattenkritik
Benjamin Bergemann
▶ Ungewollte Einwilligung? Die Rechtswirklichkeit der Informierten Zustimmung
Robert Rothmann

1.2 Zertifizierung

Fachliche Leitung: Thomas Hess

▶ Datenschutz als Wettbewerbsvorteil: Die Zertifizierung von Privacy by Design und der Stand der Technik
Maximilian von Grafenstein
▶ Dynamische Zertifizierung: Der Weg zum verordnungskonformen Cloud Computing
Johanna Hofmann

Track 2 Innovationen

Seminar 7

2.1 Umsetzung von Privacy by Design

Fachliche Leitung: Michael Kreutzer

▶ Anforderungs- und Entwurfsmuster als Instrumente des Privacy by Design
Robin Knote, Laura Friederike Thies, Matthias Söllner
▶ Erfolgsfaktoren für Privacy by Design
Sven Türpe, Andreas Poller
▶ Privatsphäre als inhärente Eigenschaft eines Kommunikationsnetzes
Matthias Marx, Maximilian Blochberger, Dominik Herrmann, Hannes Federrath

2.2 Gewährleistung von Transparenz

Fachliche Leitung: Michael Friedewald

▶ Mehr oder weniger frei? Bemerkungen zum Verhältnis von digitaler Werbung und individueller Autonomie
Sebastian Stein
▶ Smarte Regulierung von Informationskollektiven im Internet der Dinge
Charlotte Husemann, Fabian Pittroff
▶ Can the ISP be trusted?
Lukas Hartmann, Matthias Marx, Eva Schedel, Christian Roth, Wolfram Felber, Doğan Kesdoğan

Programmübersicht 03. November 2017

9:00 **Keynotes – Saal**
▶ Umsetzung der Datenschutz-Grundverordung
Paul Nemitz
▶ Notwendige Schritte zu einem modernen Datenschutzrecht
Alexander Roßnagel

10:15 **Kaffeepause**

10:30 **Track 1 Herausforderungen – Saal**
1.3 Staatliche Überwachung

Track 2 Innovationen – Seminar 7
2.3 Datenschutz in der gesellschaftlichen Kommunikation

12:30 **Mittagspause**

13:45 **Bericht aus den Konferenzsessions – Saal**
Felix Bieker, Christian Geminn

14.15 **Gesprächsrunde zur Fortentwicklung des Datenschutzes – Saal**
Nadine Absenger, Hannes Federrath, Marit Hansen, Konstantin von Notz

Resümee zur Zukunft der informationellen Selbstbestimmung
Alexander Roßnagel

Track 1 Herausforderungen

Raum: Saal

1.3 Staatliche Überwachung
Fachliche Leitung: Michael Friedewald

▶ Schutzpflicht des Staates für die informationelle Selbstbestimmung?
Martin Kutscha
▶ Datenanalysesysteme bei der Polizei im Lichte des neuen Datenschutzrechts
Paul Johannes
▶ Überwachungs-Gesamtrechnung
Benjamin Bremert, Felix Bieker, Thilo Hagendorff
▶ Ad-hoc-Kommunikation – Gesellschaftlich wünschenswert, rechtlich ungeregelt
Fabian Schaller, Patrick Lieser, Lars Almon, Flor Álvarez, Tobias Meuser

Track 2 Innovationen

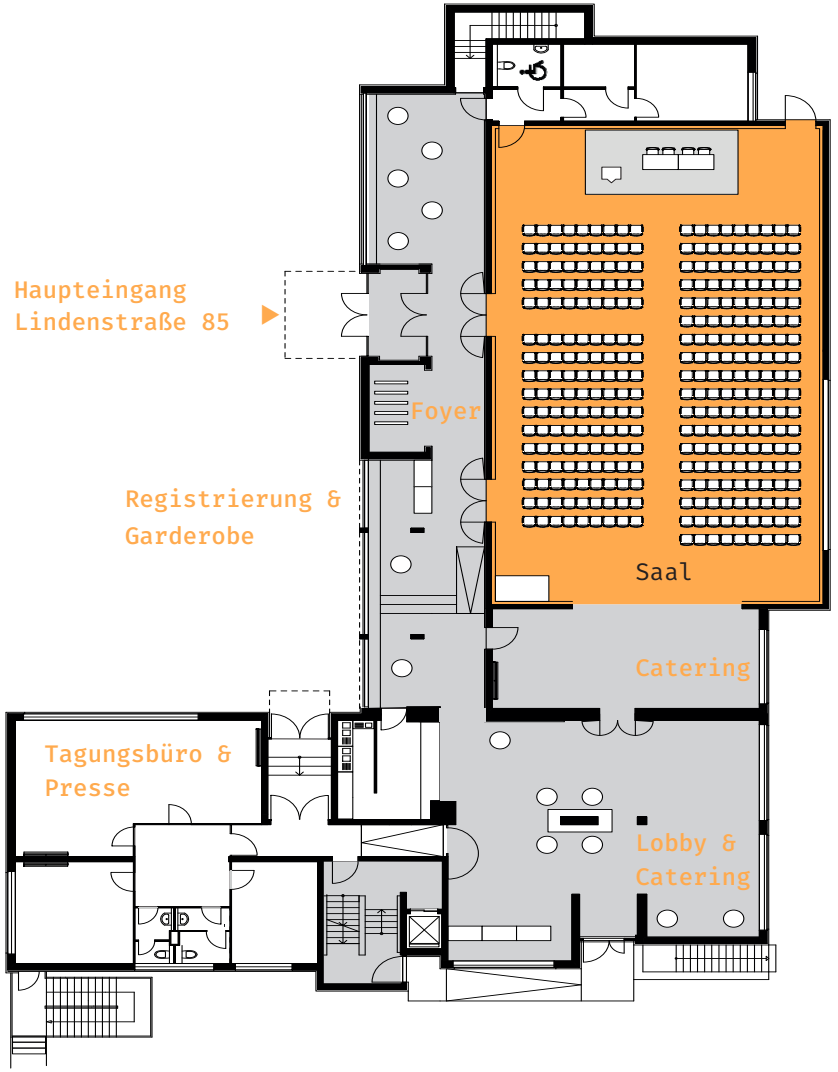
Raum: Seminar 7

2.3 Datenschutz in der gesellschaftlichen Kommunikation
Fachliche Leitung: Jessica Heesen

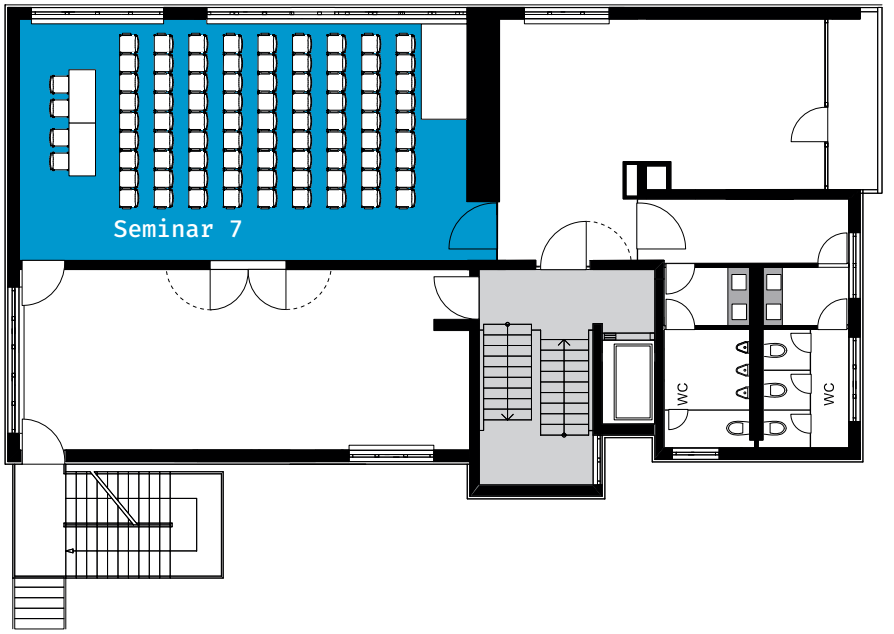
▶ Transparenz als zentrales Element von Datenschutzrecht, Ethik und Technik
Eva Schlehahn
▶ Das digitale Mosaik verstehen, Mündigkeit als Grundstein für Selbstbestimmung in der digitalen Gesellschaft
Daniel Guagnin
▶ Die Chancen von Intervenierbarkeit in (sozio-)technischen Systemen
Martin Degeling, Thomas Herrmann

Raumplan Tagungswerk

Erdgeschoss



2. Obergeschoss



Keynotes

02 November 2017

Datenschutz in Zeiten alles durchdringender Vernetzung – Herausforderungen für das Zusammenspiel von Technik und Regulierung
▶ Frank Pallas

Sind neue Technologien datenschutzrechtlich regulierbar?
▶ Gerrit Hornung

Datenschutz unter Druck: Fehlender Wettbewerb auf Plattformmärkten als Risiko für den Verbraucherschutz
▶ Katharina Nocun

03 November 2017

Umsetzung der Datenschutz-Grundverordnung
▶ Paul Nemitz

Notwendige Schritte zu einem modernen Datenschutzrecht
▶ Alexander Roßnagel

Keynotes

02 November 2017

Datenschutz in Zeiten alles durchdringender Vernetzung – Herausforderungen für das Zusammenspiel von Technik und Regulierung

Technologien, die lange Zeit unter Begriffen wie „Ubiquitous Computing“ vor allem theoretisch diskutiert wurden, etablieren sich unter anderem mit Wearables und Smart Homes geradezu schlagartig. Aus Sicht des Datenschutzes ergibt sich hieraus eine Vielzahl neuer Herausforderungen für das Zusammenspiel von technischer Entwicklung und Regulierung: Einwilligungen in ihrer bisher üblichen Form erweisen sich als zunehmend dysfunktional, für die datenschutzfreundliche Technikgestaltung („Data Protection by Design“) fehlen tragfähige, operationalisierbare Ansätze. Der Vortrag stellt ausgewählte Herausforderungen anhand aktueller technischer Entwicklungen dar und skizziert erste Ansätze zu deren Adressierung im Rahmen eines transdisziplinären „Privacy Engineerings“.

▸ **Dr. Frank Pallas** ist Senior Researcher am Fachgebiet Information Systems Engineering der TU Berlin. Nach Studium und Promotion in der Informatik forschte er von 2009 bis 2015 am Zentrum für Angewandte Rechtswissenschaft des KIT zu technisch-rechtlichen Fragestellungen von Privatheit und Nachweisbarkeit, insbesondere im Kontext von e-Energy, Elektromobilität und Cloud Computing. Von 2013 bis 2015 war er zudem Senior Researcher am FZI und von 2011 bis 2015 Gast- und Vertretungsprofessor für Informatik und Gesellschaft an der TU Berlin. Aktuell forscht er unter anderem zur technischen Repräsentation von Einwilligungen im IoT-Kontext, zur Konkretisierbarkeit des datenschutzrechtlichen Prinzips der Verhältnismäßigkeit technischer Maßnahmen und zu weiteren Aspekten des interdisziplinären „Privacy Engineering“.

Keynotes

02 November 2017

Sind neue Technologien datenschutzrechtlich regulierbar?

Sechs Monate vor dem Geltungsbeginn der Datenschutz-Grundverordnung ist die rechtswissenschaftliche Durchdringung der neuen Anforderungen weit fortgeschritten, konzentriert sich aber weithin auf die verfahrensrechtlichen Regelungen für Datenverarbeiter und Aufsichtsbehörden. Hinsichtlich der materiellen Anforderungen hat sich der europäische Gesetzgeber auf sehr abstrakte Vorgaben und Prinzipien zurückgezogen. Dies erfordert erhebliche Konkretisierungsleistungen für neue Technologien und Geschäftsmodelle, die in praktisch allen Lebensbereichen Einzug halten werden (Smart Home, Smart Car, Smart City, etc.). Da viele dieser Innovationen die abstrakten Prinzipien vor strukturelle Probleme stellen, ist es von erheblicher Relevanz, wem die Kompetenz zur Konkretisierung zukommt. Das Geflecht aus europäischer und nationaler, staatlicher und privater Regulierung ist bisher noch sehr im Fluss, wird aber erheblichen Einfluss auf die Zukunft des Datenschutzes ausüben.

▸ **Prof. Dr. Gerrit Hornung, LL.M.** studierte Rechtswissenschaften und Philosophie an den Universitäten Freiburg und Edinburgh; Referendariat in Hamburg. Promotion und Habilitation an der Universität Kassel; 2006 bis 2011 Geschäftsführer der dortigen Projektgruppe verfassungsverträgliche Technikgestaltung (provet). 2011 bis 2015 Professor für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau und Sprecher des interfakultären Instituts für IT-Sicherheit und Sicherheitsrecht (ISL). Seit 2015 Professor für Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel und Direktor am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG).

Keynotes

03 November 2017

Notwendige Schritte zu einem modernen Datenschutzrecht
Nachdem die Datenschutz-Grundverordnung beschlossen ist, stellt sich die Frage, wie die Entwicklung des Datenschutzrechts weitergeht. Dies setzt die Beantwortung von drei Fragen voraus: Welche Herausforderungen für das europäische Datenschutzrecht stellen die absehbaren Entwicklungen und Anwendungen der künftigen Informationstechnik? Für welche Risiken bietet die Datenschutz-Grundverordnung einen geeigneten Schutz der Grundrechte? Wer ist zuständig und in der Lage, die verbleibenden Regelungsdefizite zu beseitigen? Der Vortrag geht davon aus, dass die Datenschutz-Grundverordnung eine Ko-Regulierung des Datenschutzes durch Union und Mitgliedstaaten vorsieht und versucht, auf dieser Grundlage die drei Fragen zu beantworten.

▶ **Prof. Dr. Alexander Roßnagel** ist Sprecher des „Forum Privatheit". Er ist zudem wissenschaftlicher Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" und Direktor des Wissenschaftlichen Zentrums für Informationstechnik-Gestaltung (ITeG) sowie Universitätsprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel. Von 2003 bis 2011 war er Vizepräsident der Universität Kassel. Jüngste Veröffentlichung: Europäisches Datenschutzrecht – Die Datenschutz-Grundverordnung und das angepasste deutsche Datenschutzrecht, Nomos 2018.

Keynotes

02./3. November 2017

Datenschutz unter Druck: Fehlender Wettbewerb auf Plattformmärkten als Risiko für den Verbraucherschutz
Zusammenfassung liegt bei Drucklegung nicht vor.

▶ **Katharina Nocun** ist Bürgerrechtlerin, Publizistin und Ökonomin. Sie leitete bundesweit Kampagnen zum Thema Datenschutz, Whistleblower und Bürgerrechte, unter anderem für die Bürgerbewegung Campact e.V., den Verbraucherzentrale Bundesverband sowie die Kampagne „Asyl für Snowden". Sie ist Mitglied im Beirat des Whistleblower-Netzwerk e.V. und klagt gegen mehrere Überwachungsgesetze vor dem Bundesverfassungsgericht. Sie veröffentlicht regelmäßig Beiträge zum Thema Datenschutz in zahlreichen Medien und schreibt eine Kolumne beim Handelsblatt.

Umsetzung der Datenschutz-Grundverordnung
Zusammenfassung liegt bei Drucklegung nicht vor.

▶ **Paul Nemitz** ist Leitender Beamter in der Generaldirektion für Justiz und Verbraucher der Europäischen Kommission. Er hat im Juristischen Dienst der Europäischen Kommission, dem Kabinett des Kommissars für Entwicklungszusammenarbeit und in anderen Generaldirektionen Stellung genommen. Als Gastprofessor an der Hochschule für Europa in Brügge lehrt er EU-Recht.

Vorträge

Track 1 Herausforderungen

1.1
- Thilo Hagendorff
- Martin Rost
- Benjamin Bergemann
- Robert Rothmann

1.2
- Maximilian von Grafenstein
- Johanna Hofmann

1.3
- Martin Kutscha
- Paul Johannes
- Benjamin Bremert, Felix Bieker, Thilo Hagendorff
- Fabian Schaller, Patrick Lieser, Lars Almon, Flor Álvarez, Tobias Meuser

Track 2 Innovationen

2.1
- Robin Knote, Laura Friederike Thies, Matthias Söllner
- Sven Türpe, Andreas Poller
- Matthias Marx und andere

2.2
- Sebastian Stein
- Charlotte Husemann, Fabian Pittroff
- Lukas Hartmann und andere

2.3
- Eva Schlehahn
- Daniel Guagnin
- Martin Degeling, Thomas Herrmann

1.1

Übersehene Probleme des Konzepts der Privacy Literacy

▶ **Thilo Hagendorff**

Die Forderungen nach Privacy Literacy, nach Datenschutzkompetenzen und technischen Fähigkeiten, sich selbst vor Privatheitsbedrohungen zu schützen, werden typischerweise unhinterfragt aufgenommen und unkritisch weiterverbreitet. Dabei gibt es eine ganze Reihe an Problemen, welche bislang kaum bedacht worden sind. Diesen Problemen soll sich der Vortrag widmen, wobei vier Argumentationsstränge aufgegriffen werden. Diese verfolgen erstens das Problem sozialer Ungleichheiten hinsichtlich der Fähigkeiten der Mediennutzung, zweitens das Problem des nicht-rationalen Mediengebrauchs, drittens das Problem der Reduzierung von Privatheitsfragen auf Front-End-Features, und viertens das Problem der Transferierung von Verantwortung von staatlichen Institutionen hin zu Einzelpersonen.

Was meint „Risiko“ im Datenschutz?

▶ **Martin Rost**

Jede Organisation greift durch die Verarbeitung personenbezogener Daten in die Grundrechte einer Person ein. Ins Operative gewendet erzeugt dieser Eingriff Datenschutzrisiken, die für die Organisation ganz andere sind als für die betroffenen Personen (Risiken 1. Ordnung). Die Formen der Beobachtung und der Konditionierung dieser Risiken 1. Ordnung erzeugen weitere, andere Formen von Datenschutzrisiken (Risiken 2. Ordnung). In welche Beziehung lässt sich dieser Risikobegriff zur betriebswirtschaftlichen Formel „Risiko = Schadenshöhe x Eintrittswahrscheinlichkeit“, die in der DSGVO Erwähnung findet, setzen?

1.1

Das Einwilligungsparadox im Datenschutz: Eine Debattenkritik

▶ **Benjamin Bergemann**

Trotz fundierter Kritik kreisen zahlreiche Diskussionen und praktische Bemühungen um die Fortentwicklung des Datenschutzes weiterhin auf die informierte Einwilligung. Das Festhalten an der Einwilligung – trotz fortwährender Kritik – bezeichne ich als Einwilligungsparadox. Problematisch ist das Einwilligungsparadox, da es nicht nur den Blick auf die Grenzen der Einwilligung und ihre Alternativen verstellt, sondern auch von weiteren Problemen und Gestaltungsoptionen im Datenschutz ablenkt. Der Vortrag beleuchtet das Einwilligungsparadox anhand einer Analyse der jüngeren deutschen Datenschutzdebatte. Auf dieser Basis erfolgt eine empirisch belehrte Debattenkritik, die dabei helfen soll, das Einwilligungsparadox zu reflektieren und mit ihm zu brechen.

Ungewollte Einwilligung? Die Rechtswirklichkeit der Informierten Zustimmung

▶ **Robert Rothmann**

Der folgende Beitrag widmet sich dem Rechtsinstitut der Informierten Zustimmung als Rechtsgrundlage zur Verarbeitung personenbezogener Daten am Beispiel des Unternehmens Facebook. Dabei geht es um die Frage, ob und inwiefern die betroffenen Nutzerinnen und Nutzer tatsächlich entsprechend der rechtlichen Bestimmungen „ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage“ in das Vertragswerk einwilligen und somit „freiwillig“ auf ihre grundrechtlichen Ansprüche verzichten. In der Beantwortung geht die Studie über eine rechtsdogmatische Abhandlung der Thematik hinaus und präsentiert exklusive Ergebnisse einer repräsentativen Erhebung unter österreichischen Usern für eine weiterführende kritische Diskussion der Qualität des rechtlichen Konzepts der Einwilligung in der Online-Welt.

1.2

Datenschutz als Wettbewerbsvorteil: Die Zertifizierung von Privacy by Design und der Stand der Technik

▶ **Maximilian von Grafenstein**

Der Vortrag untersucht Funktion und Wirkungen datenschutzrechtlicher Prinzipien beziehungsweise unbestimmter Rechtsbegriffe in Kombination mit Zertifizierungen als Instrumente der Regulierung datengetriebener Innovation. Danach sind rechtliche Anforderungen, die einen weiten Interpretationsspielraum lassen, grundsätzlich innovationsoffener als klassische Konditionalnormen, weil sie dem Regelungsadressaten mehr Spielraum bei der Umsetzung lassen. Die damit einhergehende Rechtsunsicherheit kann allerdings innovationshindernd wirken. Um diese Rechtsunsicherheit zu reduzieren, können die Regelungsadressaten bestimmte Datenverarbeitungen daher zertifizieren lassen. Unter welchen Prämissen dies tatsächlich zu dem versprochenen „Wettbewerbsvorteil durch Datenschutz" führt, kann diskutiert werden.

Dynamische Zertifizierung: Der Weg zum verordnungskonformen Cloud Computing

▶ **Johanna Hofmann**

Cloud-Kunden dürfen nach Art. 28 Absatz 1 DSGVO nur mit Anbietern zusammenarbeiten, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den Verordnungsanforderungen erfolgt und den Schutz der Betroffenenrechte gewährleistet. Zum Nachweis dürfen sie sich auf Zertifizierungen stützen. Dabei erfordert ein dynamischer Gegenstand einen dynamischen Nachweis, der dafür sorgt, dass ein neutrales kontinuierliches Monitoring der Dienste deren Datenschutz- und Datensicherheitskonformität momentgenau überwacht. Die Mitgliedsstaaten sind berufen, die Rahmenbedingungen zu konkretisieren und klare Vorgaben zu machen. Der Vortrag zeigt Lösungswege auf.

1.3

Schutzpflicht des Staates für die informationelle Selbstbestimmung?

▶ **Martin Kutscha**

Angesichts der heutigen Realität massenhafter Preisgabe und Auswertung personenbezogener Daten stellt sich die Frage, ob die klassischen Prinzipien des Datenschutzrechts wie die Zweckbindung, die Datensparsamkeit und das Erfordernis einer „informierten Einwilligung" der Betroffenen nicht längst obsolet geworden sind. Was ergibt sich in dieser Situation aus dem Postulat einer Schutzpflicht des Staates für das Individualrecht auf informationelle Selbstbestimmung? Was kann ein supranationales Datenschutzrecht leisten, oder sollte der Fokus stärker auf die Instrumente des technischen (Selbst-) Datenschutzes gerichtet werden?

Datenanalysesysteme bei der Polizei im Lichte des neuen Datenschutzrechts

▶ **Paul Johannes**

Datenanalyse- und Entscheidungsunterstützungssysteme sind Softwaresysteme, die aus einer großen Menge von unstrukturierten Daten für operative und strategische Aufgaben relevante Informationen ermitteln, aufbereiten, übersichtlich zusammenstellen und bei der Auswertung helfen. Ihr Einsatz muss datenschutzverträglich erfolgen. Aus dem neuem Datenschutzrecht lassen sich auch technische Gestaltunganforderungen ableiten.

1.3

Überwachungs-Gesamtrechnung

▶ **Benjamin Bremert, Felix Bieker, Thilo Hagendorff**

Im Rahmen seines Urteils zur Vorratsdatenspeicherung aus dem Jahre 2010 hat das BVerfG den Gedanken aus dem Volkszählungsurteil, dass der Einzelne unter den Bedingungen automatischer Datenerhebung und -verarbeitung nicht zum bloßen Informationsobjekt werden darf, weitergeführt und für die Einführung anlassloser Überwachungsmaßnahmen eine Grenze der Gesamtüberwachung gezogen. Danach darf die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden. Das Paper zeigt mittels der verfassungsrechtlichen Grundlagen die Notwendigkeit des als „Überwachungs-Gesamtrechnung" bekannt gewordenen Instrumentariums auf, stellt eine mögliche konkrete Umsetzung dar und erläutert sodann die mit der Implementierung einhergehenden Probleme.

Ad-hoc-Kommunikation – Gesellschaftlich wünschenswert, rechtlich ungeregelt

▶ **Fabian Schaller, Patrick Lieser, Lars Almon, Flor Álvarez, Tobias Meuser**

Bei einem Ad-hoc-Kommunikationsnetzwerk auf Peer-to-Peer-Basis ist rechtlich gesehen jede Nutzerin und jeder Nutzer zugleich Anbieter. Dieser hat aber keinerlei Möglichkeit, auf die Technik selbst Einfluss zu nehmen und verfügt auch über keine vollständigen Informationen über das Netzwerk. Sogar die Gesamtzahl der Teilnehmerinnen und Teilnehmer ist der einzelnen Nutzerin oder dem einzelnen Nutzer in der Regel unbekannt. Dadurch ist es ihm unmöglich, seine datenschutzrechtlichen Pflichten zu erfüllen. Als Lösungsansatz bietet sich hier die Verpflichtung des App-Anbieters an. Hierzu bedarf es spezieller gesetzlicher Regelungen für diese Kommunikationsnetzwerke, damit diese ihren gesellschaftlich wünschenswerten Effekt auch verwirklichen können, ohne dabei den Datenschutz der Nutzerin oder des Nutzers zu vernachlässigen.

2.1

Anforderungs- und Entwurfsmuster als Instrumente des Privacy by Design

▶ **Robin Knote, Laura Friederike Thies, Matthias Söllner**

Artikel 25 DSGVO formuliert in abstrakter Form Anforderungen an Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Zur Konkretisierung dieser Vorgaben beitragen können Anforderungs- und Entwurfsmuster, die es ermöglichen, datenverarbeitende Applikationen so zu entwickeln, dass rechtliche Anforderungen methodisch bereits im Prozess der Systementwicklung integriert werden und so ein Ausgleich zwischen der Förderung der Dienstleistungsqualität und der Rechtsverträglichkeit geschaffen wird. Ziel ist es dabei nicht, lediglich rechtliche Mindeststandards einzuhalten, sondern einen möglichst hohen Grad an Rechtsverträglichkeit zu erreichen. Besondere Relevanz erlangen diese Muster bei datenintensiven Produkten, wie kontextsensitiven Applikationen.

Erfolgsfaktoren für Privacy by Design

▶ **Sven Türpe, Andreas Poller**

Privacy by Design steht für den Versuch, Datenschutz durch Interventionen nicht nur im Betrieb, sondern bereits in der Entwicklung von IT-Systemen zu erreichen. Das ist nötig, da die Konsequenzen von Entwurfsentscheidungen später schwer zu kompensieren sind. Doch Softwareentwicklung ist als anspruchsvolle analytisch-gestalterische Tätigkeit schwer zu steuern. Mit Appellen ist es nicht getan und auch gezielte Versuche der Einflussnahme haben oft nicht die erhoffte Wirkung. Damit Privacy by Design funktioniert, bedarf es echter ökonomischer Anreize, der effektiven Vertretung von Datenschutzanforderungen im Entwicklungsprozess, geeigneter Feedbackmechanismen sowie eines Ökosystems, das Datenschutz auch über Projektgrenzen hinaus entlang von Softwarelieferketten behandelt.

2.1 / 2.2

Privatsphäre als inhärente Eigenschaft eines Kommunikationsnetzes

▶ Matthias Marx, Maximilian Blochberger, Dominik Herrmann, Hannes Federrath

Die Aktionen von Endnutzerinnen und Endnutzern beim Surfen können nicht nur durch Cookies, sondern auch durch ihre IP-Adresse zur Profilbildung verknüpft werden. Während der Schutz der Endnutzerin oder des Endnutzers vor Cookies noch einfach gelingt, werden existierende Schutzmaßnahmen gegen ein adressbasiertes Tracking nur selten eingesetzt, denn sie erfordern Problembewusstsein und technischen Sachverstand. Es bedarf daher einer Anonymisierungslösung, die sich gut in die bestehende Infrastruktur des Internets integrieren lässt und von einer breiten Öffentlichkeit genutzt werden kann. Wir stellen eine solche Anonymisierungslösung vor, die den großen, durch IPv6 zur Verfügung stehenden Adressraum nutzt, um die Privatsphäre von Endnutzerinnen und Endnutzern auf Netzwerkebene zu schützen.

Mehr oder weniger frei? Bemerkungen zum Verhältnis von digitaler Werbung und individueller Autonomie

▶ Sebastian Stein

In diesem Beitrag sollen die begrifflichen Grundlagen des Problemkomplexes Privatsphäre, Autonomie und Manipulationspotenzial im Kontext der digitalen Werbung untersucht werden. Angesichts immer ausgefeilterer und subtilerer digitaler Werbetechniken (zum Beispiel customer tracking und -profiling, Kundengesichtserkennung, cookies-basierte Datensammlung, kommerzieller Datenverkauf) stellt sich die Frage, inwiefern durch Unterwanderung der digitalen Privatsphäre und die damit einhergehende Manipulation die Kundenautonomie eingeschränkt oder gefördert wird: In welchem Sinn, falls überhaupt, können uns digitale Werbung und Verletzung der Privatsphäre die Autonomie rauben oder erweitern? Im Lichte der Unterscheidung zwischen prinzipieller

2.2

und quantitativer Autonomie soll erwogen werden, welche Aspekte quantitativer Autonomie besonders fragil und ethisch schützenswert sind.

Smarte Regulierung von Informationskollektiven im Internet der Dinge

▶ Charlotte Husemann, Fabian Pittroff

Die digitale Vernetzung alltäglicher Gegenstände und Praktiken im Internet der Dinge birgt neue Herausforderungen für die Zukunft des Datenschutzes. Es stellt sich die Frage, wie Nutzerinnen und Nutzer angemessen über datenschutzrelevante Prozesse informiert werden können, ohne dabei über- oder unterfordert zu werden. Auf der Suche nach Lösungen wird der Beitrag die Problemsituation als Informationskollektiv analysieren und ein Schema zum Vergleich diverser Ansätze der Regulierung und Vermittlung im Internet der Dinge vorstellen. Vor diesem Hintergrund werden Potenziale und Grenzen rechtlicher Regulierung skizziert, um den angemessenen Einsatz von Delegation und Partizipation im Internet der Dinge zu erkunden.

Can the ISP be trusted?

▶ Lukas Hartmann, Matthias Marx, Eva Schedel, Christian Roth, Wolfram Felber, Doğan Kesdoğan

Die Ausübung der informationellen Selbstbestimmung muss auch für technisch nicht versierte Internetnutzerinnen und Internetnutzer sichergestellt sein. Eine Mehrheit sieht ihre Privatsphäre bedroht, weiß sich aber nicht zu schützen. Der Internet Service Provider (ISP) könnte hier als Dienstleister Anonymisierungslösungen bereitstellen. In technischen Veröffentlichungen wird zumeist die Vertrauenswürdigkeit des ISP angenommen. Ob dieses Vertrauen gerechtfertigt ist, soll in diesem Vortrag aus technischer, juristischer und soziologischer Sicht diskutiert werden. Können Transparency Enhancing Technologies (TETs) dazu beitragen, der Endnutzerin oder dem Endnutzer ein fundiertes Vertrauen zum ISP zu vermitteln?

2.3

Transparenz als zentrales Element von Datenschutzrecht, Ethik und Technik

▶ Eva Schlehahn

Transparenz ist eine wesentliche Voraussetzung, um die Prüfbarkeit von Datenverarbeitungsvorgängen zu gewährleisten. Sie ergibt sich jedoch nicht nur als Forderung aus dem Datenschutzrecht, sondern auch aus anderen Bereichen, wie etwa der Ethik und der Technik. Insoweit ergibt sich die Notwendigkeit, funktionale Anforderungen an automatisierte Datenverarbeitungssysteme kohärent zu formulieren, um Diskrepanzen zu vermeiden. Dieser Beitrag erläutert die zentralen Kernforderungen dieser unterschiedlichen Disziplinen in Bezug auf Transparenz und zeigt auf, dass sich diese gegenseitig stützen und ergänzen können. Auf diese Weise kann eine verbesserte Informiertheit und Kontrollmöglichkeit seitens des Betroffenen, wie auch Prüffähigkeit für Aufsichtsbehörden hergestellt werden.

Das digitale Mosaik verstehen, Mündigkeit als Grundstein für Selbstbestimmung in der digitalen Gesellschaft

▶ Daniel Guagnin

Technische Entwicklungen sind häufig mit einem Cultural Lag verbunden. Demokratie beruht aber auf Mündigkeit und dem Verstehen der Zusammenhänge gesellschaftlicher Strukturen wie beispielsweise der Beurteilung der Informationsquellen und der Reichweite der Folgen von Einwilligungserklärungen. Die Implikationen von Algorithmen und ihre gesellschaftliche Wirkung müssen Teil der Allgemeinbildung werden, um eine Debatte über die Potenziale und Gefahren der Digitalisierung den Experten- und Expertinnenrunden zu entheben und eine breite gesellschaftliche Diskussion zu ermöglichen.
Im Vortrag werden verschiedene Ansätze skizziert, um Bildung über die gesellschaftlichen Zusammenhänge voranzubringen und Folgen technischer Entwicklung bewusst zu machen.

2.3

Die Chancen von Intervenierbarkeit in (sozio-)technischen Systemen

▶ Martin Degeling, Thomas Herrmann

Im Vortrag soll das Datenschutz-Ziel „Intervenierbarkeit“ aus der Perspektive derjenigen beleuchtet werden, deren Daten verarbeitet werden. „Intervenierbarkeit“ bietet die Möglichkeit, kontextabhängige Entscheidungen zu treffen, die sich an der konkreten Nutzung der Daten orientieren und auch nach der Preisgabe von Daten noch durchsetzbar sind. Die Datenschutzgrundverordnung betont diesbezüglich sowohl das Recht auf Vergessenwerden als auch das Recht auf Widerspruch. Der Vortrag beschreibt die Chancen von „Intervenierbarkeit“ in (sozio-)technischen Systemen anhand konkreter Beispiele. Dabei reichen die Möglichkeiten von klassischen Methoden zur Gestaltung der Mensch-Maschine-Interaktion über organisatorische Lösungen bis hin zu Verfahren, die Daten (temporär) unbrauchbar machen.

Podiumsdiskussion

02 November 2017

Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich
▶ **Philip Schütz**

Eine Vision für die Rolle der betrieblichen Datenschutzbeauftragten
▶ **Barbara Stoeferle**

Zum Leben zu wenig, zum Sterben zu viel? Die Finanzierung deutscher Datenschutzbehörden im Vergleich

▶ **Philip Schütz**

Unterschiedliche Studien weisen darauf hin, dass Datenschutzbehörden nicht nur in Deutschland, sondern auch in anderen EU-Mitgliedsstaaten häufig personell unterbesetzt und chronisch unterfinanziert sind. Die EU-Datenschutzgrundverordnung (DS-GVO) schreibt daher vor, dass „jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen […] ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse […] effektiv wahrnehmen zu können".

Diese neue gesetzliche Vorgabe soll daher zum Anlass genommen werden, eine Bestandsaufnahme vorzunehmen, wie es um deutsche Datenschutzbehörden in finanzieller und personeller Hinsicht bestellt ist. Zudem sollen Gründe skizziert werden, warum Datenschutzbehörden in Deutschland personell und finanziell unterschiedlich aufgestellt sind.

Eine Vision für die Rolle der betrieblichen Datenschutzbeauftragten

▶ **Barbara Stoeferle**

Seit Beginn des Datenschutzes geht es darum, dass Einzelne nicht durch Machtasymmetrien oder neue Techniken in ihrem Persönlichkeitsrecht eingeschränkt werden.

Bereits im ersten BDSG wurde die Funktion des Datenschutzbeauftragten verankert. Dieser soll stellvertretend für Betroffene auf den Schutz des Persönlichkeitsrechts achten, zwischen Interessen abwägen und dabei die neuen Technologien berücksichtigen und Regeln mitgestalten.

Der Datenschutzbeauftragte wird leider oft als Kontrolleur wahrgenommen, der überwacht und zusätzliche Maßnahmen fordert, welche angeblich den Alltag behindern. Dabei wird übersehen, dass der Datenschutzbeauftragte auch schon im BDSG viele Beratungsaufgaben hat. Die DSGVO verstärkt dies und weist dem Datenschutzbeauftragten Gestaltungsmöglichkeiten zu.

„BvD – Datenschutz gestalten" lautet das Logo des BvD. Eine spannende Herausforderung!

Vortragende

A-Z

- Lars Almon
- Flor Álvarez
- Benjamin Bergemann
- Felix Bieker
- Maximilian Blochberger
- Benjamin Bremert
- Martin Degeling
- Hannes Federrath
- Wolfram Felber
- Daniel Guagnin
- Thilo Hagendorff
- Lukas Hartmann
- Dominik Herrmann
- Thomas Herrmann
- Johanna Hofmann
- Charlotte Husemann
- Paul Johannes
- Doğan Kesdoğan
- Robin Knote
- Martin Kutscha
- Patrick Lieser
- Matthias Marx
- Tobias Meuser
- Fabian Pittroff
- Andreas Poller
- Martin Rost
- Christian Roth
- Robert Rothmann
- Fabian Schaller
- Eva Schedel
- Eva Schlehahn
- Philip Schütz
- Sebastian Stein
- Matthias Söllner
- Barbara Stoeferle
- Laura Friederike Thies
- Sven Türpe
- Maximilian von Grafenstein

▸ **Lars Almon, M. Sc.**, studierte Informatik und IT-Sicherheit an der Technischen Universität Darmstadt. Seit 2015 ist er wissenschaftlicher Mitarbeiter am Fachgebiet Sichere Mobile Netze (SEEMOO) an der Technischen Universität Darmstadt. Er beschäftigt sich in seiner Forschung mit der Sicherheit von verteilten, ressourcenbeschränkten Systemen. Der Fokus liegt hierbei auf dem Internet der Dinge und drahtlosen Sensornetzwerken, sowie dem Design und der Umsetzung realitätsnaher Testumgebungen.

▸ **Flor Álvarez, M.Sc.**, absolvierte ihr Diplomstudium in Elektrotechnik und Informationsnetzwerke in Ecuador. An der Hochschule Mannheim studierte sie im Master-Studiengang Informationstechnik. Seit 2014 ist sie wissenschaftliche Mitarbeiterin am Fachgebiet Sichere Mobile Netze (SEEMOO) an der Technischen Universität Darmstadt. Dort befasst sie sich unter anderem mit der Erforschung eines dezentralen Kommunikationssystems auf Basis von Smartphones, das sich zum einen mit Methoden zur Erstellung, Speicherung und Weiterleitung von Nachrichten in infrastrukturlosen Netzen beschäftigt und zum anderen Mechanismen zur Gewährleistung einer sicheren Kommunikation in solchen Netzen bereit stellt.

▸ **Benjamin Bergemann** ist Politikwissenschaftler und forscht in der Forschungsgruppe Politikfeld Internet am Wissenschaftszentrum Berlin für Sozialforschung (WZB) zur Politik des Datenschutzes. Im Mittelpunkt seiner Arbeit stehen die sich wandelnden Paradigmen und Konflikte des Datenschutzes sowie ihre Folgen für Freiheit und Selbstbestimmung. Er bedient sich hierzu feld- und diskurstheoretischer Herangehensweisen. Daneben engagiert sich Benjamin Bergemann in der netzpolitischen Zivilgesellschaft. Er ist gelegentlicher Autor für das Blog netzpolitik.org und Mitglied im Digitale Gesellschaft e.V.

▸ **Felix Bieker** ist seit 2013 juristischer Mitarbeiter im Projektreferat des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Er ist in den Projekten „Forum Privatheit“ und ITS.APT tätig. Das Projekt ITS.APT forscht zu der Frage des IT-Sicherheitsbewusstseins von Beschäftigten und will dies durch Penetration-Tests verbessern. Er ist Mitglied im „Forum Privatheit“.

▸ **Maximilian Blochberger, M.Sc.**, arbeitet seit September 2016 als wissenschaftlicher Mitarbeiter im Arbeitsbereich Sicherheit verteilter Systeme (SVS) der Universität Hamburg. Sein Hauptinteresse liegt im Bereich Datenschutz und Sicherheit in mobilen Anwendungen. Er hat Software-System-Entwicklung (B. Sc.) und Informatik (M. Sc.) von 2009 bis 2016 an der Universität Hamburg studiert. Neben seinem Studium hat er von 2012 bis 2016 bei der froglogic GmbH gearbeitet und war dort mit den Themen Softwareentwicklung, Software-Testing und Qualitätssicherung beschäftigt.

▸ **Benjamin Bremert** ist seit 2016 juristischer Mitarbeiter im Projektreferat des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Er arbeitet in den Projekten „Forum Privatheit“ und iTESA. Im Projekt iTESA geht es um die Frage der Zulässigkeit einer Smart Data-Anwendung zur Erkennung von Reiserisiken.

▸ **Dr. Martin Degeling** ist post-doctoral fellow am Institute for Software Research der Carnegie Mellon Universität in Pittsburgh. Seine Dissertation „Online Profiling“: Analyse und Intervention zum Schutz von Privatheit erschien 2016 und untersucht am Beispiel von Googles Interessenprofiling für Online Werbung, welche Folgen Data Mining für die Privatheit der Einzelnen als auch Privatheit im Allgemeinen hat. Sein Forschungsinteresse gilt darüber hinaus der Entwicklung von Werkzeugen zur Förderung von Transparenz von Intervenierbarkeit in datenverarbeitende Systeme, die ansonsten unbemerkt von den Betroffenen agieren.

▸ **Prof. Dr. Hannes Federrath** ist seit 2011 Leiter des Arbeitsbereichs Sicherheit in verteilten Systemen an der Universität Hamburg. Seine Arbeitsschwerpunkte sind Sicherheit im Internet, IT-Sicherheits- und Risikomanagement, Kryptographie und Mobile Computing. Von 1989 bis 1994 studierte er an der Universität Dresden Informatik und promovierte 1998 zur Sicherheit mobiler Systeme. Von 1999 bis 2000 forschte er am International Computer Science Institute Berkeley, Kalifornien. Von 2000 bis 2003 vertrat er eine Professur an der Freien Universität Berlin und leitete dort die Security-Gruppe. Von 2003

bis 2011 war er Inhaber eines Lehrstuhls für Management der Informationssicherheit an der Universität Regensburg.

▸**Wolfram Felber** ist stellvertretender Referatsleiter des aufsichtsbehördlichen Bereichs des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Zuvor war er juristischer Mitarbeiter im Projektbereich des Hauses und hat dort die Projekte AppPETs (Datenschutzfreundliche Smartphone-Anwendungen ohne Kompromisse) und AN.ON-Next (Anonymität Online der nächsten Generation) betreut.

▸**Daniel Guagnin** hat am Zentrum Technik und Gesellschaft der Technischen Universität Berlin zur Rolle von Datenschutz im Sicherheitssektor, die Rolle von Grundrechten und Vertrauen der Bürgerinnen in Sicherheitstechnologien sowie zu Auswirkungen von Profiling-Technologien auf die Grundrechte geforscht. In seiner Doktorarbeit diskutiert er die kritische Rolle von Vertrauen in Software und untersucht Freie Software Communities als Ansatz für Vertrauens- und Macht-Regulierung zwischen Expertinnen und Laien. Seit 2017 arbeitet er bei Praemandatum im Rahmen von Beratungstätigkeiten an der Übersetzung von Wissen über Datenschutz in die angewandte Praxis.

▸**Dr. Thilo Hagendorff** studierte Philosophie, Kulturwissenschaften und Deutsche Literatur in Konstanz und Tübingen. Er promovierte 2013 mit einer soziologischen Arbeit zum Thema „Sozialkritik und soziale Steuerung". Seit 2013 ist er wissenschaftlicher Mitarbeiter am Internationalen Zentrum für Ethik in den Wissenschaften und seit 2014 Dozent an der Universität Tübingen. Er ist Mitglied im „Forum Privatheit".

▸**Lukas Hartmann** ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik IV (IT-Sicherheitsmanagement) von Doğan Kesdoğan an der Universität Regensburg. Am Karlsruher Institut für Technologie (KIT) hat er Mathematik und Informatik studiert. Im Rahmen seiner wissenschaftlichen Tätigkeit arbeitet er im vom BMBF geförderten Projekt „Anonymität Online der nächsten Generation" (AN.ON-Next) zur Entwicklung datenschutzfreundlicher

Lösungen für den Endverbraucher. Hierbei beschäftigt er sich unter anderem mit Datenschutzlösungen für zukünftige Mobilfunknetze der fünften Generation (5G). Seine Forschungsthemen befinden sich im Spannungsfeld vernetzter Systeme, Datenschutz und Gesellschaft.

▸**Dr. Dominik Herrmann** hat bis 2008 an der Universität Regensburg Wirtschaftsinformatik studiert. Danach war er dort als Studiengangkoordinator tätig. Im Jahr 2011 wechselte er an den Fachbereich Informatik der Universität Hamburg, wo er 2014 promoviert wurde. Seine Dissertation wurde unter anderem mit dem Dissertationspreis der Gesellschaft für Informatik (GI) ausgezeichnet. Zwischen 2015 und 2017 war er an der Universität Siegen mit der Vertretung der Professur für IT-Sicherheitsmanagement beauftragt. Herrmann erforscht datenschutzfreundliche Systeme und Angriffe auf die Privatsphäre. Er ist GI-Junior-Fellow, Mitglied des GI-Präsidiums und Mitherausgeber des 14-tägigen Newsletters GI-Radar.

▸**Prof. Dr. Thomas Herrmann** ist seit 2004 Professor für Informations- und Technikmanagement am Institut für Arbeitswissenschaft der Ruhr-Universität Bochum. Er ist Mitglied der Fakultät für Elektro- und Informationstechnik und der Wirtschaftswissenschaftlichen Fakultät. Seine derzeitigen Forschungsinteressen befassen sich mit soziotechnischem Design im Bereich Wissens- und Prozessmanagement, Computerunterstützung von gemeinsamem Lernen, Kreativitätsförderung und Datenschutz. Er war Professor für Informatik und Gesellschaft von 1992 bis 2004 an der Universität Dortmund und dort Prorektor für Neue Medien und Infrastruktur von 2002 bis 2004. Zurzeit ist er Datenschutzbeauftragter der Ruhr-Universität Bochum und Mitglied von Paluno – The Ruhr Institute for Software Technology – an der Universität Duisburg-Essen.

▸**Johanna Hofmann, LL.M**, studierte Rechtswissenschaften an der Universität Potsdam. Wissenschaftliche Mitarbeiterin in Kanzleien in Berlin, Brüssel und Barcelona. 2012 Zweite Juristische Staatsprüfung in Berlin. 2014 LLM am King's College, London. Seit 2014 wissenschaftliche Mitarbeiterin in der

„Projektgruppe verfassungsverträgliche Technikgestaltung“ (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG). Mitarbeit in dem Projekt „Vertrauenswürdige Cloud-Services durch dynamische Zertifizierung qualitativer, datenschutzrechlitcher und sicherheitstechnischer Anforderungen: Next Generation Certification“ (NGCert). Seit 2015 ist sie Doktorandin an der Universität Kassel.

▸ **Charlotte Husemann** hat Rechtswissenschaften studiert. Seit 2015 ist sie Mitarbeiterin der „Projektgruppe verfassungsverträgliche Technikgestaltung“ (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) und arbeitet seit Januar 2017 in dem Projekt „Smart Environment, Smart Information?“. Sie ist Mitglied im „Forum Privatheit“.

▸ **Paul Johannes, LL.M.**, (EULISP) studierte Rechtswissenschaften und Informatik an der Friedrich Schiller Universität, der Leibniz Universität und der Queen Mary University. Seit 2009 ist er Rechtsanwalt mit den Tätigkeitsschwerpunkten IT-Recht und Datenschutzrecht, seit 2010 wissenschaftlicher Mitarbeiter in der „Projektgruppe verfassungsverträgliche Technikgestaltung“ (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG). Mitarbeit unter anderem in den Projekten BeLab, ProPrivacy und LiDaKrA. Seit Oktober 2017 ist er stellvertretender Geschäftsführer der Projektgruppe.

▸ **Prof. Dr. Doğan Kesdoğan** absolvierte seinen Master 1994 und wurde fünf Jahre später mit Auszeichnung promoviert. An der RWTH Aachen Universität habilitierte er 2007 im Bereich Computerwissenschaften. Berufserfahrung sammelte Kesdoğan als Sicherheitsexperte bei Mannesmann o.tel.o und als Gastforscher im Forschungszentrum IBM.T.J. Watson in den USA. Im Jahr 2002 war er als Gastdozent am Lehrstuhl von Prof. Tanenbaum für Computersysteme an der Vrije Universität in den Niederlanden. Außerdem war er von 2008 bis 2013 Lehrstuhlinhaber an der Universität Siegen für IT-Sicherheit und bekam eine außerplanmäßige Professur an der Universität für Wissenschaft und Technologie in Norwegen von 2007 bis 2013. Aktuell ist Kesdoğan Inhaber des Lehrstuhls für IT-Sicherheit an der Universität Regensburg.

▸ **Robin Knote** ist wissenschaftlicher Mitarbeiter und Doktorand am Fachgebiet Wirtschaftsinformatik der Universität Kassel. Während seiner Studienzeit (Informatik sowie IT-Management und -Consulting) war er in verschiedenen Softwareentwicklungs-, IT-Dienstleistungs- und Beratungsunternehmen, unter anderem bei Sopra Steria Consulting, PwC, Beiersdorf und QSC tätig. In seiner Dissertation erforscht er Lösungen zur Gestaltung kontextsensitiver Systeme, insbesondere smarter persönlicher Assistenten, im Spannungsfeld von Funktionalität, Qualität und Privatheit.

▸ **Prof. Dr. Martin Kutscha** ist Professor i. R. für Staats- und Verwaltungsrecht an der Hochschule für Wirtschaft und Recht Berlin. Er studierte von 1968 bis 1973 Rechtswissenschaft an den Universitäten Kiel, Marburg und Hamburg. Nach dem Referendariat, der Promotion an der Universität Bremen und dem Zweiten juristischen Staatsexamen 1977 war er als Rechtsanwalt, Redakteur einer juristischen Fachzeitschrift sowie als wissenschaftlier Mitarbeiter an der Universität Konstanz tätig. Von 1990 bis 2013 lehrte er an der Hochschule für Wirtschaft und Recht Berlin Staats- und Verwaltungsrecht. Seine Forschungsschwerpunkte sind Fragen des Grundrechtsschutzes, insbesondere in den Bereichen der Inneren Sicherheit, des Datenschutzes und des Beamtenrechts.

▸ **Patrick Lieser, M. Sc.**, hat nach seiner Ausbildung als Fachinformatiker für Systemintegration Informationssystemtechnik an der Technischen Universität Darmstadt studiert. Seit 2015 ist er wissenschaftlicher Mitarbeiter der Forschungsgruppe Distributed Sensing Systems am Fachgebiet Multimedia Kommunikation an der Technischen Universität Darmstadt. Er beschäftigt sich in seiner Forschung mit infrastrukturunabhängigen Kommunikationssystemen, welche im Katastrophenfall dabei helfen, Kommunikation in einem betroffenen Gebiet wiederherzustellen, sodass sich die Bevölkerung sowie die Einsatzkräfte koordinieren können.

▸ **Matthias Marx** studierte Informatik-Ingenieurwesen an der Technischen Universität Hamburg-Harburg. Er schloss seinen Master mit einer Arbeit über ein biometrisches Authentifizierungsverfahren ab. Seit 2016 arbeitet er als

wissenschaftlicher Mitarbeiter am Arbeitsbereich Sicherheit in verteilten Systemen bei Prof. Dr. Hannes Federrath an der Universität Hamburg. Dort forscht er im Rahmen des BMBF-Projekts AN.ON-Next an datenschutzfreundlichen Techniken, die in die Internet-Infrastruktur integriert werden, um zu ihrer massenhaften Verbreitung beizutragen. Bei der Initiative Freifunk Hamburg engagiert er sich seit 2012 für freie Netzwerke.

▸**Tobias Meuser, M. Sc.**, studierte Wirtschaftsinformatik an der Fernuniversität Hagen und Informatik an der Technischen Universität Darmstadt. Seit 2017 arbeitet er als wissenschaftlicher Mitarbeiter der Forschungsgruppe Distributed Sensing Systems am Fachgebiet Multimedia Kommunikation der Technischen Universität Darmstadt. Er beschäftigt sich in seiner Forschung mit der Informationsbewertung in verteilten Sensorsystemen. Diese Bewertung kann helfen, wichtige Informationen in verteilten Netzwerken zu priorisieren und so die Netzqualität in verschiedensten Szenarien zu verbessern. Beispiele für solche Szenarien sind Katastrophensituationen und Fahrzeugnetzwerke.

▸**Fabian Pittroff** hat Politische Theorie, Literatur- und Kulturwissenschaften studiert. Er arbeitet seit 2014 am Fachgebiet Soziologische Theorie der Universität Kassel. Seine Forschungsschwerpunkte sind Selbsttechnologien, Kontroversenkartografie und die Zukunft der Privatheit.

▸**Andreas Poller** arbeitet seit 2006 am Fraunhofer Institut SIT und bereits seit 2001 in der Fraunhofer Gesellschaft, vor 2006 im Bereich der künstlichen Intelligenz und maschinellen Bildverarbeitung. Er schloss 2006 sein Studium der Angewandten Informatik an der TU Chemnitz ab. Seine Tätigkeitsschwerpunkte am SIT sind Sicherheitsanalysen von IT-Systemen und -Prozessen, Forschung an Verfahren zur sicheren Softwareentwicklung, organisationswissenschaftliche Aspekte von IT-Sicherheit in der Softwareentwicklung und Privatsphärenschutz in Soziale-Netzwerke-Plattformen.

▸**Martin Rost** arbeitet beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. Er ist der Erfinder der Standard-Datenschutzmethodik, die von den deutschen Datenschutzaufsichtsbehörden, mit Ausnahme des LDA Bayern, im November 2016 als Methode zur Prüfung und Beratung verabschiedet wurde.

▸**Christian Roth, M.Sc.**, ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik IV (IT-Sicherheitsmanagement) von Prof. Dr. Doğan Kesdoğan an der Universität Regensburg. Dort betreut er mehrere Lehrveranstaltungen im Bachelor und Master. Inhaltlich beschäftigt er sich Rahmen des vom BMBF geförderten Projekts „Anonymität Online der nächsten Generation“ (AN.ON-Next) mit Konzepten zur datenschutzfreundlichen Gestaltung von Internet-Serviceangeboten, insbesondere im Kontext der zukünftigen Generation des Mobilfunks 5G. Ferner unterstützt er das AN.ON-Next Projekt organisatorisch. Zuvor hat er an der Universität Regensburg Wirtschaftsinformatik mit dem Schwerpunkt IT-Sicherheit studiert.

▸**Robert Rothmann** studierte Soziologie an der Universität Wien. Spezialisierung in Rechts- und Kriminalsoziologie. Wissenschaftlicher Mitarbeiter in verschiedenen interdisziplinären Forschungsprojekten an der Schnittstelle Technik/Recht/Gesellschaft. Seit 2014 ist er PhD Fellow am Institut für Staats- und Verwaltungsrecht, Juridicum, Wien.

▸**Fabian Schaller, LL.M.**, studierte Wirtschaftsrecht an der Hochschule Pforzheim und an der Universität Kassel. Anschließend arbeitete er als Juristischer Referent bei der Steuerberaterkammer München. Seit 2015 ist er wissenschaftlicher Mitarbeiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG). Dort arbeitet er im Projekt „Notfall-Kommunikationsnetze auf Basis von Mobiltelefonen (smarter), das vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Programms „Forschung für die zivile Sicherheit 2012 – 2017“ gefördert wird.

Eva Schedel ist wissenschaftliche Mitarbeiterin am Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Dort befasst sie sich in den vom Bundesministerium für Bildung und Forschung geförderten Projekten „Anonymität Online der nächsten Generation“ (AN.ON-Next) und „Datenschutzfreundliche Smartphone-Anwendungen ohne Kompromisse“ (AppPETs) mit datenschutzrechtlichen Fragen und Konzepten für Privacy by Design einschließlich Fragen des Privacy Behavior. An den Universitäten Würzburg, Aarhus/DK und Hannover hat sie Rechtswissenschaften mit Schwerpunkt Rechtsinformatik und darüber hinaus Psychologie studiert.

▸ **Eva Schlehahn** ist Juristin des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein (ULD). Zuvor hat sie eine Fachanwaltsausbildung im Bereich IT-Recht absolviert und war als Rechtsanwältin in Flensburg tätig. Im ULD ist sie 2010 im Projektbereich tätig und hat seitdem verschiedene von der Europäischen Kommission geförderte Forschungsprojekte juristisch betreut. Ihre Forschungsarbeit unter anderem über datenschutzrechtliche Fragen von Big Data, Cloud Computing, Identitätsmanagement, UI/UX Design, IT Sicherheit und Überwachungstechnologien verfolgt einen interdisziplinären Ansatz, um Anforderungen aus Datenschutzrecht, Ethik und Technik effektiv zusammen zu bringen.

▸ **Philip Schütz, M.A.**, geboren und aufgewachsen in Berlin, studierte Politikwissenschaft, Anglistik und Rechtswissenschaften an der Universität Heidelberg und am Institut d’Etudes Politiques Lille, Frankreich mit Abschluss 2009 als Magister Artium. Von 2010 bis 2017 arbeitete er als wissenschaftlicher Mitarbeiter im Competence Center Neue Technologien am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe mit dem thematischen Schwerpunkt Datenschutz und Privatheit. Zudem ist er Doktorand am Seminar für Politikwissenschaft der Universität Göttingen (Promotionsthema: Datenschutzbehörden im internationalen Vergleich) und seit Mai 2017 Datenschutzkoordinator bei dm-drogerie markt.

▸ **Dr. Sebastian Stein** ist seit 2016 wissenschaftlicher Mitarbeiter und EPG-Dozent am Internationalen Zentrum für Ethik in den Wissenschaften in Vertretung von PD Dr. Julia Dietrich, Universität Tübingen, Deutschland. 2016 war er Dozent und wissenschaftlicher Mitarbeiter bei Prof. Dr. Anton Friedrich Koch, Lehrstuhl für theoretische Philosophie an der Ruprecht-Karls-Universität Heidelberg, Deutschland. 2012 war Stein Promotionsstudent im Fach politische Theorie, Thema: Hegels Begriff des freien Willens, Betreuer Michael Inwood, an der University of Oxford, Großbritannien.

▸ **Barbara Stoeferle** studierte Technische Informatik an der Hochschule Ulm und absolvierte dort eine der ersten Ausbildungen zur geprüften Datenschutzbeauftragten. Seit 1997 ist sie als Datenschutzberaterin und –beauftragte bei dsm-s GmbH tätig und betreut kleinere Krankenhäuser und Maximalversorger. Weiterhin ist sie an verschiedenen Hochschulen Lehrbeauftragte für Datenschutz. Barbara Stoeferle ist Gründungs- und Ehrenmitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. Sie arbeitet aktiv im Ausschuss Berufsbild an der Weiterentwicklung des beruflichen Leitbildes des DSB mit. Desweiteren ist sie Sprecherin des Arbeitskreises Medizin des BvD sowie Mitglied der RG Ulm.

▸ **Laura Friederike Thies, MLE.**, ist wissenschaftliche Mitarbeiterin im Projekt AnEkA (Anforderungs- und Entwurfsmuster zur rechtsverträglichen und qualitätszentrierten Gestaltung kontextsensitiver Applikationen) in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel unter der Leitung von Prof. Dr. Alexander Roßnagel. Sie hat Rechtswissenschaften an der Georg-August-Universität Göttingen, der Universität Coimbra und der Humboldt-Universität zu Berlin studiert.

▸ **Sven Türpe** ist Wissenschaftler am Fraunhofer-Institut SIT und beschäftigt sich dort mit der Schnittstelle von IT-Sicherheit, Softwaretechnik und Entwicklungsarbeit. Ausgehend von der Frage, wie Sicherheitseigenschaften in der Softwareentwicklung gestaltet werden, untersucht er insbesondere die Wechselwirkung von Sicherheitsanforderungen mit anderen Gestaltungs-

dimensionen, die Rolle von Plattformen und Programmierschnittstellen sowie die Organisation und Steuerung von Entwicklungsvorgängen in Unternehmen. Daneben beschäftigt er sich mit ihren Konsequenzen sowie mit Fragen des Datenschutzes.

▸ **Maximilian von Grafenstein, LL.M.**, ist Leiter des Forschungsprogramms „Akteure, Daten und Infrastrukturen" am Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG), Partner der Rechtsanwaltsanwaltskanzlei iRights.Law und Gründer des Legal Tech Startups „Innovation and Law". Max' Forschungsschwerpunkt liegt im Bereich der Governance datengetriebener Innovation. In den letzten vier Jahren leitete er die HIIG Startup Law Clinic, in der er über 100 Startup-Unternehmern bei der Lösung rechtlicher Fragen in Hinsicht auf ihre Produkt- und Geschäftsmodellinnovationen unterstützte.

Weitere Beteiligte

A-Z

- ▸ **Nadine Absenger**
- ▸ **Johannes Caspar**
- ▸ **Michael Friedewald**
- ▸ **Christian Geminn**
- ▸ **Marit Hansen**
- ▸ **Jessica Heesen**
- ▸ **Thomas Hess**
- ▸ **Achim Klabunde**
- ▸ **Michael Kreutzer**
- ▸ **Konstantin von Notz**
- ▸ **Thilo Weichert**

▶ **Dr. Nadine Absenger** ist seit 1. September 2017 Leiterin der Abteilung Recht beim DGB Bundesvorstand in Berlin. Von Januar 2012 bis August 2017 war sie Leiterin des Referats Arbeits- und Sozialrecht im Wirtschafts- und Sozialwissenschaftlichen Institut (WSI) der Hans-Böckler-Stiftung in Düsseldorf, von Mai bis August 2017 zudem kommissarische Abteilungsleitung des WSI. Darüber hinaus ist Frau Dr. Absenger Lehrbeauftragte für Koalitions-, Tarif- und Arbeitskampfrecht an der Juristischen Fakultät der Heinrich-Heine-Universität Düsseldorf sowie Rechtsanwältin in einer Wuppertaler Rechtsanwaltskanzlei.

▶ **Prof. Dr. Johannes Caspar** wurde 1992 nach dem Ersten juristischen Staatsexamen zum Dr. jur. an der Fakultät für Rechtswissenschaften der Universität Göttingen mit einer Dissertation zur Rechts- und Staatsphilosophie Jean-Jacques Rousseaus promoviert. 1999 erfolgte die Habilitation für die Fächer „Staatsrecht, Verwaltungsrecht und Rechtsphilosophie". Von 1999 bis 2000 hatte er eine Vertretungsprofessur an der Universität Marburg inne und war als Rechtsanwalt tätig. Danach war er unter anderem stellvertretender Leiter des Wissenschaftlichen Dienstes im Schleswig-Holsteinischen Landtag. 2009 wurde er zum Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ernannt; seine Wiederwahl erfolgte im Jahr 2015.

▶ **Dr. Michael Friedewald** leitet das Geschäftsfeld „Informations- und Kommunikationstechnik" am Fraunhofer Institut für System- und Innovationsforschung ISI in Karlsruhe. Er studierte Elektrotechnik, Wirtschaftswissenschaften und Technikgeschichte an der Rheinisch-Westfälischen Technischen Hochschule Aachen. Er beschäftigt sich mit Voraussetzungen, Prozessen und Folgen des technischen Wandels vor allem im Bereich IKT. Er ist Koordinator des vom BMBF geförderten Projekts „Forum Privatheit".

▶ **Dr. Christian Geminn** ist Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel. Er studierte Rechtswissenschaften in Mainz und Leicester und wurde 2013 mit seiner Dissertationsschrift „Rechtsverträglicher Einsatz von Sicherheitsmaßnahmen im öffentlichen Verkehr" promoviert. Er ist Mitglied im „Forum Privatheit".

▶ **Marit Hansen** ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das Unabhängige Landeszentrum für Datenschutz (ULD). Davor war die Diplom-Informatikerin sieben Jahre lang stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein. Im ULD hat sie den Bereich der Projekte für technischen Datenschutz aufgebaut. Die gesellschaftlichen Herausforderungen, die aus der zunehmenden Digitalisierung resultieren, betrachten und bearbeiten Frau Hansen und ihr Team interdisziplinär und in Kooperation mit Forschung und Wissenschaft. Seit 1995 arbeitet Frau Hansen zu Themen des Datenschutzes und der Informationssicherheit. Ihr Schwerpunkt liegt auf der grundrechtskonformen Gestaltung von Systemen, insbesondere durch Datenschutz „by Design" und „by Default". Sie ist Mitglied im „Forum Privatheit".

▶ **PD Dr. Jessica Heesen** ist Leiterin einer Nachwuchsforschungsgruppe zur Medien- und Informationsethik am Internationalen Zentrum für Ethik in den Wissenschaften der Universität Tübingen. Nach einem Magisterabschluss der Philosophie beschäftigte sie sich im Schwerpunkt mit technikphilosophischen und ethischen Fragen einer Gesellschaft im digitalen Wandel. Derzeit stehen insbesondere die Konzepte „Solidarität" und „gesellschaftliche Integration" in Bezug auf informationstechnische Innovationen im Vordergrund der Forschung. Sie ist Mitglied im „Forum Privatheit".

▶ **Prof. Dr. Thomas Hess** ist seit 2001 Universitätsprofessor für Betriebswirtschaftslehre und Wirtschaftsinformatik sowie Direktor des Instituts für Wirtschaftsinformatik und neue Medien der Ludwig-Maximilians-Universität München. Seit 2003 ist er Mitglied im Board des Center for Digital Technology and Management (CDTM) von LMU München und TU München. Er koordiniert seit 2005 das Zentrum für Internetforschung und Medienintegration (ZIM) an der LMU München, als Co-Vorstand des Internet Business Clusters München e.V. ist er seit 2011 aktiv. Der langfristige Forschungsschwerpunkt von

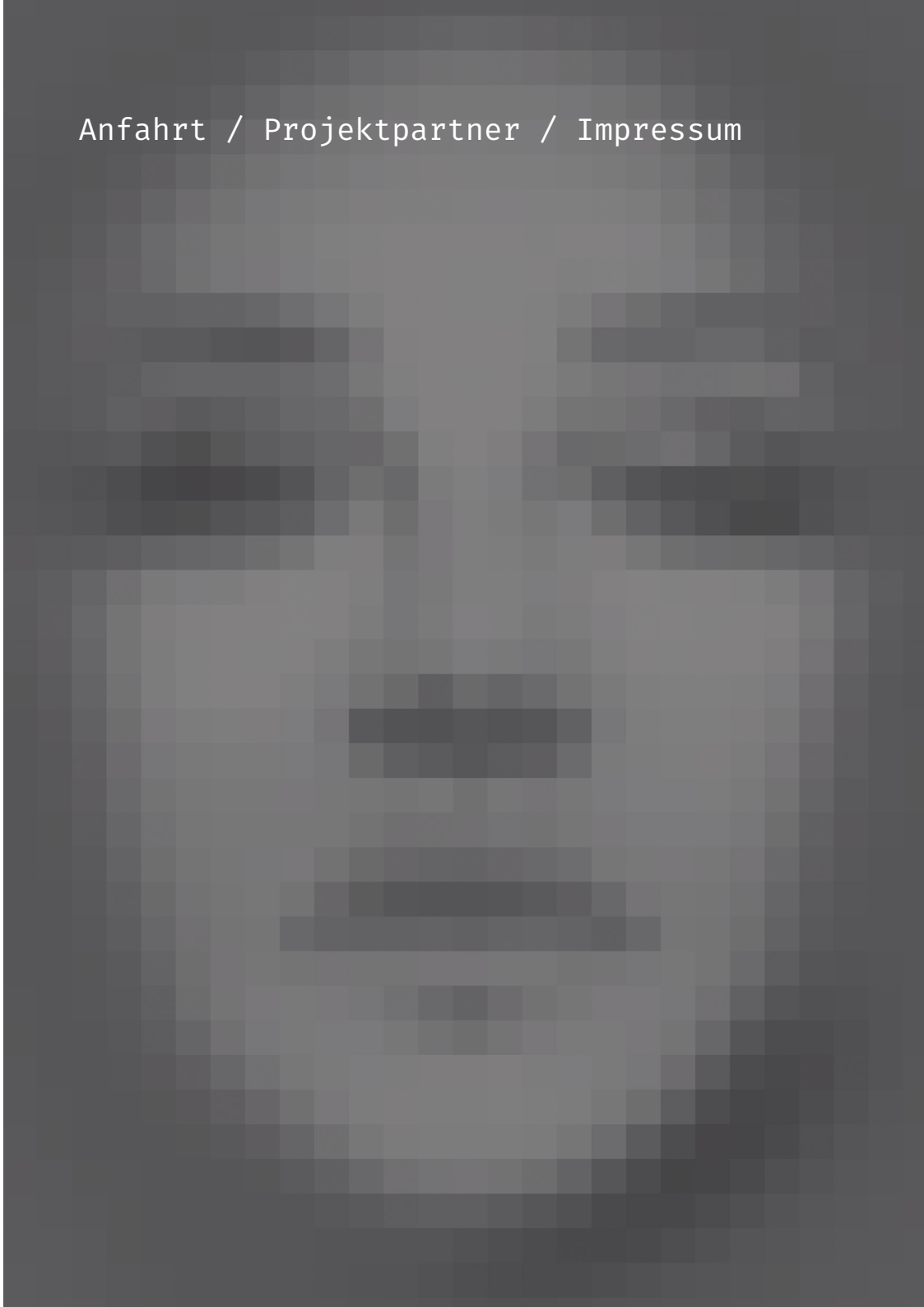
Thomas Hess liegt in unternehmerischen Aspekten der Bereitstellung und Nutzung digitaler Technologien. Sein methodischer Fokus konzentriert sich auf großzahlig empirische Arbeitsweisen, ergänzt durch gestaltungsorientierte Forschung sowie formale Kalküle. Er ist Mitglied im „Forum Privatheit".

▶ **Dr. Michael Kreutzer** ist Diplom-Informatiker (Universität des Saarlandes). Nach dem Studium arbeitete er als IT-Consultant in Luxemburg. Anschließend war er Berater für Distributed Object Computing in Freiburg. Er promovierte an der Universität Freiburg im Bereich robuster Dienstfindung von infrastrukturlos vernetzten IT-Systemen. Ab 2005 wurde er zum Koordinator der Darmstädter IT-Sicherheitsforschungszentren DZI, CASED und EC SPRIDE ernannt. Seit Ende 2015 ist Dr. Kreutzer verantwortlich für strategische Industriebeziehungen am Fraunhofer-Institut für Sichere Informationstechnologie SIT. Seit mehr als 15 Jahren publiziert er Forschungsarbeiten zum technischen Privatsphärenschutz. Er ist Mitglied im „Forum Privatheit".

▶ **Dr. Konstantin von Notz** ist seit 2009 gewähltes Mitglied des Deutschen Bundestags. Von 2009 bis 2013 war er innen- und netzpolitischer Sprecher, seit 2013 ist er stellvertretender Fraktionsvorsitzender und netzpolitischer Sprecher der Fraktion Bündnis 90/Die Grünen. Er studierte von 1993 bis 1998 Rechtswissenschaft an der Ruprecht-Karls-Universität Heidelberg und legte dort 1998 das erste Staatsexamen ab. Von 2001 bis 2004 war er Rechtsreferendar am Landgericht Lübeck und legte dort 2004 das zweite Staatsexamen ab. 2002 wurde er in Heidelberg mit einer Dissertation über Lebensführungspflichten im evangelischen Kirchenrecht zum Dr. jur. promoviert. Im Februar 2013 übernahm er im Rahmen des Programms „Parlamentarier schützen Parlamentarier" des Bundestagsausschusses für Menschenrechte und humanitäre Hilfe eine Patenschaft für den kubanischen Dissidenten Antonio Rodiles. Als Mitglied von Transparency International leitete er von 2006 bis 2008 die Regionalgruppe Hamburg und Schleswig-Holstein.

Dr. Thilo Weichert, Jurist und Politologe, ist Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e. V. (DVD). Von 2004 bis Juli 2015 war er Datenschutzbeauftragter von Schleswig-Holstein und damit Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD) in Kiel, zuvor stellv. ULD-Leiter. Davor war Weichert als Rechtsanwalt, Politiker, Hochschuldozent, Justiziar und Publizist in Freiburg/Breisgau, Stuttgart, Dresden und Hannover tätig. Von 1992 bis 1998 war er als Referent beim Landesbeauftragten für Datenschutz Niedersachsen, 1991 als Berater der Bürgerkomitees zur Auflösung der Staatssicherheit tätig.

Anfahrt / Projektpartner / Impressum



Anfahrt

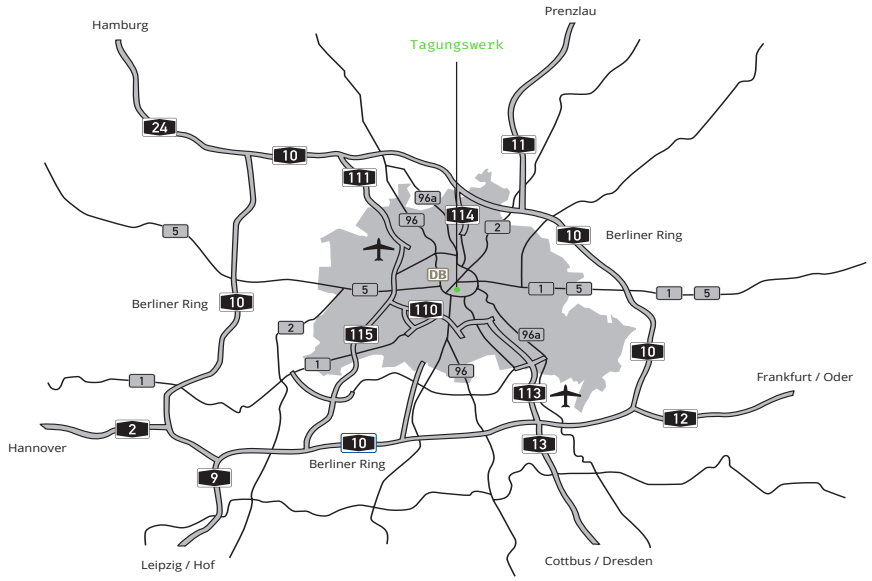
Tagungswerk
Lindenstr. 85
10969 Berlin

Anfahrt mit dem Auto aus Richtung Hannover/München

- von der A2/A9 auf den Berliner Ring (A10)
- am Dreieck Nuthetal auf die A115 Richtung Berlin-Zentrum
- am Dreieck Funkturm auf die A100 bis Ausfahrt Tempelhofer Damm, links abbiegen auf den Tempelhofer Damm, immer geradeaus auf den Mehringdamm
- rechts abbiegen auf das Tempelhofer Ufer, weiter geradeaus auf das Waterloo-Ufer
- links in die Lindenstraße einbiegen
- nach 800 Metern befindet sich links das Tagungswerk

Anfahrt mit dem Auto aus Richtung Hamburg/Rostock

- von der A24 auf den Berliner Ring (A10) Richtung Prenzlau, Frankfurt/Oder, Berlin Zentrum
- an der Ausfahrt Kurt-Schumacher-Platz auf die A105 Richtung Wedding
- links abbiegen auf den Kurt-Schumacher-Damm
- rechts abbiegen auf die Scharnweberstraße, geradeaus weiter auf die Müllerstraße, immer geradeaus, auf die Chausseestraße
- weiter geradeaus auf die Friedrichstraße, dann links abbiegen auf die Kochstraße
- rechts abbiegen in die Lindenstraße
- nach 200 Metern befindet sich rechts das Tagungswerk



Anfahrt mit dem Auto aus Richtung Frankfurt (Oder)/Dresden

- von der A12/A13 auf den Berliner Ring (A10) Richtung Berlin Zentrum
- am Schönefelder Kreuz auf die A113 Richtung Berlin Zentrum
- am Dreieck Treptow links auf die B96a/Am Seegraben, Richtung Flughafen Schönefeld
- rechts abbiegen auf die Waltersdorfer Chaussee (B179), immer geradeaus auf die Neuköllner Straße
- rechts abbiegen auf die Stubenrauchstraße
- links abbiegen auf die A113
- am Dreieck Neukölln auf die A100 Richtung Tempelhof
- rechts abbiegen auf den Tempelhofer Damm, immer geradeaus, dann auf den Mehringdamm
- rechts abbiegen auf das Tempelhofer Ufer
- weiter geradeaus auf das Waterloo-Ufer
- links in die Lindenstraße einbiegen
- nach 800 Metern befindet sich links das Tagungswerk

Anfahrt

Anfahrt mit öffentlichen Verkehrsmitteln

- U-Bahn: U6 bis Kochstraße, 5 Minuten Fußweg
- Bus: 248, M 29 bis Jüdisches Museum

Anfahrt mit dem Auto ab Flughafen Schönefeld (23 km, 35 Minuten)

- links in die Straße Am Seegraben, dann rechts in die Mittelstraße Richtung Berlin/Stadtmitte, geradeaus auf Am Seegraben
- links auf die Waltersdorfer Chausee (B179), weiter geradeaus auf die Neuköllner Straße
- rechts auf die Stubenrauchstraße
- links auf die A113 Richtung Neukölln/A100
- am Autobahndreieck Neukölln/Buschkrugallee links auf die A100 Richtung Hamburg/Tempelhof bis Ausfahrt Tempelhofer Damm
- links abbiegen auf den Tempelhofer Damm, geradeaus weiter auf den Mehringdamm
- rechts in das Tempelhofer Ufer
- weiter geradeaus auf das Waterloo-Ufer
- links in die Lindenstraße abbiegen
- nach 800 Metern befindet sich links das Tagungswerk

Anfahrt mit öffentlichen Verkehrsmitteln ab Flughafen Schönefeld (23 km, 35 Minuten)

- Regionalexpress RE 7 (Richtung Dessau), Regionalbahn RB 14 (Richtung Nauen) bis Friedrichstraße
- U6 (Richtung Alt-Mariendorf) bis Kochstraße
- 5 Minuten Fußweg

- Bus SXF1 (Richtung Südkreuz) bis Südkreuz
- Bus 248 (Richtung Ostbahnhof) bis Jüdisches Museum

Anfahrt mit dem Auto ab Flughafen Tegel (20 Km, 30 Minuten)

- auffahren auf A111 Richtung Zentrum, dann weiter auf A100 Richtung Wilmersdorf bis Ausfahrt Tempelhofer Damm
- links abbiegen auf den Tempelhofer Damm, geradeaus weiter auf den Mehringdamm
- rechts in das Tempelhofer Ufer
- weiter geradeaus auf das Waterloo-Ufer
- links in die Lindenstraße einbiegen
- nach 800 Metern befindet sich links das Tagungswerk

Anfahrt mit öffentlichen Verkehrsmitteln ab Flughafen Tegel

- Bus 128 bis Kurt-Schumacher-Platz
- U6 (Richtung Alt-Mariendorf) bis Kochstraße
- 5 Minuten Fußweg

Projektpartner

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Fraunhofer

UNIKASSEL VERSITÄT

Eberhard Karls Universität Tübingen | Internationales Zentrum für Ethik in den Wissenschaften (IZEW)

Universität Duisburg-Essen

LMU Ludwig-Maximilians-Universität München

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Gefördert vom
Bundesministerium für Bildung und Forschung BMBF

Projektpartner
Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe

Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt

Fachgebiet Soziologische Theorie an der Universität Kassel

Universität Tübingen
Internationales Zentrum für Ethik in den Wissenschaften (IZEW)

Universität Duisburg-Essen, Fachgebiet Sozialpsychologie

Ludwig-Maximilians-Universität München, Institut für Wirtschaftsinformatik und neue Medien

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel

Impressum

Herausgeber
Fraunhofer-Institut für
System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

Kontakt
Michael Friedewald
Geschäftsfeldleiter Informations- und Kommunikationstechniken
Tel.: +49 721 6809–146
Fax: +49 721 6809–315
info@forum-privatheit.de

Fraunhofer-Institut für
System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Redaktion
Barbara Ferrarese
Michael Friedewald

Grafische Gestaltung
Sabine Wurst

Realisation
Jeanette Braun

Fotoarbeit
shutterstock.com/Anna Ismagilova

Druck
Stober GmbH
Druck und Verlag, Eggenstein