GERMAN DATA SCIENCE DAYS 2023

CDPS TUM CENTER FOR DIGITAL PUBLIC SERVICES

Lehrstuhl für Recht und Sicherheit der Digitalisierung
TUM Center for Digital Public Services
Technische Universität München

Plädoyer für einen konstruktiv-abwägenden Datenschutz

Datennutzung als Verfassungspflicht und ethisches Gebot

Univ.-Prof. Dr. Dirk Heckmann
Mitglied des Bayerischen Verfassungsgerichtshofs

Digitalisierung

"Besserer Datenschutz ist eine moralische Pflicht"

8. Dezember 2022, 15:56 Uhr | Lesezeit: 6 min

Alena Buyx, Jahrgang 1977, studierte Medizin, Philosophie, Soziologie und Gesundheitswissenschaften. Seit 2020 ist sie Vorsitzende des Deutschen Ethikrats. (Foto: Political Moments/Jutta Prechtel/SZ Photo)

„Besserer Datenschutz ist eine moralische Pflicht. Datenschutz ist kein Selbstzweck, der dient einem wichtigen Ziel. Er ist wesentlich für den ***Schutz von Patienten, den Schutz ihres Grundrechts auf informationelle Selbstbestimmung*** *und ihrer persönlichen Interessen. Diese Rolle muss er erfüllen. Aber, das haben der Deutsche Ethikrat und auch der Sachverständigenrat im Gesundheitswesen beide kürzlich betont, Datenschutz darf nicht zum Gegenteil werden,* ***er darf Patienten nicht schaden****. Und er muss* ***mit anderen wichtigen Gütern und Grundrechten - auf Gesundheit, auf Lebensschutz - abgewogen*** *werden. Da kann es sein, dass die grundrechtliche Pflicht zum Schutz von Leben und Gesundheit im Einzelfall* ***stärker wiegt als das Restrisiko****, das bei bestimmter Datennutzung für die informationelle Selbstbestimmung verbleibt.“*

Handelsblatt

MEINE NEWS | HOME POLITIK UNTERNEHMEN TECHNOLOGIE FINANZEN MOBILITÄT KARRIERE ARTS & STYLE MEINUNG VIDEO SERVI

Deutschland Konjunktur International Ökonomische Bildung

andelsblatt > Politik > Deutschland > Datenschutz: Warnung der Ethikrat-Chefin Buyx erntet Kritik

Suchbegriff, WKN, ISIN

DIGITALISIERUNG DES GESUNDHEITSWESENS

„Uninformiert und schwer erträglich“: Datenschützer attackiert Ethikrat-Chefin

Die Chefin des Deutschen Ethikrats warnt vor einem zu strikten Datenschutz bei der Digitalisierung des Gesundheitswesens – und erntet dafür heftigen Widerspruch.

Dietmar Neuerer

09.12.2022 - 11:00 Uhr • 4 x geteilt

*Die Positionen der Ethikrat-Chefin zum Datenschutz seien „**uninformiert und schwer erträglich**, gerade weil sie mit dem Anspruch moralischer Überlegenheit geäußert werden“, sagte Brink dem Handelsblatt. „Ethiker sollten gelernt haben, dass man gesellschaftlich bestimmende Entwicklungen wie die Digitalisierung **nicht durch einseitige und zuspitzende Äußerungen** vorantreibt, sondern **alle relevanten Interessen mit ruhigem Blick einbezieht und abwägt**“, betonte der Behördenchef.*

☆ KELBER: E-REZEPT-GESETZ VERLETZT EU-RECHT

Oberster Datenschützer warnt Kassen

APOTHEKE ADHOC, 19.08.2020 13:24 Uhr

Bundesdatenschutzbeauftragter Professor Dr. Ulrich Kelber sieht das Patientendatenschutzgesetz als europarechtswidrig – und plant deshalb aufsichtsrechtliche Maßnahmen gegen die gesetzlichen Krankenkassen.
Foto: Bundesregierung/ Kugler

***Berlin* - Bundesdatenschutzbeauftragter Professor Dr. Ulrich Kelber sieht das vom Bundestag verabschiedete Patientendatenschutzgesetz (PDSG) als europarechtswidrig. Sollte es nicht zu Nachbesserungen kommen, bevor das Gesetz vom Bundesrat bestätigt wird, sehe er sich gezwungen, Maßnahmen gegen die unter seiner Aufsicht stehenden Krankenkassen einzuleiten. Konkret geht es bei Kelbers Kritik um das Zugriffsmanagement und das Authentifizierungsverfahren.**

27. August 2020 – Brigitta Engel

"Folgen einer europarechtswidrigen Gesetzgebung beim Patientendatenschutzgesetz", Pressekonferenz mit Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI); Dagmar Hartge, Landesbeauftragte für den Datenschutz Brandenburg; Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen; Stefan Brink, Landesbeauftragter für den Datenschutz Baden-Württemberg. Bild: Screenshot aus YouTube-Video

Öffentliche Warnung vor der Anwendung eines Gesetzes

Univ.-Prof. Dr. jur. Dirk Heckmann

Lehrstuhl für Recht und Sicherheit der Digitalisierung
TUM School of Governance | Fakultät für Informatik
Technische Universität München

Gutachterliche Stellungnahme

für den Gesundheitsausschuss des Deutschen Bundestages

Sachverständigen-Anhörung vom 27. Mai 2020 zum

Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten
in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG)
Drucksache 19/18793 v. 27.4.2020 und weiteren Anträgen

25. Mai 2020

Fazit

Das Konzept eines zeitlich gestuften Berechtigungskonzepts ist datenschutzkonform und auch rechtspolitisch zu begrüßen. Es schränkt die Datenhoheit des Patienten nicht ein, sondern trägt der technischen Entwicklung Rechnung. Damit forciert es die Digitalisierung im Gesundheitswesen mit all ihren Vorteilen und überlässt es dem Patienten/Versicherten, in welchem Tempo er an dieser Entwicklung teilhaben möchte.

Verfassungsbeschwerde zur elektronischen Patientenakte gescheitert | Nachricht | Das BVerfG hat eine Verfassungsbeschwerde gegen Regelungen zur elektronischen Patientenakte nicht ... | BVerfG 1. Senat | 1 BvR 619/20

Gericht/Institution:	**BVerfG**
Erscheinungsdatum:	**26.01.2021**
Entscheidungsdatum:	**04.01.2021**
Aktenzeichen:	1 BvR 619/20, 1 BvQ 108/20
Quelle:	juris
Normen:	§ 68b SGB 5, § 299 SGB 5, § 68 SGB 5, § 284 SGB 5, Art 2 GG ... mehr

„Nach Auffassung des BVerfG ist die Verfassungsbeschwerde bereits unzulässig, weil die Nutzung der elektronischen Patientenakte freiwillig ist und der Beschwerdeführer nicht unmittelbar und gegenwärtig in seinen eigenen Rechten betroffen ist."

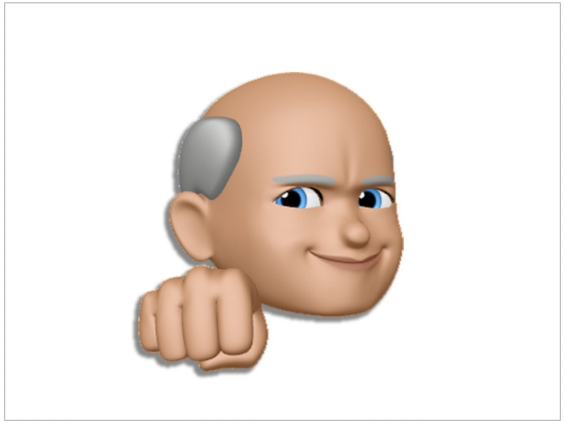
ÜBER MEDIEN

Kommentar

Datenschutzbeauftragter Kelber

Last Action Hero: Datenschutz Man

von Hendrik Wieduwilt | 4. Februar 2022



Ulrich Kelber, wie er sich selbst sieht

Screenshot: Twitter/UlrichKelber

Manchmal, wenn der Tag etwas müde daherkommt, feuert Kelber wiederum seine Fans an: „Bringt mich mal auf den neuesten Stand. Welche Urban Legends zum Datenschutz gab es denn an diesem Wochenende?“ schreibt er unter Applaus. Ein anderes Mal fragt er, ob an der mangelnden Digitalisierung der Datenschutz, das Wetter oder „die Außerirdischen“ schuld sind, haha. „Schreibt’s mir in die Kommentare“, heißt es bei den Youtubern, der Zweck ist gleich: Aufmerksamkeit, Likes, Reichweite.

Libra

Home Über Libra Köpfe Newsletter

BEHÖRDENKOMMUNIKATION

TEILEN PDF DOWNLOAD

Wie Datenschützer tweeten, tröten, warnen

Prof. Dr. Anne Paschke

Die Datenschutzbehörden nutzen viele Plattformen für Warnungen – manchmal schränkt das zu Unrecht Grundrechte von Unternehmen und Nutzerschaft ein.

*„Sollte eine Behörde dagegen selbst warnend tätig werden wollen, sind Kurznachrichtendienste problematische Medien: Die dort übliche schnelle Taktung müsste auf den **Ruhepuls rechtsstaatlicher Achtsamkeit** heruntergefahren werden.*
Das gebieten für den Bereich staatlicher Warnungen schon die durch das Bundesverfassungsgericht entwickelten Anforderungen aus der „Glykol“-Rechtsprechung.“

CDPS
TUM CENTER FOR DIGITAL PUBLIC SERVICES

Microsoft 365 – so sollte Datenschutzaufsicht nicht sein

Deutschlands Datenschutzbehörden tragen eine große Verantwortung für Staat und Gesellschaft. Ihr Umgang mit dem Datenschutz muss grundlegend neu justiert werden.

Von Kristin Benedikt, Thomas Kranig und Rolf Schwartmann

Die deutschen Datenschutzaufsichtsbehörden haben Ende November 2022 eine Stellungnahme zu Microsoft 365 veröffentlicht, die es in sich hat. Microsoft-Kunden können danach einen rechtmäßigen Einsatz der Software nicht nachweisen, mit anderen Worten: Microsoft 365 ist rechtswidrig. Nach dem Willen der Aufsicht soll hierzulande die Nutzung von Microsoftprodukten also faktisch eingestellt werden. Nehmen Deutschlands Unternehmen, Schulen, Städte und Gemeinden, Gerichte und Gesetzgebungseinrichtungen die Empfehlung zu diesem „digitalen Lockdown" ernst, dann steht hier faktisch alles still, denn es gibt keine alternative Software, die in der Fläche einsetzbar wäre. Der Beschluss aus dem November wiederholt einerseits eine Bewertung eines Arbeitskreises der Datenschutzkonferenz (DSK) aus dem Jahr 2020. Allerdings gab es damals Widerspruch aus den eigenen Reihen: Den Datenschutzbehörden von Baden-Württemberg, Bayern, Hessen und des Saarlandes war die Bewertung zu undifferenziert. Vor allem seien nur (veraltete) Vertragsbestimmungen von Microsoft zur Grundlage der Entscheidung gemacht worden. Es habe keine eigenständige Prüfung der Technik stattgefunden. Zum anderen seien rechtsstaatliche Grundsätze verletzt worden, da Microsoft nicht förmlich angehört worden sei. Nun bekräftigt das Gremium einstimmig sein „Microsoft-Verbot". Der Fall braucht einen konstruktiven Ausgang und verdient eine grundlegende Einordnung.

1. Datenschutzrecht

Europa hat im Jahr 2018 die Datenschutzgrundverordnung (DSGVO) ins Werk gesetzt und eine belastbare Grundlage für Datenverarbeitungen geschaffen. Das Gesetz ist viel besser als sein Ruf. Es gibt schon in seinem ersten Artikel weise abgewogene verbindliche Maßgaben vor. Erstens: Das Datenschutzrecht schützt natürliche Personen bei der Verarbeitung ihrer Daten. Zweitens: Das Datenschutzrecht schützt die Wirtschaft bei der Verarbeitung der Daten zu deren freiem, wirtschaftlichem Verkehr im Binnenmarkt. Ergänzend legt das Recht fest: Datenschutz genießt keinen Vorrang, und Datenverarbeitung ist dem Dienst an der Menschheit verpflichtet. Das Recht auf Datenschutz muss fair abgewogen werden mit den anderen europäischen Grundrechten. Das gilt insbesondere für die wirtschaftlichen Freiheiten im Binnenmarkt, die in praktische Konkordanz, also in einen harmonischen Wohlklang mit dem Datenschutz gebracht werden müssen. Weitere und entstehende neue Datenakte wie die Entwürfe der KI-Verordnung oder des Data Act unterstützen den Ansatz des vielfältigen Einsatzes von Daten zum Wohl von Gesellschaft, Wirtschaft und Staat auf Basis der DSGVO.

Es hilft auch Unternehmen und Behörden, denn sie können zuverlässige Anbieter auswählen. Insgesamt gilt es, mit Wirtschaft, Wissenschaft und Gesellschaft konstruktiv zusammenzuarbeiten. Die Stiftung Datenschutz des Bundes etwa hat jüngst „Grundsatzregeln für die Anonymisierung personenbezogener Daten" und einen zugehörigen Praxisleitfaden für die Durchführung der Anonymisierung veröffentlicht. Die Praxis erhält damit konkrete Handreichungen. Im Rahmen des Digitalgipfels der Bundesregierung hat die Fokusgruppe Datenschutz des Bundesinnenministeriums schon im Jahr 2019 einen entsprechenden Ansatz zur Pseudonymisierung vorgelegt. Vertreter von Aufsichtsbehörden waren auch hier konstruktiv beteiligt.

Mit der Digitalisierung leben bedeutet schon in der Gegenwart, mit einer sich dynamisch entwickelnden Zukunftstechnologie zu leben. Jede neue Technik von der Eisenbahn über die Autofahrt bis zum Fliegen verlangt der Menschheit ab, Risiken zu kalkulieren, wenn sie sich für deren Einsatz entscheidet. Das bedeutet, Verkehrungen gegen vorhersehbare Gefahren sorgfältig zu treffen und mit unvermeidbaren Restrisiken zu leben. Wir beklagen in diesem Wissen jährlich weit mehr als eine Million Verkehrstote rund um den Globus.

Auch Datenverarbeitung ist Risikotechnologie. Ein Smartphoneprozessor rechnet etwa deutlich mehr als 100 Millionen Mal schneller als der Apollo 11 Guidance Computer, der vor über 50 Jahren in der Mondrakete verbaut war. Auch wenn damit heute jedes Kind mehr Computertechnik einsetzt als eine Apollo-11-Rakete, kommt die neue Technik nicht als Raketenwissenschaft daher. Wir erleben Datenverarbeitung als in harmlose Alltagsgegenstände verpackt und füttern sie von Siri bis Echo mit Privatwissen, das im Weltwissen der Nutzer aufgeht. Wir speisen das Netz über vernetzte Endgeräte – vom Rasenmäher über Smartphones bis hin zu vernetzten Autos – mit persönlichen Daten in Ton, Text, Bild und Standorten. Weil die Technik so einfach bedient werden kann, aber rechtlich so komplex ist, sieht, spürt und beachtet man deren Risiken so wenig wie Madame Curie die Wirkung von Röntgenstrahlen. Ohne deren Einsatz wollen wir aber auch nicht leben. Wir treffen sorgsam Vorkehrungen gegen ihr Risiko.

Die wenigsten werden auch auf datengestützte Navigation zur Fortbewegung oder gar auf die Nutzung einer Schreib- oder Videokonferenzsoftware verzichten wollen. Auf Microsoft 365 können wir aktuell nicht verzichten, wenn das digitale Leben weitergehen soll. Die Europäische Union hat sich dazu entschieden, mit einer eigenen Datenstrategie für den Binnenmarkt ihren Platz auf der digitalwirtschaftlichen Weltkarte einzunehmen. Derzeit behaupten sich dort die USA, China und Indien. Wir machen uns im Bewusstsein der damit verbundenen Risiken zum Baustein im Internet der Menschen und der Dinge. Mit jedem Foto, das

Wir können, wollen und werden deswegen aber nicht auf unsere Grundrechte verzichten. Die deutschen Datenschutzaufsichtsbehörden haben einen wichtigen Anteil an der Herstellung der Ausgewogenheit des Systems zu deren Schutz. Sie müssen alle Ziele und Interessen ausgewogen wahren, welche die Erwägungsgründe der DSGVO benennen und welche die neuen Datenakte betonen. Die Aufsichtsbehörden sollten ihre unabhängige Stellung im Lichte eines digitalen Europas neu justieren. Der europäische Gesetzgeber strebt mit der digitalen Datenstrategie einen Binnenmarkt an, in dem die oberste Prämisse nicht die Datenminimierung oder Datenvermeidung, sondern die Datennutzung zum Wohle der Allgemeinheit ist. Das erfordert ein Umdenken: weniger diffuse Produktwarnung und mehr Beratung zur datenschutzkonformen Datennutzung.

CDPS
TUM CENTER FOR DIGITAL PUBLIC SERVICES

bitkom

Themen | Marktdaten | Presse | Bitkom

Pressebereich > Bitkom zu den Ergebnissen des Corona-Gipfels

Bitkom zu den Ergebnissen des Corona-Gipfels

- **Bitkom-Präsident Berg: „Digitale Covid-19-Testpässe schnellstmöglich einführen“**

Berlin, 23. März 2021 - Die Bund-Länder-Runde hat eine Verschärfung der Maßnahmen zur Eindämmung der Corona-Pandemie beschlossen. **Dazu erklärt Bitkom-Präsident Achim Berg:**

„**Datenschutzrechtliche Prinzipienreiterei** gefährdet derzeit jene Menschenleben, die sich durch den flächendeckenden Einsatz digitaler Lösungen retten ließen. In der jetzt beginnenden, für die Menschen in Deutschland besonders herausfordernden Phase der Pandemie brauchen wir eine **neue Abwägung zwischen dem Schutz von Daten und dem Schutz von Leben**. Digitale Lösungen müssen nunmehr flächendeckend und ohne langwierige Vorfeld-Diskussionen eingesetzt werden können.“

CDPS
TUM CENTER FOR DIGITAL PUBLIC SERVICES

Brauchen wir eine „neue Abwägung“?

Nein!

Es wäre gut, überhaupt einmal abzuwägen.

Was bedeutet es, (Gesundheits-) Daten nicht zu nutzen?

Wissenschaftlicher Beirat
für Digitale Transformation

AOK Die Gesundheitskasse.

Gesundheitsdatennutzung: jetzt!

Vertrauen stärken, Lösungen umsetzen

- Keine **Tatsachenbasis** für Diagnosen, Therapien, Gesundheitsvorsorge
- Gesundheitssystem **kollabiert**
- Menschen sterben oder leiden

Positionspapier vom 7.7.2022

- Verstoß gegen **Untermaßverbot**
- Einschränkung vieler Grundrechte
- Keine **evidenzbasierte Politik**
- Delegitimierung des Staates

Datenschutz heißt nicht Datenaskese

Art. 1 DSGVO – Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten **und zum freien Verkehr solcher Daten**.

(2) …

(3) Der **freie Verkehr personenbezogener Daten** in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten **weder eingeschränkt noch verboten** werden.

„Verbotsprinzip“ – mit vielfachem Erlaubnisvorbehalt

Art. 6 Abs. 1 DSGVO – Rechtmäßigkeit der Verarbeitung [in einem dieser Fälle]:

a) … b) … c) …

d) die Verarbeitung ist **erforderlich, um lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person **zu schützen**.

#toddurchdatenschutz ?

Nein!

„Verbotsprinzip“ – mit vielfachem Erlaubnisvorbehalt

Art. 6 Abs. 1 DSGVO – Rechtmäßigkeit der Verarbeitung [in einem dieser Fälle]:

a) … b) … c) … d) …

e) die Verarbeitung ist für die **Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt**

Gesetzliche Grundlage

Demokratische Legitimation

Verhältnismäßigkeitsgrundsatz

12. BayIfSMV Text gilt ab: 28.04.2021 Gesamtvorschrift gilt bis: 09.05.2021 **Gesamtansicht**
Fassung: 05.03.2021

§ 2 Kontaktdatenerfassung

[1]Soweit nach dieser Verordnung oder aufgrund der in ihr vorgesehenen Schutz- und Hygienekonzepte zum Zweck der Kontaktpersonenermittlung im Fall einer festgestellten Infektion mit dem Coronavirus SARS-CoV-2 Kontaktdaten erhoben werden, gilt neben § 28a Abs. 4 Satz 2 bis 7 IfSG Folgendes:

1. zu dokumentieren sind jeweils Namen und Vornamen, Anschrift und eine sichere Kontaktinformation (Telefonnummer oder E-Mail-Adresse) sowie der Zeitraum des Aufenthaltes;

2. werden gegenüber dem zur Erhebung Verpflichteten Kontaktdaten angegeben, müssen sie wahrheitsgemäß sein.

[2]Die Erhebung der Kontaktdaten nach Satz 1 kann auch in elektronischer Form erfolgen, soweit dabei eine hinreichend präzise Dokumentation der Daten nach Satz 1 Nr. 1 sichergestellt wird. [3]Behörden, Gerichte und öffentliche Stellen, die Aufgaben im öffentlichen Interesse erfüllen oder in Ausübung öffentlicher Gewalt handeln, können im Rahmen des Zutritts zu den jeweiligen Gebäuden oder Räumlichkeiten ebenfalls personenbezogene Daten erheben; Satz 1 gilt entsprechend.

„Verbotsprinzip“ – mit vielfachem Erlaubnisvorbehalt

Art. 6 Abs. 1 DSGVO – Rechtmäßigkeit der Verarbeitung [in einem dieser Fälle]:

a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

Einwilligung des Betroffen => Informationelle **Selbst**bestimmung!

Voraussetzungen:

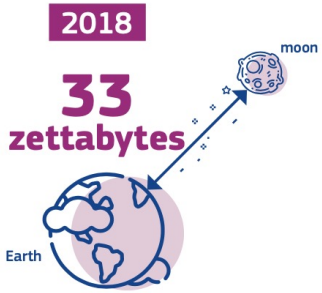
- ✓ Freiwillig
- ✓ Verständliche, transparente Information

Das Wesen des Datenschutzes

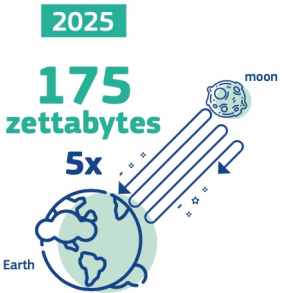
- Er dient nicht dem Schutz von Daten, sondern der **Menschen** (Persönlichkeitsschutz)
- Er soll verhindern, dass unbefugtes Wissen (für unredliche Zwecke) **missbraucht** wird
- Er fordert einen **sorgfältigen Umgang mit Daten**, auch im eigenen Interesse
- Rechte bei der Gestaltung von IT-Systemen gleich einbauen (**Privacy by design**)
- Datenschutz dient der **Gestaltung des digitalen Lebens**: das ist zuweilen anstrengend, aber unverzichtbar

→ Würde jemand die Straßenverkehrsordnung als Verhinderung von Mobilität sehen?

Umdenken in Brüssel: Entstehen eines „Datenwirtschaftsrechts“



Stored on 512 GB tablets, it would form a tower that reaches the moon.



Enough to make the journey to the moon and back five times.

Umdenken in Brüssel: Entstehen eines „Datenwirtschaftsrechts“

EUROPÄISCHE KOMMISSION

Datenstrategie

Data Governance Act

in Kraft

- Abbau technischer Hindernisse beim Datenteilen
- „Datenaltruismus“ und Datenspenden
- Zugang zu Daten der öffentlichen Hand

Data Act

- Datenzugangsrechte für IoT-Daten
- Verhinderung von Lock-In-Effekten
- Datenzugang für den Staat bei öffentlichem Notstand

Corona-Infektionen

Telekom gibt anonymisierte Mobilfunkdaten an das RKI weiter

European Health Data Space

- Bessere Primärnutzung von Gesundheitsdaten zur Erbringung von Gesundheitsdiensten
- Sekundärnutzung der Daten für Forschung, Entwicklung, Innovation

Konflikt europäischer Datenregulierung mit der DSGVO

Die Schutzziele der DSGVO sind „inkompatibel mit der Maxime des sharing is caring des neuen EU-Datenrechts“

Heinzke BetriebsBerater 18/2022, I.

DSGVO und Data Act „stehen [...] wie Altarbilder, die unterschiedliche Geschichten erzählen, nebeneinander.“

Thomas Fuchs, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit

Das Wesen der Datennutzung

- Ohne Datennutzung gäbe es **keine digitale Gesellschaft**, keine Digitalwirtschaft und keinen digitalen Staat
- Ohne Nutzung von Gesundheitsdaten gäbe **keine Gesundheitsvorsorge**, kaum eine wirksame Heilbehandlung, keine Diagnosen, keine Therapien
- **Gesundheitsforschung** braucht Gesundheitsdaten
- Datennutzung dient der **Gestaltung des digitalen Lebens**: das ist zuweilen eingreifend, aber unverzichtbar

→ Die Nutzung von Daten ist Grundrechtsausübungsvoraussetzung!

Und wie genau sind Chancen und Risiken abzuwägen?

Kriterien der Abwägung

- Kein Vorrang informationeller Selbstbestimmung (Privatheit): **Menschenbild eines gemeinschaftsgebundenen Individuums**
- DSGVO ist Verfahrensrecht. Datenschutzaufsichtsbehörden sind **Verfahrenswächter**. Sie dienen dabei einem speziellen Grundrecht, sind aber in ihrer Aufsichtspraxis **an alle Grundrechte gebunden**
- Inkaufnahme von **Risiken der Datenpreisgabe**: Gesundheitsschutz und andere Grundrechtsgewährleistungen rechtfertigen, ja fordern sogar „Eingriffe“
- Besonders in Krisen: „Datenschutz“ konzentrieren auf **Missbrauchsabwehr**

→ **BfDI und LfD(I) tragen als „schrankenlose Behörden“ (*Winfried Veil*) viel Verantwortung!**

Zusammenfassende Thesen

Genauso wie die DSGVO und die Datenschutzgrundrechte eine Datenschutzfolgeabschätzung verlangen, lässt sich aus den kollidierenden, der Datennutzung entgegengebrachten Grundrechten eine Pflicht zur Folgeabschätzung im Hinblick auf jegliche Datenschutzaufsichtsmaßnahmen herleiten. Die Datenschutzaufsichtsbehörden sind in Deutschland an die Beachtung aller (!) Grundrechte gebunden (Art. 1 Abs. 3 GG), also auch solchen, die eine verstärkte Datennutzung ermöglichen oder einfordern.

Die Datennutzung als Grundrechtsausübungsvoraussetzung darf nicht übermäßig eingeschränkt werden. Deshalb muss in jeder Aufsichtsmaßnahme begründet werden, wie sich diese auf (legitime) Datennutzung auswirkt und welche Abwägungskriterien der Entscheidung zugrundeliegen. Das Ergebnis muss justitiabel sein.

„Datenschützer“ sollen nicht auf der „hellen Seite“ stehen, sondern ihre technische und rechtliche Expertise zum Wohle Aller zur Verfügung stellen. Nur so gelingt eine akzeptanzstiftende Gestaltung der Digitalen Transformation.

A. Datenschutz im Kontext zunehmender Digitalisierung, Automatisierung und Vernetzung

I. Digitalisierung und Datenverarbeitung

Die Verarbeitung von Daten ist ein seit Jahrtausenden erarbeitetes und sich ständig weiterentwickelndes Kulturgut der Menschheit. Dies belegen Zeugnisse wie Zählsteine, Keilschriftdokumente oder die Erfassung der „Zehn Gebote", die auf Steintafeln niedergeschrieben und damit festgehalten („gespeichert") wurden, um ihre Rezeption und Weiterverarbeitung zu erleichtern und wichtige Gedanken für die Nachwelt zu erhalten. Auch dabei handelt es sich um eine strukturierte Sammlung von Aussagen, mit oder ohne konkreten Personenbezug. Lange Zeit war **Papier das Hauptträgermedium** der Datenverarbeitung, bis mit der Entwicklung moderner Computer die **elektronische Datenverarbeitung** Einzug in die Behörden, Unternehmen und auch in die Haushalte der Menschen gehalten hat.[1] Die fortschreitende Digitalisierung hat wiederum zu einem starken Anstieg[2] des Datenaufkommens geführt. Jeder digitale Prozessschritt erzeugt zusätzlich Metadaten, durch die Verknüpfung von Daten entstehen neue Kontexte, aus denen wiederum Informationen gewonnen werden, die in weiteren Daten verkörpert werden. 1

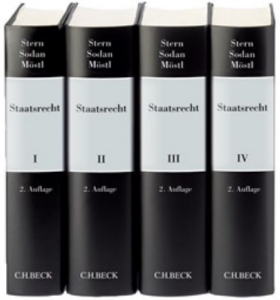
[1] Zur Geschichte der (automatisierten) Datenverarbeitung vgl *Simitis/Hornung/Spiecker gen. Döhmann* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Einl. Rn. 6 ff.

[2] Hierzu Tätigkeitsbericht der Bundesnetzagentur Telekommunikation 2020/2021, abrufbar: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Taetigkeitsberichte/2021/Telekommunikation2020.pdf?__blob=publicationFile&v=4 (abgerufen am 2.2.2022).

CDPS
TUM CENTER FOR DIGITAL PUBLIC SERVICES

TUM

Ausführlicher *Heckmann/Paschke*, Datenschutz, in:



Drucken

Ankündigung | Toptitel

Stern / Sodan / Möstl

Das Staatsrecht der Bundesrepublik Deutschland

Gesamtwerk in 4 Bänden

Band I: Historische Grundlagen und Grundbegriffe des Staatsrechts, Strukturprinzipien der Verfassung. Band II: Staatsorgane, Staatsfunktionen, Finanzwesen. Band III: Allgemeine Lehren der Grundrechte. Band IV: Die einzelnen Grundrechte

Handbuch
Buch. Hardcover (In Leinen)
2., vollständig neu bearbeitete Auflage. 2022
Rund 5000 S.
C.H.BECK. ISBN 978-3-406-77510-9

Twitter: @elawprof
dirk.heckmann@tum.de
www.tum-cdps.de

Mehr zu Datennutzung, Recht und Ethik bei #fornet23

Es sprechen u.a. Digitalministerin Judith Gerlach, Prof. Dr. Alena Buyx, Stefan Vilsmeier (CEO Brainlab), Nicole Formica-Schiller, Prof. Dr. Philipp Rauschnabel, Prof. Dr. Dr. Eric Hilgendorf, Prof. Dr. Anne Paschke u.v.a.m.