

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

Handelsblatt > Politik > Deutschland > Datenschutz: Warnung der Ethikrat-Chefin Buys 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 Datenschutzwarner 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 – PDSEG)
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:



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

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.



Ulrich Kelber, [wie er sich selbst sieht](#)

Screenshot: Twitter/UlrichKelber

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.“*

Die deutschen Datenschutzaufsichtsbehörden haben Ende November 2022 eine Stellungnahme zu Microsoft 365 veröffentlicht, die es in sich hat: Microsoft-Kunden können durch einen rechtswidrigen Einsatz der Software nicht rauskommen, mit anderen Worten: Microsoft 365 ist rechtsbrechend. Nach dem Willen der Anbieter soll fortwährend die Nutzung von Microsoft-Produkten als falsch eingestuft werden. Neben Deutschlands Unternehmen, Schulen, Städte und Gemeinden, Gerichte und Gesetzgebungsinstanzen die Empfehlung in diesem „digitalen Lockdown“ ernst, dass nicht ihre Systeme alles rül, denn es gibt keine alternative Software, die in der Pflicht ersetzbar wäre. Der Beschluss von der November wiederholt einseitig eine Bewertung eines Auftritts: keine der Datenschutznormen (DSG) aus dem Jahr 2000. Allerdings gab es damals Widerstand aus den eigenen Reihen: Das Datenschutzbüro von Baden-Württemberg, Bayern, Hessen und der Saarland war die Bewertung zu unklar. Vor allem eine nur (wahrscheinlich) Vertragsbeziehungen von Microsoft zur Grundlage der Darstellung gemacht werden. Es habe keine eigenständige Prüfung der Technik stattgefunden. Den anderen seien rechtswidrige Grundrechte verletzt worden, da Microsoft nicht hinreichend angekündigt worden sei. Das heißt: die Grenzen der Nutzung von „Microsoft-Verbot“. Der Fall breitet einen konstruktiven Ausgang und verleiht eine grundsätzliche Bewertung.

1. Datenschutzrecht

Europa hat im Jahr 2018 die Datenschutzverordnung (DSGVO) ins Werk gesetzt und eine bedeutsame Grundlage für Datenschutz geschaffen. Das Gesetz ist viel besser als sein Ruf. Es gibt schon in einem ersten Artikel viele abgewogene weiche Möglichkeiten von Erfolgen. Das Datenschutzrecht schützt natürliche Personen bei der Verarbeitung ihrer Daten. Zweitens: Das Datenschutzrecht schützt die Wirtschaft bei der Verarbeitung der Daten zu deren ökonomischen, wirtschaftlichen Vorteil im Binnenmarkt. Drittens: Es ist ein Recht, das mit Datenschutz gereicht: keine Verträge 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 praktischer Hinsicht, also in einem harmonischen Verhältnis mit dem Datenschutz gebracht werden müssen. Weiter und entscheidend: Die Datenschutz- und die Rechte der KI-Verordnung oder die Daten- und die Rechte der KI-Verordnung sind die einzigen Erben des Ansatzes des vollständigen Einsetzes von Daten zum Wohl von Gesellschaft, Wirtschaft und Staat auf Basis der DSGVO.



**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

Es hilft auch Unternehmen und Behörden, dass sie können zuverlässige Anbieter auswählen. Insgesamt gilt es, mit Wirtschaft, Wissenschaft und Gesellschaft fortwährend zusammenzuarbeiten. Die Stellung Datenschutz des Bundes sowie der Länder, die Datenschutz für die Anonymisierung personenbezogener Daten und einen abgegrenzten Prozess. Insbesondere für die Durchsetzung der Anonymisierung, verpflichtend. Die Praxis steht damit kleiner Handreichungen. Im Rahmen des Digitalisierungs der Bundesregierung hat die folgende Gruppe Datenschutz der Bundesministeriums schon im Jahr 2019 einen entsprechenden Ansatz zur Prozessumstellung vorgelegt. Vertreter von Aufsichtsbehörden waren auch hier beteiligt beteiligt.

Mit der Digitalisierung leben bedeutet schon in der Gegenwart, dass eine sich dynamisch entwickelnde Zukunftstechnologie zu leben. Jede neue Technik von der Eisenbahn über die Automobil bis zum Fliegen verlangt die Menschheit ab, Risiken zu kalkulieren, wenn sie sich für einen Einsatz entscheidet. Das bedeutet, Vorkehrungen gegen verheerende Gefahren sorgfältig zu treffen und mit unvermeidbaren Risiken zu leben. Wir bekümmern in diesem Wissen jährlich weit mehr als eine Million Verfallsfälle rund um den Globus.

Auch Datenverarbeitung ist Risikotechnologie. Ein Smartphonensensor misst, was deutlich mehr als 100 Millionen Mal schneller als die Apple 11. Guidances Computer, der vor über 50 Jahren in der Mondraute verbaut war. Auch wenn damit heute jeder Kindersche Computer ein Ersatz als eine Apple-11-Rakete, kommt die neue Technik nicht als Raketenumschiffung daher. Wir erleben Datenverarbeitung als in hundertfacher Abhängigkeit von uns und füttern sie von sich bis Echo mit Privatwissen, das im Weltwissen der Nation aufsteigt. Wir wissen, dass jeder verarbeitete Endgeräten – vom Rasenmäher über Smartphon bis hin zu vernetzten Autos – mit persönlichen Daten in Text, Text, Bild und Standorten. Weil die Technik so einfach bedient werden kann, aber rechtlich so komplex ist, existiert, spielt und bruchst sich deren Blick so wenig wie Moderne Caras die Wirkung von Raketentests. Ohne deren Einsatz wollen wir aber auch nicht leben. Wir treffen gegen Vorkehrungen gegen die Risiken.

Die vorstehenden werden auch auf den gesellschaftlichen Normen der Fortbewegung oder gar auf die Nutzung einer Schreib- oder Videokamera als Werkzeugen verstanden werden. Auf Microsoft 365 können wir aktuell nicht verzichten, wenn das digitale Leben weitergeführt soll. Die menschliche Union hat sich dazu entschieden, mit einer eigenen Datenstrategie für den Binnenmarkt. Diese liegt auf der digitalen, wirtschaftlichen Weltkarte einzuzeichnen. Daran haben wir auch die USA, China und Indien. Wir machen uns im Bewusstsein der damit verbundenen Risiken zum Beispiel im Inneren 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.

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.“

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



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**.

der brutkasten NEWS VIDEO EVENTS JOBSUCHE

Unsere Storypages: Te

#toddurchdatenschutz ?

Nein!

Dominik Perlaki am 27.03.2020

Datenschutz vs. Menschenleben: Dann sterben halt 10 Mal so viele

Kommentar. In Südkorea und anderen asiatischen Ländern spielten Datennutzung und Tracking-Apps eine wichtige Rolle dabei, die Coronavirus-Pandemie schnell unter Kontrolle zu bringen. In Österreich fehlt dafür das solidarische Datenverständnis. Menschenleben sind scheinbar nicht so wichtig. Und die Wirtschaftskrise wird nebenbei noch schlimmer.

Kopiert, Jetzt teilen! Zusammenfassung aus

„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**

12. BayIfSMV
Fassung: 05.03.2021

Text gilt ab: 28.04.2021

Gesamtvorschrift gilt bis: 09.05.2021

Gesamtansicht     

§ 2 Kontaktdatenerfassung

¹Soweit 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.

²Die 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. ³Behörden, 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.

Gesetzliche Grundlage

Demokratische Legitimation

Verhältnismäßigkeitsgrundsatz

„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 Betroffenen => Informationelle **Selbstbestimmung**!

Voraussetzungen:

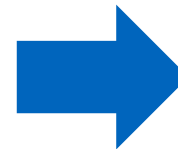
- ✓ Freiwillig
- ✓ Verständliche, transparente Information

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“



Umdenken in Brüssel: Entstehen eines „Datenwirtschaftsrechts“



Datenstrategie

in Kraft

Data Governance Act

- 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(1) 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**.

	Rn.
III. Verfahrensvorkehrungen zur angemessenen Ausgestaltung der Datenverarbeitung	64
IV. Typische Gefährdungslagen und Auflösung von Grundrechtskollisionen	70
1. Verarbeitung personenbezogener Daten als abstraktes Gefährdungsszenario	71
2. Konkrete Gefährdungslagen durch staatliche Datenverarbeitung	74
3. Gefährdungen durch ausländische Staaten und Geheimdienste	82
4. Gefährdungslagen durch private Akteure	86
V. Das Dilemma der Datenübermittlung in unsichere Drittländer	92
D. Datenpolitik zwischen Datenschutz und Datennutzung	97
1. Datennutzung als Voraussetzung der Grundrechtsgewährleistung	97
II. Datenschutz durch Technikgestaltung und Interessenausgleich	106
III. Datennutzung und Datenschutz in der deutschen Datenpolitik	108
IV. Datennutzung und Datenschutz in der europäischen Datenpolitik	110
E. Datenschutzrecht und Datenschutzpraxis	118
I. Die Rolle der Datenschutzaufsichtsbehörden für Auslegung und Anwendung der DS-GVO	119
II. Der Umgang mit Vollzugsdefiziten im Datenschutzrecht	128
F. Ausgewählte Probleme des Datenschutzrechts	132
I. Datenschutz in sozialen Netzwerken	132
1. Selbstdarstellung und Preisgabe eigener Daten in sozialen Netzwerken ..	136
2. Weitergabe von Daten Dritter in sozialen Netzwerken	139
3. Datenschutz bei Minderjährigen und Jugendschutz	140
II. Der Datenschutz im Spannungsverhältnis zu Wissenschafts-, Presse-, Informations- und Meinungsfreiheit	143
1. Datenverarbeitung im Kontext der Meinungs- und Informationsfreiheit ..	144
2. Datenverarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten	147
3. Datenverarbeitung zu Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken	148
III. Der Datenschutz im Beschäftigungsverhältnis	150

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 Anstieg² 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 Zur Geschichte der (automatisierten) Datenverarbeitung vgl. *Simitis/Horring/Spiecker* gen. *Döhmman* in: *Simitis/Horring/Spiecker* gen. *Döhmman*, *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/Telekommunikation20201.pdf?__blob=publicationFile&v=4 (abgerufen am 2.2.2022).

Ausführlicher *Heckmann/Paschke*, Datenschutz, in:



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

Drucken

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

Mehr zu Datennutzung, Recht und Ethik bei #fornet23



Digitale Verantwortung Digitalpolitik For..Net Symposium

📅 20. April 2023 - 21. April 2023 📍 IHK für München und Oberbayern

Datennutzung für Medizin, Verwaltung und Justiz | Neue rechtliche und ethische Fragen zu Künstlicher Intelligenz und eXtended Reality



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.