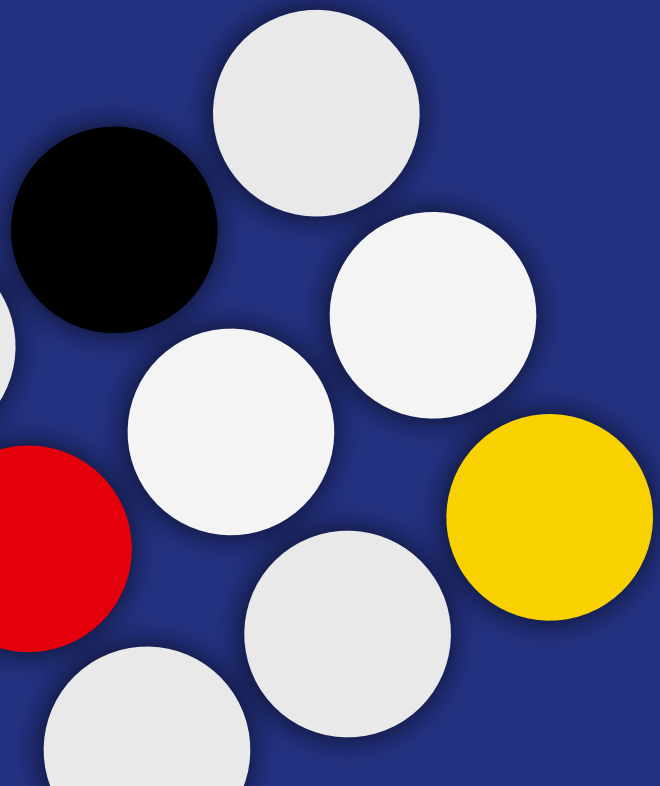
STIFTUNG DATENSCHUTZ

POLITIKBRIEF – FRÜHJAHR 2020

# DATENSCHUTZ ZUM NUTZEN ALLER: AKTUELLE PERSPEKTIVEN



ÜBERBLICK

Liebe Leserinnen und Leser,

derzeit bemühen sich viele Einrichtungen und Organisationen darum, mit technischen und organisatorischen Mitteln die COVID-19-Pandemie zu bekämpfen. Die Frage, wie sich dabei Daten zum Nutzen aller teilen und einsetzen lassen, ohne dass Einzelnen Nachteile daraus entstehen, bewegt gerade ganz konkret viele Menschen. Im vergangenen November haben wir diese Frage mit Expertinnen und Experten im Rahmen unserer Konferenz zur Datenteilungspflicht[1] diskutiert. Wir hätten uns nicht vorstellen können, dass diese Frage schon so bald von solcher Dringlichkeit für die Gesundheit und das Leben vieler Menschen ist.

Die größte Bedeutung für den Umgang mit der Pandemie hat das Verhalten der Bevölkerung. Aufgabe der Politik ist es jetzt noch mehr als sonst, die Bürgerinnen und Bürger zu überzeugen, mit Verhaltensänderungen ihren Beitrag für die Gemeinschaft zu leisten. Dass bestimmte Bürgerrechte zeitweise eingeschränkt werden müssen, wie das Recht auf Versammlungsfreiheit, aber auch der Schutz der Privatsphäre, stellt kaum noch jemand grundsätzlich in Abrede. Wie die Rechte gegeneinander abgewogen werden und wie schnell und umfassend sie nach Ende der Pandemie wiederhergestellt werden, wird die Haltung der Bürgerinnen und Bürger langfristig beeinflussen.

Ich persönlich war jedenfalls erstaunt, wie bereitwillig Menschen ihre Privatsphäre einschränken ließen und lassen. So würden laut einer Umfrage[2] mehr als die Hälfte der Deutschen öffentlichen Stellen gestatten, das persönliche Bewegungsprofil zu nutzen, um die Verbreitung des Virus nachzuvollziehen.

Wir haben den aktuellen Stand der Dinge für Sie zusammengestellt.

Bleiben Sie gesund!

**Frederick Richter, Vorstand der Stiftung Datenschutz**

1 datentag.de
2 https://sds-links.de/45w

# DATENSCHUTZ VS. GESUNDHEIT – KONFLIKT DER GRUNDRECHTE?

Die Stiftung Datenschutz vertritt seit ihrer Gründung die pragmatische Sichtweise, dass Datenschutz handhabbar sein muss. Die gesetzlichen Vorgaben sollten auf die jeweilige Situation und die Schutzgüter abgestimmt sein. Zu strenge Anforderungen schaden der Akzeptanz; sorgloser Datenumgang kann Menschen schwer schaden. Nun werden Grundrechte – das Fundament unserer Demokratie – zum Schutz von Leben und Gesundheit eingeschränkt oder gar ausgesetzt: Gesundheitsämter übermitteln Listen mit den Adressen Erkrankter an die Polizei[3], ein Wirtschaftsverband will, dass Bewegungsprofile und Kreditkartendaten an die Behörden weitergegeben werden und verlangt, dass der Privatsphärenschutz hintanzustehen hat[4], Lehrerinnen sollen ihre Schulleitung über Krankheits- und Verdachtsfälle in ihren Klassen informieren und fordern dafür die Mitwirkung der Eltern. Die Datenschutzgrundverordnung hilft da nur im Einzelfall, ihr Ziel ist in erster Linie der Schutz von Rechten und Freiheiten des Individuums[5] und nicht der Schutz der freiheitlichen Gesellschaft an sich.

Dabei ist die Bereitschaft, auf individuelle Privatsphäre zu verzichten, um sich selbst und andere zu schützen, in der Bevölkerung so hoch, dass es umfassender Zwangsmaßnahmen vielleicht gar nicht bedarf. So würden 71,9 Prozent der Deutschen freiwillig persönliche Gesundheitsdaten, Bewegungsprofil oder soziale Kontaktpunkte mit öffentlichen Institutionen wie dem Robert-Koch-Institut teilen, 54,6 Prozent würden öffentlichen Stellen gestatten, das persönliche Bewegungsprofil zu nutzen, um die Verbreitung des Virus nachzuvollziehen.[6]

Dennoch darf die momentane Bereitschaft der Bevölkerung, Eingriffe in ihre Privatsphäre (und in viele andere Grundrechte) hinzunehmen, nicht dazu führen, dass die erforderliche politische und gesellschaftliche Debatte ausfällt. Sonst besteht die Gefahr – wie immer wieder geschehen – dass einmal eingeführte Maßnahmen Begehrlichkeiten wecken, die Daten, wenn sie schon vorhanden sind, auch für andere Zwecke zu verwenden. Als abschreckendes Beispiel dürfen die automatische Kennzeichenerfassung und die ausgesetzte Vorratsdatenspeicherung dienen.

Diese Beispiele machen anschaulich, wie kurz der Weg von einer Datennutzung zur Bekämpfung von Verbrechen zu einer Datennutzung zur Bekämpfung bloßer Vergehen sein kann. Daher muss bei allen Einschränkungen der Grundrechte, die zur Bekämpfung der COVID-19-Pandemie erforderlich werden, immer bedacht werden, wie diese wieder rückgängig gemacht werden, sobald sie nicht mehr erforderlich sind.

3 *https://sds-links.de/d30*
4 *https://sds-links.de/gcf* :„Der Schutz der individuellen Privatsphäre bleibt auch in Krisenzeiten ein hohes Gut. Angesichts der aktuellen Situation wiegt der allgemeine Schutz des Lebens und der Gesundheit jedoch schwerer."
5 Artikel 1 Absatz 2 EU-Datenschutzgrundverordnung
6 *https://sds-links.de/45w*

# „DAFÜR GIBT ES DOCH 'NE APP“

Schon ganz zu Beginn[7] der Pandemie wurde diskutiert, wie man die bei der Nutzung von Smartphones anfallenden Daten erfassen und einsetzen könnte, um Infektionsketten nachvollziehbar zu machen. Da viele Menschen Smartphones stets bei sich tragen und diese ihren Aufenthaltsort – und damit den ihrer Nutzer – erfassen und weitergeben können, lag es nahe, sich dies zunutze zu machen. Aber natürlich gibt es für dieses komplexe Problem keine einfache Lösung, und eine rein technische schon gar nicht.

## FUNKZELLENABFRAGEN, GPS

So hatte das Bundesministerium für Gesundheit in einem ersten Entwurf zur Änderung des Infektionsschutzgesetzes vorgesehen, Standortdaten von Mobilfunkgeräten mittels Funkzellenabfragen zu nutzen, um Kontaktpersonen von Viruserkrankten zu identifizieren und zu benachrichtigen. Funkzellendaten können ohne Zutun der Mobilfunkkunden vom Netzbetreiber weitergegeben werden. Diese Idee erwies sich als untauglich, schon weil die Funkzellenabfrage viel zu ungenau ist. So sind die Funkzellen in dünn besiedelten Gebieten viel zu groß und in dicht besiedelten Gebieten viel zu voll, als dass ihre Überwachung belastbare Hilfe bei der lokalen Nachverfolgung einzelner infizierter Personen hätte leisten können. Diesem fragwürdigen Nutzen stünde ein tiefer Eingriff in die Privatsphäre gegenüber, weil aus den Daten auch hervorgehen könnte, wer wann mit wem wie lange telefoniert und SMS ausgetauscht hat.

Eine andere Möglichkeit wäre die Aufzeichnung und Weiterleitung von GPS-Daten durch eine App. Damit würde der Standort des Smartphones nachverfolgbar. Konkrete Anwendungskonzepte gibt es bisher nicht.

## PAN EUROPEAN PRIVACY PROTECTING PROXIMITY TRACING (PEPP-PT)

Gerade wird die Nutzung von Bluetooth diskutiert, eine Funktechnik, die je nach Endgerät kurze (bis 1 m), mittlere (bis ca. 10 m) und längere (bis ca. 100 m) Distanzen überbrücken kann. Auf dieser Technologie basiert das Anfang April vorgestellte System PEPP-PT[8] [9], das auf Initiative eines deutschen Unternehmens von einem internationalen Team entwickelt wird. Beteiligt sind das Robert-Koch-Institut und das Fraunhofer Institut für Nachrichtentechnik; das Bundesamt für die Sicherheit in der Informationstechnik und der Bundesdatenschutzbeauftragte beraten.

Die Technologie sieht vor, dass Smartphones, deren Besitzer einander lange genug ausreichend nah für eine Infektion gekommen sind, über den Funkstandard Bluetooth anonym einen befristet gültigen Zahlencode austauschen, der lokal auf den Geräten generiert und gespeichert wird. Sollte ein Nutzer positiv auf das Virus getestet werden, sollte er die Zahlencodes der Zeiten, zu denen andere Smartphones in Ansteckungsdistanz waren, an den Server des Betreibers übermitteln. Die App warnt dann alle betroffenen Personen davor, dass sie ebenfalls infiziert sein könnten, ohne dass der Serverbetreiber die Betroffenen identifizieren kann. Die Erfassung von Bewegungsdaten oder die Identifizierung des Infizierten gegenüber Dritten ist nicht erforderlich. Inzwischen gibt es auch Vorschläge von dritter Seite, wie die notorisch schwierige Anonymisierung der Daten noch besser gewährleistet werden kann, zumal die Bluetooth-Technologie ihre eigenen Probleme mit sich bringt.

Manche Datenschutzexperten äußern sich allerdings skeptisch.[10] So könnte die Freiwilligkeit durch den sozialen Druck beeinträchtigt werden, insbesondere, wenn die Verwendung der App mit der Lockerung von Ausgangsbeschränkungen und ähnlichen Maßnahmen verknüpft wird.

7 *https://sds-links.de/ebx*
8 *https://sds-links.de/u5m*
9 *https://sds-links.de/0hp*
10 *https://sds-links.de/22q*

## ES GIBT KEINE EINFACHE LÖSUNG FÜR ALLE PROBLEME

Aus Sicht des Datenschutzes erscheint PEPP-PT prinzipiell ein guter Beitrag im Rahmen eines Gesamtkonzepts, wenn es gelingt, viele Menschen für die freiwillige Teilnahme zu gewinnen. Die Akzeptanz wird auch davon abhängen, dass der Betreiber des Systems vertrauenswürdig ist und dass die Sicherheit und die Integrität der App nachweisbar und überprüfbar sind, am besten indem der Code offengelegt wird. Grundsätzlich ist aber die Akzeptanz in der Bevölkerung für eine solche App hoch, wie eine aktuelle Untersuchung[11] zeigt: Knapp drei Viertel der Befragten würden die App ganz sicher oder wahrscheinlich installieren. Dass die Bundesregierung mit der Unterstützung einer solchen App in ihrem Ansehen steigen würde, glaubt übrigens die Hälfte der Befragten über alle Parteipräferenzen hinweg.

Wie groß der Nutzen ist, hängt dann am Ende nicht von der Technik ab, sondern davon, dass auch genügend Kapazitäten für Tests und für die Betreuung von Infizierten zur Verfügung stehen. Eine einfache Lösung, gar für alle denkbaren Probleme, kann ein technisches System gar nicht sein; diese Vorstellung war noch nie richtig und ist es auch in dieser Situation nicht. Eine App kann sinnvoll nur ein Teil einer Gesamtstrategie sein. Unter dem Aspekt des Datenschutzes ist PEPP-PT jedoch ein vielversprechender Ansatz.

**Welche Rolle der Datenschutz in der aktuellen Situation spielt, diskutieren wir mit Expertinnen und Experten ausführlich in einer Online-Veranstaltung „Datenschutz und Virusbekämpfung – Lösung durch Technik?“ am 30. April 2020.**

→ **www.stiftungdatenschutz.org/veranstaltungen**

11 *https://sds-links.de/i4p*

# AKTUELLE VORHABEN


## DATENDIALOG ONLINE

Unser Vorstand Frederick Richter im Gespräch mit Prof. Dr. Viktor Mayer-Schönberger zum Thema **„Datenteilung & Datenzugang – welche Lösungen brauchen wir?“**

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 Buchkapiteln über die Verwaltung von Informationen, und arbeitet derzeit zu den gesellschaftlichen Folgen von Big Data.

## DATENTAG ONLINE – 30. APRIL 2020 – IN VORBEREITUNG

Zum Thema **„Datenschutz und Virusbekämpfung - Lösung durch Technik?“** bereiten wir gerade eine neue Ausgabe unseres DatenTag in Form einer **Online-Konferenz** vor. Das Programm erfahren Sie rechtzeitig.

→ **www.stiftungdatenschutz.org/veranstaltungen**


## DATENDEBATTEN IV

Im Mai erscheint unser neues Buch **„DatenDebatten IV: Datenschutz im vernetzten Fahrzeug“**. Der Band betrachtet in Expertenbeiträgen über das gesamte Spektrum beteiligter Perspektiven die Bedeutung von Daten für die individuelle Mobilität im „connected car“ und deren Auswirkungen auf die Privatsphäre.


# RÜCKBLICK

## DATENTAG „DATEN, MACHT UND MONOPOLE“

Eine Konferenz zu Umsetzungsmöglichkeiten und Erfolgschancen einer Regulierung von Daten zur Wettbewerbsförderung (Datenteilungspflicht). Berlin, 26.11. 2029

In unserer digitalen Welt fallen täglich rieseige Datenmengen an. Diese Daten haben einen Wert, auch wenn die vielen Metaphern – Öl, Grundwasser... – nie ganz zutreffen. Das Konzept der Datenteilungspflicht ist eine mögliche Antwort auf die Frage, wie dieser Wert zu nutzen ist. Denn der Datenbesitz verleiht Macht.

Die vorgeschlagene Pflicht zum Teilen anonymer Daten überträgt in gewisser Weise den im öffentlichen Sektor schon länger diskutierten Open Data-Gedanken auf den privaten Bereich. Der Vorschlag möchte Daten, die beispielsweise bei Industrieunternehmen oder Verkehrsbetrieben liegen, für neue Geschäftsmodelle oder neue Formen der Daseinsvorsorge öffnen.

Auf dem DatenTag der Bundesstiftung wurden die Chancen und Herausforderungen betrachtet, die hier liegen. Mit Expertinnen und Experten verschiedener Disziplinen und Sektoren wurde herausgearbeitet, ob und wie eine Datenteilungspflicht sowohl dem Gemeinwohl als auch der nationalen Digitalökonomie förderlich sein kann. Ziel des Tages war es, mehr Klarheit zu datenschutzrechtlichen, kartellrechtlichen und technologischen Dimensionen zu erlangen. Neben wirtschaftlichen und juristischen Voraussetzungen wurden auch die Anforderungen an die Politik diskutiert. Auch die Praxis wurde beleuchtet: In welchen Branchen gibt es bereits freiwillige Initiativen von data sharing? Welche Anreize bestehen für Unternehmen zur Freigabe von Daten an den Wettbewerb oder die Allgemeinheit?“

Viele grundsätzliche Punkte bedürfen noch einer Klärung – etwa, welche Rolle die Anonymisierung spielt und welche Maßstäbe hier anzulegen sind.


## DATENTAG „DATENSCHUTZ IM EHRENAMT"

Viel ist in den vergangenen zwei Jahren über die Anwendung der DSGVO in der Wirtschaft geschrieben und diskutiert worden. Dabei treffen die Datenschutzpflichten genau so den sogenannten Dritten Sektor: Organisationen, die nicht profitorientiert arbeiten und daher zum großen Teil von ehrenamtlichem Engagement getragen werden. Im Rahmen eines DatenTages „Datenschutz im Ehrenamt" gingen wir den dort drängenden Fragen nach: Wie kommen ehrenamtliche Organisationen mit den neuen rechtlichen Vorgaben klar? Was wird vom Datenschutz und dessen Durchsetzung erwartet, damit gutes Tun und bürgerschaftliches Engagement nicht leiden?

## DER JOURNALISTENPREIS DER STIFTUNG DATENSCHUTZ 2019

Der Journalistenpreis der Stiftung Datenschutz 2019 wurde an Harald Maass verliehen für seine Reportage „Totale Kontrolle", erschienen im SZ-Magazin vom 15. März 2019. Der Text beschreibt die Unterdrückung der muslimischen Minderheit der Uiguren durch die chinesischen Behörden mithilfe allumfassender Überwachung.

Der mit 5.000 Euro dotierte Journalistenpreis der Stiftung Datenschutz wird seit 2017 vergeben; 2019 erstmals mit freundlicher Unterstützung des Deutschen Spendenrats. Der Preis würdigt eine journalistische Arbeit, die sich durch ausgewogene Einordnung und verständliche Erklärung komplexer Vorgänge mit Bezug zum Datenschutz auszeichnet.

# 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, Sebastian Himstedt, Florian König

**Redaktionsschluss**
14. April 2020

**Agenturpartner**

KING CONSULT | Kommunikation

Sehr gut. Danke. Kommunikation.