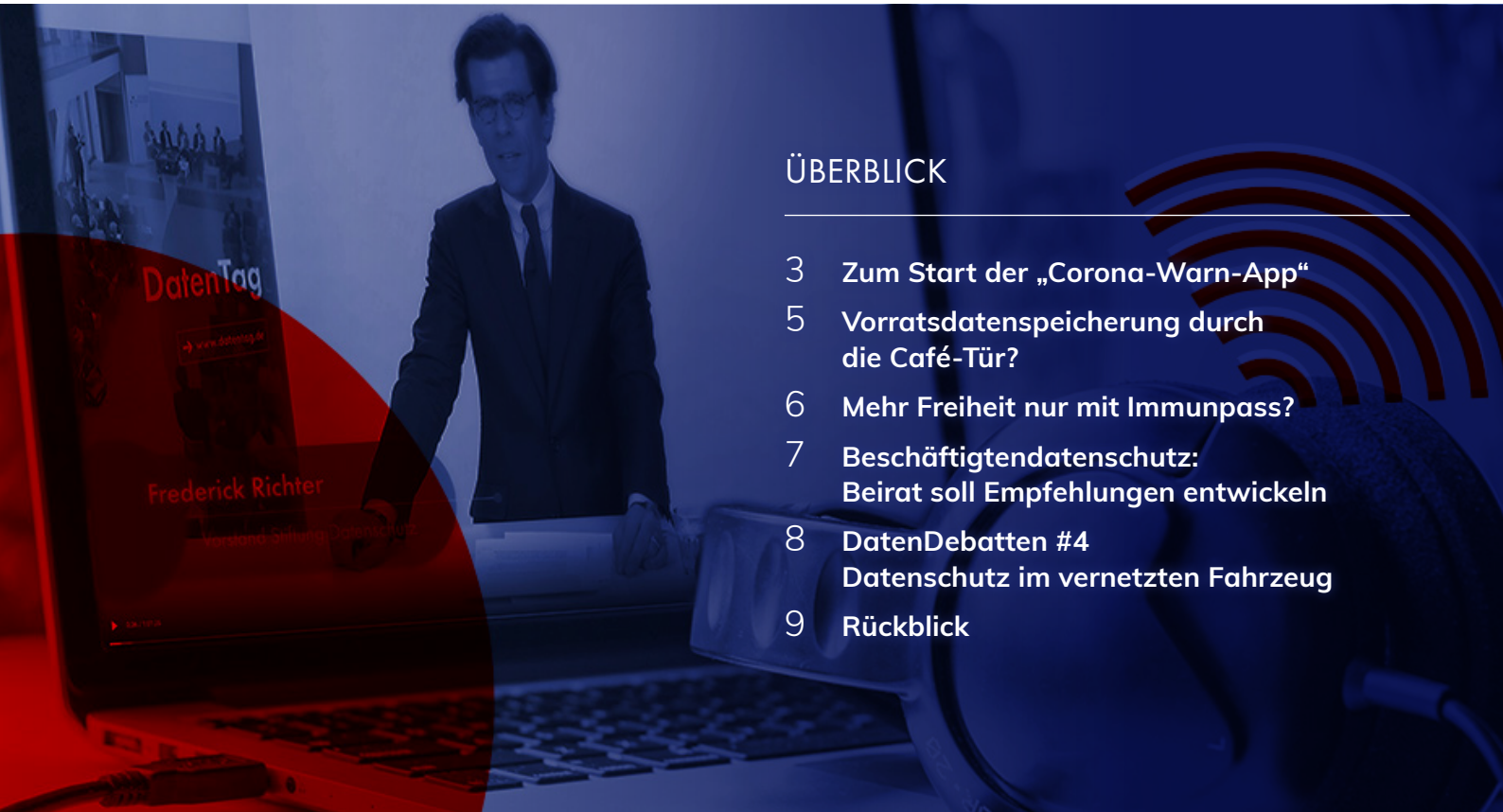
STIFTUNG DATENSCHUTZ

POLITIKBRIEF – SOMMER 2020

CORONA-WARN-APP, IMMUNITÄTSPASS…

DATENSCHUTZ IN DER PANDEMIE



ÜBERBLICK

Liebe Leserinnen und Leser,

kurz vor der parlamentarischen Sommerpause meldet sich noch einmal die Stiftung Datenschutz bei Ihnen. Turbulente Wochen und Monate liegen hinter Ihnen, hinter uns allen. Die Pandemie hat alles erschüttert. Auch für Datenschutz und Datenpolitik brachte sie viele Diskussionspunkte und kritische Themen: Welche Institutionen sollten in Krisenlagen auf welche Gesundheitsdaten der Bevölkerung zugreifen können? Welche Datensammlungen sind wirklich notwendig, um bei Bedarf Infektionsketten nachverfolgen zu können? Was müssen Bildungsträger und die dort handelnden Personen beachten, wenn sie plötzlich Lerninhalte digital vermitteln sollen? Die Geschwindigkeit, mit der auch die indirekten Auswirkungen der Pandemie die Gesellschaft erreichten, zwang zu schnellen Reaktionen – und nicht immer konnten die gewählten Lösungen mit den hohen Ansprüchen des Datenschutzes mithalten. So spielten beim plötzlichen Umzug an Heimarbeitsplätze und Online-Schulen Datensicherheit und Datenschutz zunächst eine untergeordnete Rolle. BüroarbeiterInnen, Eltern und Lehrerschaft taten ihr Bestes in einer beispiellosen Situation, leider oft ohne ausreichende Unterstützung von Arbeitgebern und Schulbehörden. Hoffen wir, dass der erwartete Schub Richtung Digitalisierung auch ein Schub zu mehr Datenbewusstsein ist.

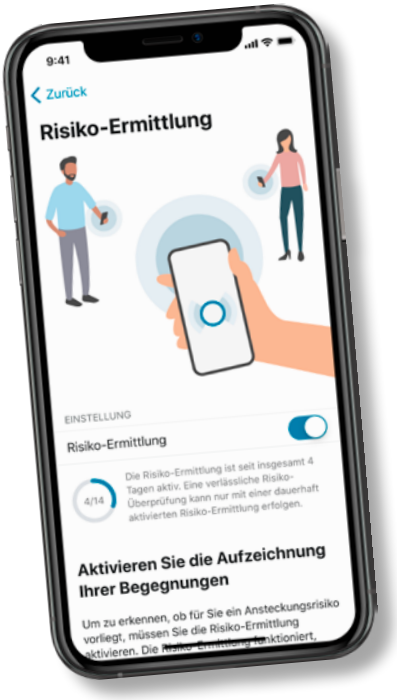
Größerer Sensibilität bedarf es auch, wenn es darum geht, mit Daten Vorsorge zu treffen. In den meisten Bundesländern müssen Gastronomiebetriebe derzeit viele Daten ihrer Gäste einsammeln, bevor sie diese bewirten dürfen. Damit soll die Möglichkeit für Gesundheitsbehörden geschaffen werden, bei Infektionen Nachforschungen anzustellen. Wir sehen den Sinn dieser Verordnungen, aber wir hätten uns sehr gefreut, wenn in den Bundesländern zunächst überlegt worden wäre, welche Daten hier wirklich benötigt werden – sämtliche Kontaktdaten aller Gäste oder nur Daten zur schnellen Erreichbarkeit einer Person pro Gruppe? Was die in dieser Woche gestartete Corona-Warn-App betrifft, so sehen wir uns bestätigt: Es geht nicht ohne Transparenz und Freiwilligkeit. Beides ist mit dem vorliegenden Konzept nun gegeben, sodass es auch aus Sicht des Datenschutzes keiner grundsätzlichen Kritik mehr bedarf und die App auch seitens der Stiftung Datenschutz empfohlen werden kann. Zu hoffen ist jetzt, dass breites Vertrauen hergestellt werden kann, auf dass die Zahl der Nutzenden so groß werde, dass der verfolgte Ansatz der App auch funktioniert.

Alles Gute wünscht

Frederick Richter, Vorstand der Stiftung Datenschutz

ZUM START DER „CORONA-WARN-APP“

In der vergangenen Ausgabe unseres Politikbriefs hatten wir verschiedene Aspekte der Idee beleuchtet, mit Hilfe von Smartphone-Apps die Kontakte von positiv getesteten Personen nachzuvollziehen. Dass hier erhebliches Missbrauchspotenzial besteht, liegt auf der Hand. Konzepte, die auf GPS-Daten oder Funkzellenabfragen beruhten, waren schnell vom Tisch: Zu tief wäre der Eingriff in die Privatsphäre, zu schwierig die technische Umsetzung gewesen.

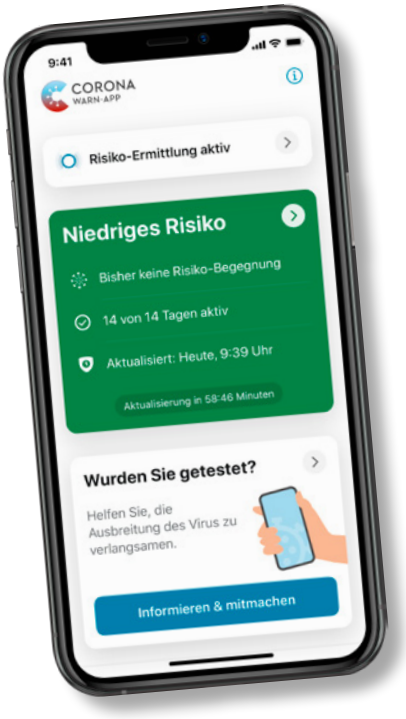


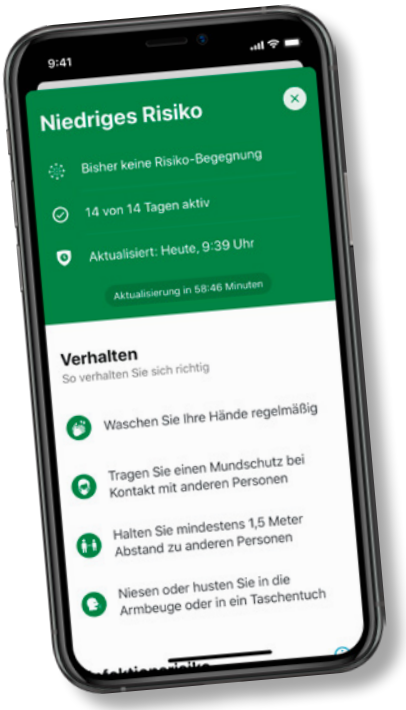
Zunächst erschien aus Sicht des Datenschutzes das Konzept PEPP-PT prinzipiell und unter bestimmten Voraussetzungen als ein guter Beitrag im Rahmen eines Gesamtkonzepts. Zu diesen Bedingungen gehörte ein vertrauenswürdiger Betreiber, denn die anfallenden Daten sollten dort zentral gespeichert werden, woraus sich die Gefahr missbräuchlicher Zugriffe ergeben kann. Dagegen wandten sich Mitte April mehr als 300 Wissenschaftlerinnen und Wissenschaftler von angesehenen Einrichtungen, darunter mehr als fünfzig aus Deutschland, in einem offenen Brief[1]: „Auch wenn die Wirksamkeit von Apps zur Ermittlung von Kontaktpersonen umstritten ist, wir müssen sicherstellen, dass die umgesetzten Maßnahmen die Privatsphäre ihrer Nutzer wahren und es so unmöglich machen, die Daten für ungerechtfertigte Diskriminierung und Überwachung zu missbrauchen. … Es ist von entscheidender Bedeutung, dass wir, um die gegenwärtige Krise zu überwinden, nicht ein Instrument schaffen, das eine groß angelegte Datenerhebung über die Bevölkerung ermöglicht, weder jetzt noch zu einem späteren Zeitpunkt.“

In diesem Sinn wandten sich kurz darauf mehrere Organisationen – darunter auch die Stiftung Datenschutz – an Kanzleramtsminister Helge Braun und Gesundheitsminister Jens Spahn mit der Bitte, die zwischenzeitlich bekannt gewordene Vorentscheidung für den zentralen Ansatz noch einmal zu überdenken: „Eine App, die zumindest eine Aussicht auf Erfolg haben soll, muss ein transparentes Konzept verfolgen, quelloffen programmiert werden, auf zentrale Datenspeicherung verzichten und die Anonymität der Nutzerinnen und Nutzer so weitgehend wie möglich schützen.“

Und das taten die beiden Minister – und erklärten am 26.4.: Die Nutzung der App durch möglichst große Teile der Bevölkerung sei die Grundlage ihres Erfolges. „Um dieses Ziel zu erreichen, setzt die Bundesregierung auf eine dezentrale Softwarearchitektur, die die in Kürze zur Verfügung stehenden Programmierschnittstellen der wesentlichen Anbieter von mobilen Betriebssystemen nutzt und gleichzeitig die epidemiologische Qualitätssicherung bestmöglich integriert.“ Gemeint ist die von Google und Apple gemeinsam entwickelte Schnittstelle in den Betriebssystemen Android und iOS. Auf deren Basis können nun individuelle Apps entwickelt werden – Voraussetzung dafür, dass die Apps bald auch in den europäischen Nachbarländern funktionieren.

1 https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view





In Deutschland haben Telekom und SAP die „Corona-Warn-App“ entwickelt[2] und den Quellcode veröffentlicht[3], damit unabhängige Experten ihn auf Fehler und Schwächen überprüfen können. Bislang ist die Resonanz sehr positiv; aus Datenschutz- und Datensicherheits-Aspekten scheint derzeit nichts dagegen zu sprechen, die App zu installieren. Die App ist in dieser Woche erschienen, begleitet von einer breiten Kampagne des Presse- und Informationsamts der Bundesregierung, das auch bei zahlreichen zivilgesellschaftlichen Organisationen, Wirtschaftsverbänden und anderen Einrichtungen des öffentlichen Lebens um Unterstützung wirbt. Die ist auch dringend nötig, weil viele Menschen noch immer Sorge haben, durch die App überwacht zu werden.

Derzeit wird in der Netzpolitik intensiv diskutiert, ob es ein Begleitgesetz für die Corona-Warn-App geben soll, wie in Australien oder der Schweiz, nachdem eine Gruppe von Expertinnen und Experten einen entsprechenden Entwurf[4] vorgelegt hatte. Das Gesetz soll sicherstellen, dass die Nutzung der App nur freiwillig erfolgen kann, dass so wenig wie möglich Daten erfasst und zum frühestmöglichen Zeitpunkt wieder gelöscht werden; dass ein Zugriff durch Dritte ausgeschlossen bleibt und dass niemandem Vor- oder Nachteile aus einer Nutzung bzw. Nicht-Nutzung entstehen können. Der Bundesdatenschutzbeauftragte hält ein solches Gesetz nicht für zwingend erforderlich, wie er in einem Brief[5] an das Bundesgesundheitsministerium darlegt, weil ohne Gesetz die Datenschutzgrundverordnung greife und damit alle Rechte für die betroffenen Personen sowie das Verbot der Weitergabe und der nicht zweckgebundenen Nutzung. Eine wie auch immer erzwungene Einwilligung in die Installation und Nutzung der App wäre nicht freiwillig und daher nach dem Datenschutzrecht auch unwirksam.

Wie viel Vertrauen die Bevölkerung in die Corona-Warn-App setzt und wie hilfreich sie bei der Bekämpfung der Pandemie ist, wird sich erst in den kommenden Monaten zeigen. Schon jetzt ist aber die Geschichte der Corona-Warn-App ein Exempel dafür, dass der oft als Hindernis geschmähte Datenschutz Menschen und ihre Grundrechte schützt. Dazu hat das persönliche Engagement vieler Expertinnen und Experten beigetragen und die Bereitschaft von Politikern, deren Stimme zu hören.

2 https://www.coronawarn.app/de/
3 https://github.com/corona-warn-app
4 https://www.malteengeler.de/wp-content/uploads/2020/05/Vorschlag-fu%CC%88r-ein-Gesetz-zur-Einfu%CC%88hrung-und-zum-Betrieb-einer-App-basierten-Nachverfolgung-von-Infektionsrisiken-mit-dem-Corona-Virus-Version-1.0.pdf
5 https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/Schreiben-an-BMG_Corona-App-Gesetz.pdf

VORRATSDATENSPEICHERUNG DURCH DIE CAFÉ-TÜR?

Wenig Vertrauen einflößend ist dagegen der föderale Flickenteppich von Anordnungen, welche Daten von Gästen jeweils in den wieder geöffneten Cafés und Restaurants erfasst werden sollen: Namen ja, aber auch Adressen? Oder reicht die Telefonnummer? Von allen am Tisch oder nur von einer Person? Trägt man sich in eine lange Liste ein oder auf einen einzelnen Zettel? Wie lange sind die Listen aufzubewahren und wie vor unbefugtem Zugriff zu schützen?

So viele Vorteile der Föderalismus bringt, so wenig sinnvoll sind hier die zahlreichen, im Detail verschiedenen Vorschriften. Hoffen wir, dass wir in einigen Monaten besser wissen, was sinnvoll ist. Denn dass diese Datensammlung das „neue Normal“ sein wird, scheint auf absehbare Zeit sicher. Aus Sicht des Datenschutzes geht es vor allem um das „Wie“ solcher Maßnahmen. Es ist nämlich nicht erforderlich und damit unverhältnismäßig, wenn viele Bundesländer sämtliche Gäste verpflichten, ihre kompletten Kontaktdaten für mehrere Wochen in allen besuchten Lokalen zu hinterlassen. Anstatt sowohl Name und Anschrift als auch elektronische Kontaktdaten und Telefonnummer abzufragen, reicht es für eine – bestenfalls – zeitnahe Ansprache durch Gesundheitsämter vollkommen aus, wenn von Besucherinnen und Besuchern der Gastronomie lediglich ein Kontaktdatum nach Wahl zur schnellen Erreichbarkeit abgefordert wird. In dieser Richtung sollten die Landesverordnungen nachjustiert werden. Auch verstärkte Aufklärung der Wirte und Betreiberinnen zum richtigen Umgang mit den eingesammelten Bürgerdaten muss stattfinden, damit nicht – wie bereits geschehen – private Telefonnummern auf offenen Listen für alle einsehbar herumliegen.

MEHR FREIHEIT NUR MIT IMMUNPASS?

Bundesgesundheitsminister Jens Spahn hält die Einführung von sogenannten Immunitätsausweisen für sinnvoll und erforderlich. Dies soll durch einen zusätzlichen Eintrag im Impfpass realisiert werden. Damit können Menschen, die eine COVID-19-Erkrankung überstanden haben und immun sind, ihren Gesundheitsstatus dokumentieren. Sie können (wahrscheinlich) nicht mehr erkranken und das Virus nicht übertragen und wären somit frei von Einschränkungen, denen andere zur Infektionsvermeidung unterliegen. Lässt man einmal unbeachtet, dass noch nicht klar ist, wie lange eine Immunität überhaupt anhält und dass rückwirkende Antikörper-Tests derzeit noch mit einer hohen Fehlerquote behaftet sind – wie ist ein solcher Ausweis unter Datenschutz-Aspekten zu bewerten?

Daten zur Gesundheit werden vom verfassungsmäßigen Recht auf informationelle Selbstbestimmung und von der Datenschutz-Grundverordnung besonders geschützt. Ein Immunitätsausweis erfordert es, den gesundheitlichen Status bekannt zu machen, um bestimmte Vorteile und größere Freiheiten zu erhalten. Das widerspricht dem Grundgedanken des Datenschutzes und ist geeignet, eine Tür zur Diskriminierung aufzustoßen. Diese würde insbesondere Angehörige von sogenannten Risikogruppen betreffen, die von bestimmten Freiheiten oder auch Tätigkeiten ausgeschlossen blieben. Auch der Bundesdatenschutzbeauftragte sieht die Gefahr einer missbräuchlichen Verwendung[6] und hält die Mitteilung des Immunstatus nur in gesetzlich geregelten Fällen für zulässig.

Insgesamt ist ein solcher Ausweis (bzw. Eintrag in den Impfausweis) geeignet, das so dringend benötigte Vertrauen in den Schutz von Gesundheitsdaten zu beschädigen.

Derzeit beschäftigt sich der Deutsche Ethikrat auf die Bitte von Minister Spahn hin mit der Thematik und möchte bis zur parlamentarischen Sommerpause eine Stellungnahme vorlegen. Eine breite gesellschaftliche Debatte zu diesem sensiblen Thema wäre zu begrüßen.

6 https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_zweites-Gesetz-Schutz-bei-epidemischer-Lage.pdf?__blob=publicationFile&v=2

BESCHÄFTIGTENDATENSCHUTZ: BEIRAT SOLL EMPFEHLUNGEN ENTWICKELN

Bewerbung, Gehalt, Urlaub, Krankheit – im Beschäftigtenverhältnis werden zahlreiche personenbezogene, oft auch besonders sensible Daten verarbeitet. Dennoch gibt es in Deutschland auch unter der DSGVO kein eigenes Gesetz, das den Schutz dieser Daten regelt. Dabei ist im Koalitionsvertrag vorgesehen, dass in dieser Legislatur endlich „Klarheit über Rechte und Pflichten der Arbeitgeberinnen und Arbeitgeber, der Arbeitnehmerinnen und Arbeitnehmer schaffen sowie die Persönlichkeitsrechte der Beschäftigten sicherstellen (Beschäftigtendatenschutz)“, wie es dort heißt.

Nun setzt das Bundesarbeitsministerium einen Beirat ein, der bis Jahresende Empfehlungen erarbeiten soll, wie der Schutz der Beschäftigten durchgesetzt werden kann. Ob es dazu tatsächlich ein eigenes Gesetz braucht, ist noch unklar.

Die Zusammensetzung des Beirats bezieht ganz unterschiedliche Perspektiven aus der Rechtswissenschaft und der Informatik, von Datenschutzexpertinnen sowie Wirtschafts- und Arbeitnehmervertretern ein. Die Wissenschaftliche Leiterin der Stiftung Datenschutz, Hochschulprofessorin und Datenschutzexpertin Anne Riechert ist ebenfalls in den Beirat berufen worden.

Unser Stiftungsvorstand Frederick Richter begrüßt die Initiative: „Es wird aber auch Zeit. Die Praxis seit der Umsetzung der DSGVO hat gezeigt, wie groß der Bedarf an klaren Regelungen ist. Gerade im Beschäftigungsverhältnis, das ja für die meisten Menschen Grundlage ihrer wirtschaftlichen Existenz ist, sind einige Fragen bislang ungeklärt und damit der Interpretation im Einzelfall durch Gerichte überlassen. Außerdem ergeben sich nicht erst seit der Corona-Pandemie aus der technischen Entwicklung immer neue Fragen, die weitere Herausforderungen für den Schutz von Arbeitnehmerdaten mit sich bringen.“

Kurzfristig ist jedenfalls nicht mit einem neuen Gesetz zu rechnen. Deshalb aktualisieren wir gerade unsere Handreichung „Beschäftigtendatenschutz“, die demnächst in einer erweiterten Version erscheinen wird. Darin haben wir die wichtigsten Punkte und Regeln zusammengetragen. Praxisnah und verständlich wenden wir uns damit in erster Linie an Personalverantwortliche in kleinen und mittelständischen Unternehmen, und ganz allgemein an Beschäftigte.

„Beschäftigtendatenschutz – eine Handreichung“ (PDF, 17 Seiten, für den Druck optimiert, mit Fallbeispielen)

→ **sds-links.de/BS-DS**

Die Handreichung „Beschäftigtendatenschutz“ ergänzt unsere Handreichung „Datenschutz im Betrieb“, ersetzt aber natürlich nicht den Austausch mit den betrieblichen Datenschutzbeauftragten.

→ **stiftungdatenschutz.org/dsgvo-broschueren**

Eine ausführlichere Version mit vielen Links zu Veröffentlichungen der Aufsichtsbehörden finden Sie auf unserer Informationsplattform und unter sds-links.de/Dossier-BS-DS.

→ **stiftungdatenschutz.org/dsgvo-info**

DATENDEBATTEN #4
DATENSCHUTZ IM VERNETZTEN FAHRZEUG

Wie sich Sicherheitsgewinne und Komfort des vernetzten Fahrens mit dem Grundrechtsschutz der Fahrenden vereinen lassen, beleuchtet der neueste Band der DatenDebatten, der Expertenbeiträge über das gesamte Spektrum beteiligter Perspektiven enthält. Darin wird deutlich:

- Rechtliche Rahmenbedingungen bleiben hinter dem Stand der Technik zurück.
- Freier Wettbewerb und informationelles Selbstbestimmungsrecht müssen mit Blick auf einen diskriminierungsfreien Zugang hinsichtlich der im Fahrzeug generierten Daten in Einklang gebracht werden. In der Praxis wird dies jedoch durch die technischen Möglichkeiten begrenzt.
  UND:
- Viele Akteure sind an den Daten, die im vernetzten Fahrzeug generiert werden, interessiert. Sind die Forderungen nach mehr Regulierung berechtigt, oder reichen die bestehenden regulatorischen Rahmenbedingungen für neue smarte Produkte aus?

DIE BEITRÄGE

- Datenverarbeitung im Auto – Verratene Fahrer oder verhinderte Autoindustrie? (von Klaus Alpmann)
- Datencrash im vernetzten Verkehr (von Bruno Baeriswyl)
- Wozu braucht Mobilität eigentlich Daten? Bestandsaufnahme und Mobilitätsdatenvision 2030 (von Roland Goetzke und Christopher Kaan)
- Datenschutz bei der Fahrzeugentwicklung – Was hat der Datenschutzbeauftragte mit „Design“ zu tun? (von Sebastian Greß und Florian Springborn)
- Die Digitalisierung der Automobilindustrie (von Manfred Heiss)
- Datenzugang und Datenschutz im vernetzten Fahrzeug: eine ökonomische Perspektive (von Wolfgang Kerber und Daniel Gill)
- Das vernetzte Auto (von Michael Kiometzis)
- Datenschutz im vernetzten Fahrzeug (von August Markl)
- „Neutraler Server“ – Datenschutz und Datenwirtschaft im vernetzten Fahrzeug (von Jakob Metzger und Lena Mischau)
- „Neutraler Server“ für Fahrzeugdaten: Garant für Datenschutz und Datensicherheit am Beispiel des Fahrmodusspeichers (von Julius Reiter, Olaf Methner, Bénédict Schenkel und Sarah Kinzler)
- Vernetztes Fahren: Das Ende der Privatsphäre? (von Matthias Schubert, Günter Martin und Udo Scalla)
- Der smarte Beifahrer – Generali Mobility als Lebensbegleiter der Kunden (von Andrea Timmesfeld, Jeanette Anneser, Jakob Cremer, Sebastian Rudrich und Bernd Wagner)

Mit einem **Geleitwort von Bundesminister a.D. und Rechtsanwalt Gerhart R. Baum.**

ISBN 978-3-503-18754-6
erschienen im Erich Schmidt Verlag, Hrsg. Stiftung Datenschutz

→ **stiftungdatenschutz.org/datendebatten**

RÜCKBLICK

Wir schätzen den persönlichen Austausch mit Expertinnen und Experten, die lebhaften Diskussionen und die anregenden Vorträge auf unseren Veranstaltungen – ebenso die informellen Gespräche in der Kaffeepause. Das alles ist seit März nicht möglich. Aber es ist uns gelungen, interessante GesprächspartnerInnen und Vortragende online zu „versammeln“ und unseren Gästen Gelegenheit zu Fragen zu geben, in zwei ganz unterschiedlichen Online-Veranstaltungen mit jeweils hochaktuellem Bezug.

DATENTAG ONLINE – 30. APRIL 2020

Wir haben Expertinnen und Experten eingeladen, ihre Perspektiven hinsichtlich der Möglichkeiten und Grenzen technischer Lösungen für die Eindämmung der aktuellen Pandemie vorzustellen. Wir wollten erfahren, welche Rolle der Datenschutz und das Grundrecht auf informationelle Selbstbestimmung dabei spielen. Dabei sprachen wir über die verschiedenen „Corona-Apps“, die gerade für den Einsatz (auch) in Deutschland entwickelt werden, und schauten auf Länder, in denen solche Apps schon im Einsatz sind. Außerdem nahmen wir unser Thema „Datenteilungspflicht“ wieder auf und diskutierten, wie das Konzept der „Datentreuhandschaft“ in der Pandemiebekämpfung eine Anwendungsmöglichkeit finden könnte.

THEMEN UND GÄSTE

GRUNDRECHTE UNTER QUARANTÄNE – WAS VERMAG DER DATENSCHUTZ?
Univ.-Prof. Dr. Nikolaus Forgó, Universität Wien

EINE APP ALS AUSWEG?
- Hans-Christian “Chris” Boos, PEPP-PT-Konsortium
- Prof. Ulrich Kelber, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Ninja Marnau, CISPA Helmholtz-Zentrum für Informationssicherheit
- Jens Redmer, Google
- Univ.-Prof. Dr. Sarah Spiekermann-Hoff, Wirtschaftsuniversität Wien

INTERNATIONALE PERSPEKTIVEN
- Thomas Zerdick, IT Policy, European Data Protection Supervisor
- Liza Lin, The Wall Street Journal, Singapur

EINE DATENTREUHAND ZUR PANDEMIEBEKÄMPFUNG?
- Aline Blankertz, Stiftung Neue Verantwortung
- Andreas Hartl, Bundesministerium für Wirtschaft und Energie
- Prof. Dr. Rolf Schwartmann, Technische Hochschule Köln/ GDD e.V.

→ **zur Aufzeichnung: sds-links.de/datentag-corona-apps**

DATENDIALOG ONLINE – 16. APRIL 2020

Welche Rolle spielen Daten, wenn es um die Lösung drängender Probleme der Gesellschaft geht? Wie kann „Big Data“ dem Allgemeinwohl helfen? Über die Bedingungen, die erfüllt sein müssen, damit der Wert und der Nutzen, der in Daten steckt, allen zugute- kommt, sprachen wir mit Prof. Dr. Viktor Mayer-Schönberger im DatenDialog ONLINE.

Es ging um Aspekte des Teilens von Daten ebenso wie um die Frage, welche Möglichkeiten der Datenschutz für eine Erweiterung des Zugangs zu Daten schafft und welche Grenzen er diesbezüglich setzt.

Wenn eine Datenteilungspflicht nur anonymisierte Daten umfassen kann, welche Aussichten hat dann die „Datenspende“, die aktuell diskutiert wird? Wenn wir mehr Anreize für ein freiwilliges Teilen von Daten zum allgemeinen Wohl brauchen, welches Potenzial liegt dann in der Konstruktion einer Datentreuhand, und wie sollte sie gestaltet sein?

Prof. Dr. Viktor Mayer-Schönberger ist Professor für Internet-Verwaltung und -Regulierung am Oxford Internet Institute, Fakultätsangehöriger des Belfer Center of Science and International Affairs an der Harvard University und Mitglied des Digitalisierungsbeirats der Bundesregierung. Er ist Autor von zahlreichen, teils preisgekrönten Büchern, Artikeln und Aufsätzen über die Verwaltung von Informationen und arbeitet derzeit zu den gesellschaftlichen Folgen von Big Data.

→ **zur Aufzeichnung: sds-links.de/datendialog-mayer-schoenberger**

IHRE ANSPRECHPARTNER

FREDERICK RICHTER, LL.M.
Vorstand

0341 5861 555-0

mail@stiftungdatenschutz.org

PROF. DR. ANNE RIECHERT
Wissenschaftliche Leiterin

0341 5861 555-0

mail@stiftungdatenschutz.org

ANTJE SIMON (M.A.)
Büroleitung

0341 5861 555-1

mail@stiftungdatenschutz.org

UNSER ARCHIV ALLER POLITIKBRIEFE FINDEN SIE HIER

politikbrief.stiftungdatenschutz.org

IMPRESSUM

Herausgeber

Stiftung Datenschutz

Karl-Rothe-Straße 10 –14
04105 Leipzig
T 0341 5861 555-0
F 0341 5861 555-9
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

Redaktionsleitung & Mitarbeit

Anne Riechert, Antje Simon, Florian König

Redaktionsschluss
17. Juni 2020

Agenturpartner

KING CONSULT | Kommunikation