STIFTUNG DATENSCHUTZ

Stiftungsbrief **Winter 2025**

Überblick

3 **Nur sicher ist sicher.**
Eine Kampagne für den Datenschutz

6 **Worum geht es wirklich?**
Bericht vom Datentag im September 2025

9 **Palantir: Big Data for Big Brother**
Datenschutzrechtliche Einordnung

16 **Splitter**

Liebe Leserinnen und Leser,

wann haben Sie zuletzt ein Dosentelefon für vertrauliche Gespräche genutzt? Oder finden Sie auch, dass diese Lösung keinen ausreichenden Schutz bietet? Da sind wir ganz Ihrer Meinung. In unserer Image-Kampagne für den Datenschutz schlagen wir noch weitere skurrile Lösungen vor, um persönliche Daten zu schützen. Alles natürlich mit einem Augenzwinkern, denn: Nur sicher ist sicher!

Unser DatenTag im September führte das Thema der Kampagne fort. Wir diskutierten mit den Referierenden und Gästen zum „Datenschutz als Grundrecht für die Gesellschaft“. Leidenschaftliche, aber auch bestürzende Beiträge führten uns vor Augen, was und wen der Datenschutz eigentlich schützt und was es bei seiner Durchsetzung noch zu verbessern gibt.

Daran anknüpfend macht sich Kirsten Bock, Wissenschaftliche Leiterin bei der Stiftung Datenschutz, Gedanken über Palantir, mit dessen Einsatz ein Überwachungsstaat droht und nationale Sicherheitsfragen in fremde Hände gegeben werden.

Im Juli startete die neue Rubrik ***Datenschutz im Fokus*** auf unserer Website, in der wir datenschutzrechtlich relevante Themen kurz einordnen und kommentieren. Ein im November erschienenes Gutachten beleuchtet das besondere Schutzbedürfnis von Kindern und Jugendlichen. Außerdem gibt es Neuigkeiten aus dem DatenschutzArchiv.

Vermutlich wie Sie auch, sind wir gespannt, wie es mit den Vorhaben zur DSGVO-Reform weitergeht. Auch das nächste Datenschutzjahr verspricht also, spannend zu bleiben. Bis dahin wünschen wir Ihnen während der Feiertage Zeit für inspirierende Gespräche oder laute Spielerunden und den einen oder anderen datenschutzrechtlich unbedenklichen Cookie.

Viel Spaß bei der Lektüre des Stiftungsbriefs!

Herzlich grüßt

Frederick Richter,
Vorstand der Stiftung Datenschutz

EINE KAMPAGNE FÜR DEN DATENSCHUTZ

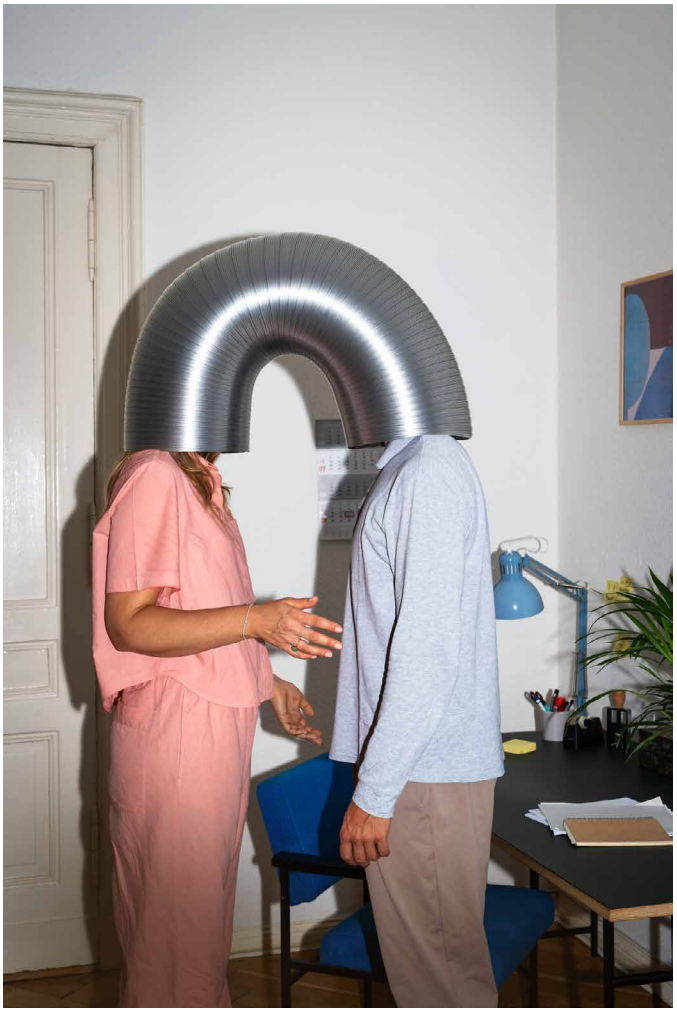
Nur sicher ist sicher.

Wir bei der Stiftung Datenschutz finden schon lange, dass die gängigen Narrative zum Datenschutz veraltet sind. Man sieht immer die gleichen Symbole (Vorhängeschloss, anyone?) und hört die gleichen Begriffe. Aber wenn die DSGVO nur mit Wörtern wie Datenschutzdschungel und Bürokratiemonster in Verbindung gebracht wird, dann ist klar, dass der dahinterliegende Gedanke eines für alle Menschen geltenden Grundrechts zunehmend verschwindet. Vor diesem Hintergrund haben wir uns im Sommer aufgemacht, das Narrativ zu ändern.

Wir haben eine Image-Kampagne für den Datenschutz entwickeln lassen, bei der uns zwei Aspekte wichtig waren: Zum einen sollte deutlich werden, dass Datenschutz keine individuelle Aufgabe ist, sondern dass sie auf gesellschaftlicher und politischer Ebene gelöst werden muss. Zum anderen wollten wir hervorheben, dass es nicht darum geht, Daten zu schützen, sondern immer die Personen, auf die sie sich beziehen. Herausgekommen sind vier Motive, die auf humorvolle Weise zeigen, dass selbstgebastelte Einzellösungen keinen wirksamen Datenschutz bieten.

Die Motive waren ein Hingucker und Publikumsmagnet beim Kampagnen-Auftakt am 23. August 2025 zum Tag der offenen Tür der Bundesregierung im Bundesministerium der Justiz und für Verbraucherschutz, wo wir sie erstmals einem Publikum vorgestellt haben. Die aufmerksamkeitsstarken Bilder waren außerdem mehrere Wochen an Berliner ÖPNV-Haltestellen zu sehen. Zusätzlich schaffen sie in digitalen Kanälen mehr Sichtbarkeit für den Datenschutz. Die Kampagne regt zum Nachdenken an und verdeutlicht Entscheider*innen, dass Datenschutz kein individuelles Thema sein kann.

Privatsphäre?
Nur sicher ist sicher.



Freiheit ist keine Bastelstunde.

Behelfsmäßige Einzellösungen bieten nur eine trügerische Sicherheit, denn echter Schutz muss von Anfang an in digitalen Systemen verankert sein.

Diskurs?
Nur sicher ist sicher.

Demokratische Debatten brauchen echte Sicherheit.

Ein starker Datenschutz sichert die vertrauliche Kommunikation und schützt die Souveränität unseres Rechtsstaats vor Manipulation und unzulässiger Einflussnahme.

Sauber?
Nur sicher ist sicher.

Digitale Integrität ist keine individuelle Last.

Das Grundrecht auf digitale Unversehrtheit verlangt nach Lösungen, die sich gewaschen haben: politische und herstellerseitige Garantien, die Geräte frei von Schadsoftware und Spionage halten.

Inkognito?
Nur sicher ist sicher.

Wirksamer Schutz funktioniert nur gemeinsam.

Datenschutz ist dann am stärksten, wenn wir ihn als Service für die Gemeinschaft verstehen, der faire Chancen sichert und strukturelle Benachteiligung verhindert.

Mehr zur Kampagne

→ https://stiftungdatenschutz.org/veroeffentlichungen/nur-sicher-ist-sicher

Mit einer Kampagne ist es natürlich nicht getan. Auch unser DatenTag im September griff daher das Thema „Datenschutz als Grundrecht für die Gesellschaft“ auf. Als Stiftung arbeiten wir weiterhin kontinuierlich daran, Datenschutz als hohes Gut der Demokratie gesellschaftlich und politisch zu verankern.

BERICHT VOM DATENTAG IM SEPTEMBER 2025

Worum geht es wirklich?

Dem Thema Datenschutz kann man sich auf vielfältige Weise nähern. In unserer DatenTag-Konferenzreihe haben wir das bereits getan: Wir haben rechtliche Diskurse zur DSGVO geführt, praktische Fragen zur Corona-Warn-App oder zur Anonymisierung diskutiert, und uns kniffligen Spezialgebieten wie Datentreuhand und Datenpreisgabe gewidmet. Zur 20. Ausgabe des DatenTags haben wir das große Ganze betrachtet. Am 16. September 2025 drehte sich deshalb alles um die Frage: Welche Rolle spielt das Grundrecht „Datenschutz“ für uns als Gesellschaft?

Mehr zum DatenTag

→ https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/datentag-datenschutz-grundrecht-gesellschaft-579

Dr. Johannes Dimroth, Ständiger Vertreter der Staatssekretärin im Bundesministerium der Justiz und für Verbraucherschutz, betonte in seinem Grußwort, dass die Fragen der Veranstaltung richtig gestellt seien – was und wovor schützt der Datenschutz? Die nachfolgenden Beiträge gaben darauf augenöffnende, leidenschaftliche und teils bestürzende Antworten.

Datenschutz als Bremse?

Prof. Dr. Hannah Ruschemeier (Universität Osnabrück) sprach in ihrer Keynote von Datenschutz als „Machtbegrenzungsinstrument". Trotzdem hielte sich aufgrund eines vagen Innovationsbegriffs immer noch die Mär vom Datenschutz als Bremse. Sie sah es als großes Problem, dass nicht-rechtskonforme Angebote einfach hingenommen werden und fragte in diesem Zusammenhang: Was kostet es an Zeit und Aufwand, wenn wir keinen Grundrechtsschutz haben?

Diese Frage griff der Journalist Falk Steiner in der anschließenden Diskussion zur Innovation durch Regulierung auf – viele Unternehmen ignorieren seiner Ansicht nach, welche Kosten entstehen, wenn sie sich nicht an die DSGVO halten. Jan Philipp Albrecht von der Heinrich-Böll-Stiftung diagnostizierte ein Rechtsdurchsetzungsdefizit, wodurch auch volkswirtschaftlicher Schaden entstehe. Michael Will, Präsident des Landesamtes für Datenschutz Bayern, fand es deshalb sinnvoll, sich an einer wirksamen Rechtsdurchsetzung anstelle nur an der Höhe von Bußgeldern messen zu lassen.

Menschenfreundliche Innovationen

Rainer Rehak vom Weizenbaum-Institut bezeichnete die mit den personenbezogenen Daten verknüpften Menschen als die Schutzobjekte des Datenschutzes und die Datenverarbeitenden als Gefahr. Das Argument des Datenschutzes als Verhinderer ließ auch er nicht gelten: Technisch sei vieles möglich, zuallererst solle Innovation aber menschenfreundlich sein.

Welche Folgen es haben kann, wenn personenbezogene Daten nicht als schützenswert gelten, zeigte der Journalist Ingo Dachwitz eindrucksvoll auf. Die Netzpolitik-Recherche zu den Databroker Files ermöglichte eine Erstellung von Bewegungsprofilen, die Rückschlüsse auf sicherheitsrelevante Berufsgruppen zulassen. Die Daten stammen aus Handy-Apps, die unter anderem GPS-Daten für Werbezwecke weitergeben und wurden dem Recherche-Team kostenlos von einem Datenhändler zur Verfügung gestellt. Dachwitz ist der Ansicht, dass beim Datenhandel automatisch gegen die Zweckbindung der Datenverarbeitung verstoßen werde.

Das Problem mit den Beschwerden

Doch wie läuft es eigentlich, wenn Betroffene sich über eine unrechtmäßige Datenverarbeitung beschweren? Zur Überlastung der Behörden berichteten Dr. Nina Herbort und Dr. Giuliana Schreck von Short Law aus ihrer Zeit bei der Datenschutzaufsicht. Diese befände sich in einer Zwickmühle. Einerseits gebe es viele Verstöße und seien Beschwerden ein Grundrecht der Betroffenen, andererseits könnten die Behörden ihre weiteren Aufgaben aufgrund der Fülle an Beschwerden kaum noch wahrnehmen.

In einer Diskussionsrunde zum bürgernahen Datenschutz bekräftigte Dr. h.c. Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein, diese Sichtweise: Auskunft werde nicht absichtlich spät gegeben, es fehle schlicht an Ressourcen. Dr. Stefan Brink vom Wissenschaftlichen Institut für die Digitalisierung der Arbeitswelt mochte trotzdem keine Hürden errichten, um die Beschwerden einzudämmen. Laut Lina Ehrig vom Verbraucherzentrale Bundesverband habe der Verbraucherschutz die Möglichkeit, kollektivrechtlich tätig zu werden und systemische Datenschutzprobleme zu adressieren. Weil auch dort die Ressourcen begrenzt seien, wähle der Verbraucherschutz Bundesverband Verfahren aus, die Breitenwirkung erzielen können. Denn: Recht entfaltet nur seine Wirkung, wenn es durchgesetzt wird. Elisabeth Niekrenz von Spirit Legal sah Sammelklagen ebenfalls als besseren Hebel.

Datenschutz ist kein Luxusgut

Den Programmpunkt „Datenschutz als Demokratieschutz“ eröffnete Markus Beckedahl vom Zentrum für Digitalrechte und Demokratie mit dem eindringlichen Aufruf, einen Überwachungsstaat nicht schlüsselfertig bereitzustellen. Autoritäre Technologien würden mit großer Geschwindigkeit exportiert. Er appellierte, Vorsicht walten zu lassen. Elisa Lindiger von Superrr Lab nahm uns bei ihren Überlegungen dazu mit, in welcher Welt wir eigentlich leben wollen. Zum Stichwort Innovationsbremse fragte sie, welche Innovation das sein solle, die es wert wäre, Grundrechte aufzugeben.

Sofia Vester, Gründerin von fix&fertig – Datenschutzhilfen für Zivilgesellschaft, forderte, dass Datenschutz kein Luxusgut sein dürfe. Unterfinanzierte Vereine dürften nicht aus Kostengründen auf die kostenlosen Angebote von US-Unternehmen angewiesen sein. Außerdem rief sie in Erinnerung, dass die Einschüchterung von Engagierten ein großes Problem sei. Datenschutz sollte hier unmittelbar als Schutz wirken.

Nur sicher ist sicher!

In stiftungseigener Sache stellten Theresa Wenzel, Kommunikationsreferentin bei der Stiftung Datenschutz, und Nils Prym, Creative Director bei der von der Bundesstiftung beauftragten Agentur I Like Visuals, eine neue Image-Kampagne für den Datenschutz vor. Unter dem Motto „Nur sicher ist sicher“ zeigen skurrile, selbstgebastelte Datenschutzlösungen, dass Datenschutz nicht als individuelles Problem betrachtet werden darf und deshalb auf politischer und gesellschaftlicher Ebene gelöst werden muss.

Den Abschluss des DatenTags bildete die Keynote der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Prof. Dr. Louisa Specht-Riemenschneider. Zuerst blickte sie wortwörtlich mit rosaroter Brille in eine von perfekt funktionierendem Datenschutz gezeichnete Zukunft. In der Realität attestierte sie jedoch, dass das Konzept der Einwilligung gescheitert sei. Ihr hartes Urteil: Das Datenschutzrecht schütze momentan nur auf dem Papier. Sie betonte den Bedarf an systemischen Lösungen für systemische Probleme. Sie war sich bewusst, wie schlecht der Ruf des Datenschutzes mitunter ist. Eine Verbesserung sei zwar wünschenswert, aber: „Datenschutz darf nerven. Hauptsache, er funktioniert!“

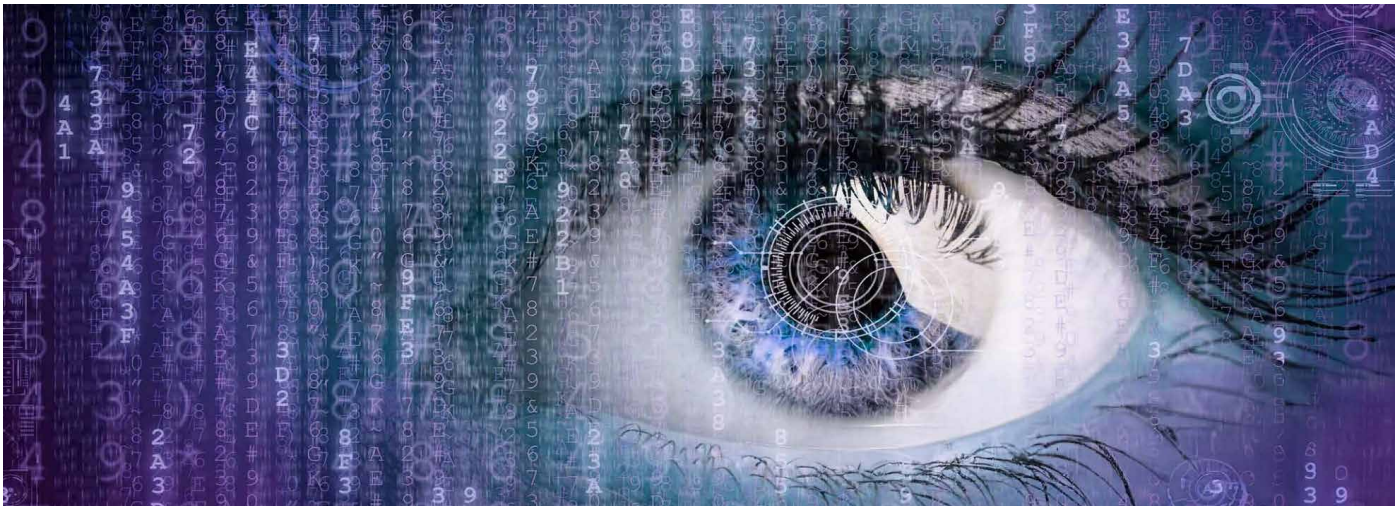
Kirsten Bock ist Juristin mit Schwerpunkt Rechtsphilosophie und wissenschaftliche Leiterin der Stiftung. Sie bearbeitet Problemstellungen zum Datenschutzrecht, zur Anonymisierung von Daten sowie zur Zertifizierung von Datenschutzbeauftragten und betreut wissenschaftliche Projekte.

DATENSCHUTZRECHTLICHE EINORDNUNG

Palantir: Big Data for Big Brother[1]

von Kirsten Bock

Wer durch die Nachrichtenseiten im Internet stöbert, stößt unweigerlich auf Berichte über eine Ausweitung von Überwachungsmaßnahmen. Eine Firma steht dabei besonders im Fokus: Palantir (abgeleitet von Palantír, der unzerstörbaren sehenden Steinkugel aus J.R.R. Tolkiens Herr der Ringe). Während vereinzelt Bundesländer die deutsche Tochter des Unternehmens, Palantir Technologies GmbH, bereits beauftragt haben,[2] wird von anderen der Einsatz kritisch[3] gesehen.



So forderte der Bundesrat im März den Einsatz als Interimslösung.[4] Bundesinnenminister Dobrindt gab Ende Juli 2025 bekannt, den bundesweiten Einsatz im Rahmen eines „Sicherheitspakets" prüfen zu lassen.[5] Die Innenministerkonferenz sieht den Einsatz eines US-amerikanischen Unternehmens hingegen kritischer und strebt eine vergleichbare europäische Lösung an.[6]

Die zu lösenden Aufgaben werden von den Befürwortern eines Palantir-Einsatzes nur skizzenhaft beschrieben. Im Wesentlichen möchten sie die

1 Rolf Gössner, Laudatio auf Peter Beuth, Big Brother Awards 2019.
2 Baden-Württemberg, Bayern, Hessen und Nordrhein-Westfalen.
3 Hamburg setzt sich für eine europäische Lösung ein, ebenso offenbar Bremen, Mecklenburg-Vorpommern, Niedersachsen, Saarland, Schleswig-Holstein und Thüringen.
4 https://www.heise.de/news/Palantir-als-Interimsloesung-Bundesrat-fordert-schnellen-Einsatz-fuer-die-Polizei-10325605.html, https://dip.bundestag.de/vorgang/entschlie%C3%9Fung-des-bundesrates-priorisierung-ausk%C3%B6mmliche-finanzierung-und-rechtssichere-implementierung-eines/320143
5 https://www.lto.de/recht/nachrichten/n/palantir-einsatz-bundesinnenminister-alexander-dobrindt-prueft-einsatz-analyse-software-palantir-usa.
6 Beschluss der 223. Sitzung der IMK, https://www.bundesrat.de/IMK/DE/termine/to-beschluesse/2025-06-13_DOK/beschl%C3%BCsse.pdf

gleichen technischen Möglichkeiten haben, die für kriminelle Handlungen genutzt werden, um so schwere Straftaten zu verhindern.

Schon konkreter sind die Beschreibungen des Verfahrens: Man wolle Muster erkennen und Vorhersagen treffen können.[7] Etwas verharmlosend wird dieses Bestreben auch als Einrichtung eines „Datenhauses" und „Datenhaus-ökosystems"[8] beschrieben. Ähnlich wie bei der Rasterfahndung der Polizei soll sich der Einsatz nicht gegen bestimmte Personen oder Gruppen richten, sondern gegen die Gesamtbevölkerung. Mit den neuen digitalen Werkzeugen sind nicht nur Verdächtige, sondern auch Kontaktpersonen, Opfer und Zeugen betroffen.[9] Zur Zusammenführung, Analyse und Mustererkennung der damit entstandenen Datenbestände soll dann die Software bzw. das Betriebssystem von Palantir sorgen.

Demgegenüber werden grundrechtliche Bedenken geltend gemacht, weil eine Maßnahme, die in Grundrechte eingreift, die Zwecke für die sie eingesetzt wird, hinreichend konkret beschreiben muss. Die Gesellschaft für Freiheitsrechte (GFF) hat daher gegen den Einsatz von systematischen polizeilichen Datenanalysen im bayerischen Programm „VeRA" auf Basis von Gotham Verfassungsbeschwerde eingereicht.[10] Die massenhafte Auswertung von Daten verletze unter anderem das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) und das Fernmeldegeheimnis (Art. 10 Abs. 1 GG), so die GFF.

Was ist Palantir?

Bei Palantir handelt es sich um ein US-amerikanisches Unternehmen, das von Alex Karp als CEO geführt wird und zu dessen Gründern und Financiers die Milliardäre Peter Thiel und Larry Allison sowie der US-Geheimdienst CIA zählen. Über den Palantir-Investor David Sacks, der von Donald Trump zum AI- und Crypto-Zar ernannt wurde, besteht ein direkter Draht zum US-Präsidenten, während Vizepräsident Vance eine enge Verbindung zu Peter Thiel hat. Alle vier sind mit Äußerungen aufgefallen, die keine aufgeschlossene Haltung zu Demokratie, Liberalismus und Rechtsstaat zeigen.[11]

Palantir gilt als „Schlüsselfirma in der Überwachungsindustrie".[12] Die Firma hat sich auf die Integration und Analyse großer heterogener Datenbestände spezialisiert und kann zur Überwachung der Gesamtbevölkerung eines Staates eingesetzt werden.

---

7 https://dip.bundestag.de/vorgang/entschlie%C3%9Fung-des-bundesrates-priorisierung-ausk%C3%B6mmliche-finanzierung-und-rechtssichere-implementierung-eines/320143

8 So etwa Andreas Dressel, Senator der Hansestadt Hamburg in einer Erklärung im Deutschen Bundesrat am 21. März 2025, https://www.bundesrat.de/SharedDocs/downloads/DE/plenarprotokolle/2025/Plenarprotokoll-1052.pdf.

9 https://netzpolitik.org/2025/gesichtserkennung-und-ki-innenminister-dobrindt-plant-neues-sicherheitspaket/

10 https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/blackbox-palantir-gff-erhebt-verfassungsbeschwerde-gegen-massenhafte-datenauswertung-durch-polizei-in-bayern

11 Vgl. z.B. Thiel/Sacks: The Diversity Myth: Multiculturalism and the Politics of Intolerance at Stanford.

12 https://www.heise.de/news/Palantir-Wachsender-Widerstand-gegen-US-Big-Data-Software-fuer-die-Polizei-10351797.html

Wie die Dienstangebote von Palantir technisch und funktional einzuordnen sind, wird unterschiedlich beschrieben. Während Palantir selbst von „Betriebsplattformen“ spricht, kommt die Einordnung als „Betriebssystem“ vermutlich näher. Zumindest handelt es sich nicht ausschließlich um „Software“.

Palantir bietet vor allem Militärs, Sicherheitsbehörden und Nachrichtendiensten sein Betriebssystem „Gotham“ an. Der Name, angelehnt an Batmans Gotham City, ist kein Zufall. Gotham ist eine modulare, umfassende Datenintegrations- und Analyseplattform, auf die verschiedene Analysefunktionen und KI-Module aufgesetzt werden können. Das System integriert strukturierte und unstrukturierte Datenquellen.[13] Nach eigenen Angaben baut Palantir für seine Kunden die digitale Infrastruktur, die es ihnen ermöglicht, „in komplexen Datenumgebungen“ und in „fragmentierten Datenlandschaften“ zu arbeiten und die „üblichen Herausforderungen zu bewältigen, die damit verbunden sind, dass Daten auf verschiedene Systeme und Formate verteilt sind“.[14]

Zudem offeriert Palantir „Foundry“ für die Datenintegration, -modellierung und -analyse, womit Entscheidungsprozesse unterstützt werden. Beide Plattformen sind modular aufgebaut und bieten die Möglichkeit, über eine interne Datenlogik (Ontologie) Daten aus unterschiedlichen Quellen miteinander zu verbinden, ohne die Daten selbst an einem weiteren Ort zusammenzuführen. Technisch handelt es sich insoweit um eine Form der Datenmodellierung mit Zugriffsrechten und extremen Analysemöglichkeiten in Form von Software-as-a-Service.[15] Beide Anwendungen nutzten KI- und Machine-Learning-Algorithmen. Gotham und Foundry bilden die technische Grundlage für die bereits bestehenden Anwendungen HessenData (Hessen), DAR (NRW) oder VeRA (Bayern).

Was spricht für einen Einsatz?

Die Verhinderung schwerer Straftaten kann als legitimer Zweck der Nutzung von Analyse- und Mustererkennungssoftware gelten. Eine manuelle Auswertung sehr großer Datenmengen sei unter Zeitdruck bei der derzeitigen Ausstattung kaum mehr zu bewältigen, heißt es auf Seiten der Polizei. Der Einsatz von Software sei geeignet, die händische Arbeit der Analysten zu ersetzen.[16]

Die von Palantir erstellten Betriebssysteme können riesige Datenmengen aus unterschiedlichen Quellen blitzschnell zusammenführen und analysieren. Diese Datenintegration ermöglicht, Informationen aus Polizeidatenbanken, Gesundheitsdaten und sogar Social-Media-Inhalten für umfassende Analysen und Prognosen zusammenzuführen. Dies kann Ermittlungen beschleunigen und die Chancen erhöhen, Muster und Zusammenhänge bei komplexen Fällen aufzudecken. Für Beschäftigte der Polizei würden durch die Analysetools nicht mehr Informationen als bisher zugänglich gemacht werden.

13 https://www.wired.com/story/palantir-what-the-company-does/#intcid=_wired-article-bottom-recirc_adcafb7b-6954-43dd-8585-73e99222f6cf_roberta-similarity1
14 https://www.palantir.com/palantir-is-still-not-a-data-company/
15 https://www.heise.de/hintergrund/Missing-Link-Machtzentrale-Palantir-eine-Software-lenkt-Organisationen-10463034.html
16 https://www.lto.de/recht/nachrichten/n/bayern-lka-zusammenarbeit-mit-palantir-daten-aufbereitung-anaylse-grundrechte

Was spricht gegen den Einsatz?

Palantir steht exemplarisch für eine neue Generation datenanalytischer Anwendungen. Eine zentrale Problematik liegt in der engen technischen und strukturellen Bindung an das Unternehmen selbst. Das System ist proprietär aufgebaut, wodurch keine realistische Möglichkeit besteht, den Anbieter zu wechseln.[17] Diese Abhängigkeit schafft ein technologisches Lock-in, das den Handlungsspielraum öffentlicher Institutionen erheblich einschränkt.

Hinzu kommt die Intransparenz der Funktionsweise. Weder die zugrundeliegende Software-Architektur noch die Ontologie sind öffentlich dokumentiert oder durch unabhängige staatliche Stellen überprüfbar. Die Art und Weise, wie Palantir Daten verknüpft, klassifiziert und operationalisiert, bleibt damit eine Black Box. Über diese Ontologie wird jedoch unmittelbar die Entscheidungslogik der nutzenden Organisationen beeinflusst – ein Umstand, der faktisch zu einer algorithmischen Steuerung durch ein privatwirtschaftliches Unternehmen führt.

Die Implementierung der Plattform erfordert darüber hinaus eine enge Zusammenarbeit mit Palantir. Dazu werden sogenannte Forward Deployed Engineers (FDSE) – auch genannt „Delta" – zu den Kunden entsendet, die direkt bei den Anwenderorganisationen tätig sind.[18] Diese US-amerikanischen Mitarbeitenden erhalten so tiefen Zugang zu sicherheitsrelevanten Infrastrukturen und Daten. Angesichts der gesetzlichen Auskunftspflichten gegenüber US-Nachrichtendiensten ergibt sich daraus ein erhebliches sicherheitspolitisches Risiko für nationale Behörden und kritische Infrastrukturbetreiber.

Kenntnisse der Datenbanken können ein hohes Sicherheitsrisiko darstellen, das für Cyberangriffe auf zentrale Datenbanken genutzt werden kann. In einer Zeit schwindenden Vertrauens in die amerikanische Regierung mahnen deutsche Politiker wie Konstantin von Notz, Kooperationen mit solchen Unternehmen seien sicherheitspolitisch fragwürdig und stünden im Widerspruch zu den Interessen europäischer Staaten.[19]

Neben den geopolitischen Fragen bestehen auf operationeller Ebene zudem gravierende Fragen der Kontrolle und Transparenz. Da die Plattform weitreichende Grundrechtseingriffe ermöglicht, müssen rechtliche Zwecke klar definiert und verhältnismäßig sein. Dies ist angesichts der intransparenten Funktionsweise und der fehlenden Evaluationsdaten zur Fehleranfälligkeit der Systeme kaum überprüfbar. Die Effektivität der Maßnahmen bleibt unbewiesen, während der Eingriffstiefe erhebliche Risiken gegenüberstehen.

Die technische Integration von Palantir eröffnet darüber hinaus Möglichkeiten, auch externe Datenquellen wie soziale Netzwerke oder Überwachungskameras einzubinden. Dieses Potenzial zeigt sich exemplarisch im Einsatz KI-gestützter Überwachungssysteme, etwa am Frankfurter Hauptbahnhof. Hier gelangen auch unbeteiligte Personen, Zeugen oder Opfer von Straftaten in den Fokus der Datenanalyse. Dies stellt einen Verstoß gegen das Prinzip

17 https://www.heise.de/hintergrund/Missing-Link-Machtzentrale-Palantir-eine-Software-lenkt-Organisationen-10463034.html
18 https://blog.palantir.com/a-day-in-the-life-of-a-palantir-forward-deployed-software-engineer-45ef2de257b1
19 https://taz.de/Ueberwachungssoftware-Palantir/!6081680/

der Zweckbindung staatlicher Datensammlung dar. Damit vergrößert sich das Risiko unbeabsichtigter oder willkürlicher Eingriffe in die Privatsphäre unschuldiger Personen.

Obwohl der Einsatz solcher Systeme offiziell auf schwere Straftaten begrenzt sein soll, ist eine technische Ausweitung auf leichtere Delikte möglich. Mit einer veränderten politischen Ausgangslage könnte der Anwendungsbereich leicht erweitert werden, ohne dass technische Hürden bestünden.

Außerdem ist wissenschaftlich zweifelhaft, ob die durch Palantir generierten Prognosen zur Kriminalitätsvorhersage valide und belastbar sind. Kriminologen verweisen darauf, dass die daraus abgeleiteten Muster häufig Scheinkorrelationen darstellen und zu diskriminierenden Entscheidungen führen können.[20]

Nicht zuletzt verursacht die Implementierung der Palantir-Systeme erhebliche Kosten,[21] deren Nutzen bisher weder empirisch nachgewiesen noch transparent kommuniziert wurde. Damit verbindet sich das Risiko einer Fehlallokation öffentlicher Mittel bei gleichzeitiger Gefährdung von Datenschutz, informationeller Selbstbestimmung und nationaler Souveränität.

Europäische Lösung als Alternative

Hamburg setzt sich für eine europäische Lösung ein, weil dies die derzeitige geopolitische Gesamtlage im Sicherheitsbereich erfordere.[22] Nur so könnten Rechtskonformität und Verfügbarkeit sichergestellt werden. Die Gefahr einer Einflussnahme durch ausländische Staaten sei ein einzukalkulierendes Risiko.[23]

Allerdings birgt auch eine europäische Lösung nach dem Vorbild der Palantir-Plattform Vorbehalte gegen eine weitreichende anlasslose Überwachung der Bevölkerung durch „heimliches Rastern einer großen Datenfülle aus verschiedenen Polizeisystemen“[24]. Letztlich bieten die bestehenden rechtlichen Einschränkungen nur einen schwachen Schutz. Landesgesetze können nicht nur einschränkend, sondern auch ausweitend geändert werden. Bei einem politischen Wechsel kann die Plattform in einer Weise genutzt werden, die der grundrechtlichen Ausprägung der Bundesrepublik fundamental entgegenstünde.

20 Butz, Felix, Polizei und Massendaten: Kriminologische Überlegungen zum Wandel polizeilicher Sozialkontrolle, in: Bliesinger et al. (Hg.), Kriminalität und Kriminologie im Zeitalter der Digitalisierung, Neue Kriminologische Schriftenreihe, Bd. 119, S. 33, 39 ff.

21 https://www1.wdr.de/nachrichten/landespolitik/nrw-polizei-datenbank-software-palantir-kosten-100.html

22 https://www.heise.de/news/Palantir-Wachsender-Widerstand-gegen-US-Big-Data-Software-fuer-die-Polizei-10351797.html

23 https://www.bundesrat.de/SharedDocs/downloads/DE/plenarprotokolle/2025/Plenarprotokoll-1052.pdf, S. 96 f.

24 https://netzpolitik.org/2025/verfassungsbeschwerde-das-problem-heisst-nicht-nur-palantir/

Automatisierte Datenanalyse zwischen Freiheitsrecht und Sicherheitsinteresse

Die zentrale Frage, welche Daten unter welchen Bedingungen in automatisierte Analysen und Mustererkennungen einfließen dürfen, lässt sich nicht allein auf Grundlage einfachgesetzlicher Regelungen, etwa durch Polizeigesetze, beantworten. Sie unterliegt vielmehr den verfassungsrechtlichen Vorgaben, insbesondere dem Schutz der informationellen Selbstbestimmung und den Freiheitsversprechen der Verfassung.

Der Staat darf rechtmäßig erhobene und gespeicherte Informationen zur Bekämpfung von Terrorismus und schwerer Kriminalität nutzen, sofern diese Maßnahmen legitimen Zwecken dienen, auf einer klaren gesetzlichen Grundlage beruhen und die Grundrechte der Bürger*innen wahren. Eine präzise Analyse solcher Daten kann im öffentlichen Interesse liegen und gehört zu den legitimen Aufgaben staatlicher Sicherheitsbehörden.

Problematisch wird der Einsatz automatisierter Analysesysteme jedoch dann, wenn Daten unbescholtener Bürger*innen in die Auswertung einfließen und der Zweckbindungsgrundsatz der polizeilichen Datenerhebung verletzt wird. Dies führt zur Aushöhlung rechtsstaatlicher Schranken und gefährdet das Vertrauen in die Polizei. Zeug*innen, Opfer und Hinweisgeber müssen sich darauf verlassen können, dass ihre Informationen ausschließlich zweckgebunden und sorgsam verarbeitet werden. Eine Strategie, die auf massenhafte, verdachtsunabhängige Datenerhebung – also auf Massenüberwachung – statt auf gezielte Ermittlungen auf Basis konkreter Verdachtsmomente setzt, ist mit einem demokratischen Rechtsstaat unvereinbar.

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung betont, dass die Freiheitswahrnehmung der Bürger*innen nicht umfassend erfasst und registriert werden darf (BVerfGE 125, 260, 324). Freiheit ist dabei als die Summe der Gewährleistungsgehalte der Grundrechte und grundrechtsgleichen Rechte zu verstehen.[25] Entsprechend ist die Nutzung von Analyse- und Auswertungssoftware stets am Schutzbereich dieser Grundrechte zu messen.

Neben den verfassungsrechtlichen Fragestellungen, ist die technische und institutionelle Vertrauenswürdigkeit der eingesetzten Systeme zu prüfen. Gerade unter dem Gesichtspunkt der „Souveränität“ erscheint der Einsatz von Software eines US-amerikanischen Unternehmens wie Palantir problematisch. Die enge Verzahnung mit US-Nachrichtendiensten und die rechtlichen Zugriffsmöglichkeiten nach dem Foreign Intelligence Surveillance Act (FISA) lassen Zweifel an der Sicherheit und Autonomie der Datenverarbeitung aufkommen.

Auch wenn das Unternehmen betont, keine Daten selbst zu speichern, bleibt über die Softwarearchitektur zumindest ein potenzieller indirekter Zugriff möglich. Selbst betreiberseitig abgeschottete Systeme, die auf Servern deutscher Behörden laufen, sind nicht zwingend sicher gegen Zugriffe durch

25 Pohle, Jörg, Freiheitsbestandsanalyse statt Überwachungs-Gesamtrechnung, fiff-Kommunikation 2019, Heft 4, S. 37, 40.

Mitarbeitende des Anbieters. Die fehlende Transparenz der Programmstruktur im Sinne einer „Black Box“ erschwert zudem die Kontrolle durch deutsche Behörden und Sicherheitsexperten erheblich.

Das BVerfG hat im Urteil zum Hessischen Polizeigesetz betont, dass es bei schwerwiegenden Eingriffen in das Recht auf informationelle Selbstbestimmung darauf ankommt, dass die Eingriffsschwelle vom Gesetzgeber klar definiert wird und dass Analyse und Auswertung hinreichend bestimmt formuliert sein müssen. Insbesondere müsse bei der Verarbeitung von Informationen klar zwischen Personen, von denen eine Gefahr ausgehe, und Daten solcher Personen, die unbeteiligt sind, klar unterschieden werden können.

Ausblick

Über den Einsatz der Palantir-Software wird das Bundesverfassungsgericht entscheiden. Es wird darauf ankommen, ob die durch die Anwendung der Software erfolgenden Grundrechtseingriffe verfassungsrechtlich gerechtfertigt werden können. Eine solche Rechtfertigung kann nur gelingen, wenn die Anwendung im Verhältnis zu den mit ihr verfolgten Zwecken verhältnismäßig ist. Spannend wird hier, ob das BVerfG den Einsatz zum Anlass nehmen wird, auch die Geeignetheit und die Erforderlichkeit des Einsatzes zu prüfen. Gerade die Erforderlichkeit spielt bei der datenschutzrechtlichen Beurteilung eine besondere Rolle. Die Verarbeitung eines Datums ist datenschutzrechtlich nur dann erforderlich, wenn der legitime Zweck der Verarbeitung ohne die Verarbeitung des Datums nicht erfüllt werden kann. Eine solche Erforderlichkeit dürfte bei Gesamt-Analysen und Auswertungen nicht bestehen.

Palantir ist mehr als nur ein technisches Werkzeug. Es ist ein Machtinstrument, das Daten, Entscheidungen und letztlich ganze Behördenstrukturen weitgehend unbemerkt und kaum überprüfbar beeinflusst. Wer über den Einsatz solcher Systeme spricht, muss daher nicht nur über technische Beherrschbarkeit, sondern auch über demokratische Kontrolle und die Freiheitsversprechen des liberalen, freiheitlichen Rechtsstaates sprechen.

Dieser Text erschien zuerst in einer kürzeren Fassung in der Zeitschrift Computer und Arbeit 12/25.

Splitter

Das besondere Schutzbedürfnis von Kindern und Jugendlichen

In unserer Arbeit mit Vereinen und anderen ehrenamtlich Engagierten stellen wir immer wieder fest, wie viele Fragen es rund um die personenbezogenen Daten von Kindern und Jugendlichen gibt. Die einen fragen sich, ob sie Kinder beim Vereinsfest fotografieren dürfen. Die nächsten möchten wissen, wie sie sensible gesundheitliche Daten schützen können, die für eine Ferienfreizeit erfasst werden müssen. Wieder andere wollen Sicherheit darüber, ob sie mit Jugendlichen über Messenger-Dienste kommunizieren dürfen. Bei all diesen Beispielen stellt sich die Frage, inwieweit Kinder und Jugendliche selbst entscheiden dürfen und ob ihre Eltern mit einbezogen werden müssen. Dies wird in den bestehenden gesetzlichen Regelungen und in der Rechtsprechung nicht ausreichend klar adressiert.

Deshalb haben wir ein Gutachten zum Schutz personenbezogener Daten Minderjähriger in Auftrag gegeben. Autorin Dr. Diana Ettig analysiert die bestehende Rechtslage und gibt unter Berücksichtigung der Rechtsprechung und der Veröffentlichungen von Aufsichtsbehörden belastbare Handlungsempfehlungen für die Praxis. Der Schwerpunkt des Gutachtens liegt auf der Verarbeitung personenbezogener Daten im ehrenamtlichen Engagement und in Vereinen.

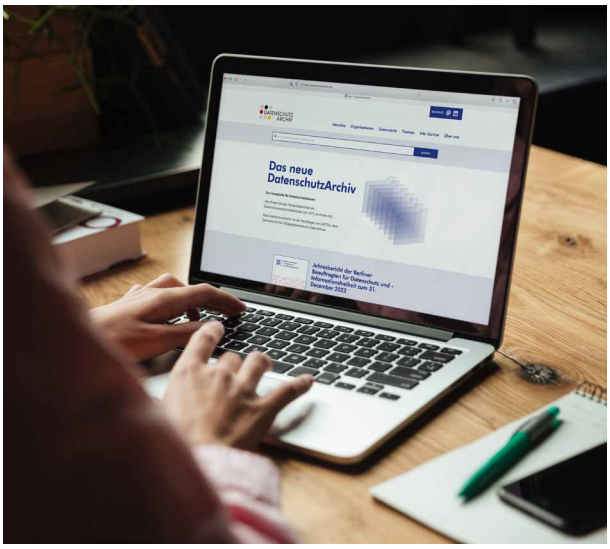
Wir hoffen, dass das Gutachten ein hilfreiches Werkzeug im Vereinskontext darstellt und freuen uns darüber, dass es bereits auf positive Resonanz gestoßen ist.

„Ich bin gerade sehr begeistert von der Ausarbeitung von Dr. Diana #Ettig für die @DS_Stiftung“

„Denn das Team der Stiftung Datenschutz hat ein Gutachten von Diana Ettig kostenlos veröffentlicht, das bei all den vorgenannten Fragen wirklich sehr gute, brauchbare und aktuelle Antworten liefert.“

Mehr Infos zum Gutachten:

→ https://stiftungdatenschutz.org/praxisthemen/schutzbeduerfnis-kinder-jugendliche



Neuigkeiten aus dem DatenschutzArchiv

Mit dem Re-Launch 2024 wurde das DatenschutzArchiv ausgebaut: Als Sammlung von Tätigkeitsberichten gestartet, ist jetzt eine breitere, thematisch strukturierte Wissensplattform daraus geworden. Diese Struktur schafft eigenständige Rubriken, die unterschiedliche Dokumenttypen der Aufsichtsbehörden gezielt adressieren. Insbesondere klar abgegrenzte Bereiche wie Leitlinien, Stellungnahmen und die ergänzenden Themen-Stichworte vereinfachen die Suche nach relevanten Texten.

Das DatenschutzArchiv ist im Jahr 2025 weitergewachsen. Die Dokumente der Datenschutzkonferenz und des Europäischen Datenschutzausschusses sind hinzugekommen. Ebenfalls neu ist der Gesetzestext der DSGVO einschließlich der Erwägungsgründe – erstmals ohne Tracking auf einer gemeinnützigen Webseite.

Zum DatenschutzArchiv:

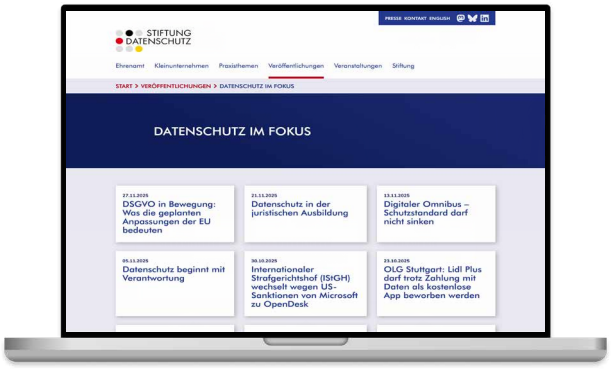
→ https://datenschutzarchiv.org/start

Die Rubrik „Leitlinien“ bündelt nun praxisbezogene Hinweise wie Guidelines, Working Paper, Anwendungshinweise, Orientierungshilfen und Factsheets der europäischen und nationalen Aufsichten an einem Ort. Für Praktikerinnen und Praktiker bedeutet das: Statt die einschlägigen Auslegungshilfen mühsam auf diversen Behörden-Websites zu suchen, lassen sie sich in einer zentralen Kategorie systematisch auffinden und vergleichen – ein deutlicher Zeit- und Effizienzgewinn im Arbeitsalltag.

Unter „Stellungnahmen“ fasst das Archiv Bewertungen, Positionspapiere, Entschließungen, Beschlüsse und „Opinions“ zusammen. Diese Rubrik macht die normative „Soft Law“-Schicht des Datenschutzrechts transparenter: Wer etwa die Linie der Aufsichtsbehörden zu neuen Technologien, zur KI-Regulierung oder zu branchenspezifischen Fragen nachzeichnen will, erhält hier eine konsolidierte Sicht, die sich direkt in Argumentationslinien für Gutachten, Stellungnahmen oder Schriftsätze übersetzen lässt.

Im Bereich „Themen“ sind zu bestimmten Themenbereichen die in den Tätigkeitsberichten verstreuten Texte auffindbar. Für die Anwendungspraxis ist das ein hilfreicher Schritt hin zu einer Wissensdatenbank: Ähnliche Sachverhalte (etwa Gesundheitsdaten, Beschäftigtendatenschutz, Scoring, KI) lassen sich dadurch über Behördengrenzen hinweg systematisch vergleichen, was insbesondere kleineren Organisationen ohne eigene Datenschutzabteilung einen niedrigschwelligen Zugang zu konsistenter Rechtsanwendung eröffnet. Die Suche verbessern wir kontinuierlich.

Für die Datenschutzpraxis und -rechtsanwendung wird das DatenschutzArchiv so immer mehr zu einer Fundstelle, die nicht nur Rechtstexte, sondern auch die gelebte Aufsichtspraxis sichtbar macht.



Datenschutz im Fokus

In diesem Jahr haben wir auf unserer Website eine Rubrik eingeführt, die für uns längst überfällig war: ***Datenschutz im Fokus***. Dort bündeln wir Beiträge, in denen wir über aktuelle Themen und Dauerbrenner informieren. Unsere Wissenschaftliche Leiterin, Kirsten Bock, und unser Vorstand, Frederick Richter, ordnen die Themen ein.

Warum machen wir das nicht ausschließlich über Social Media? Nicht alle Menschen möchten Social Media nutzen. Uns ist wichtig, dass unsere Einordnungen unabhängig von Timelines, Algorithmen und Plattformzugängen zugänglich bleiben.

Zum Datenschutz im Fokus:

→ https://stiftungdatenschutz.org/veroeffentlichungen/datenschutz-im-fokus

Seit dem Start der Rubrik zeigt sich, wie vielfältig das Feld ist, zu dem wir Orientierung bieten wollen. Wir greifen dabei gesetzliche Entwicklungen wie DSGVO-Anpassungen oder EU-Initiativen zu digitalen Grundrechten auf, beleuchten zentrale Gerichtsentscheidungen zu Themen wie pseudonymisierten Daten oder dem EU-US-Datentransfer und beobachten technische sowie gesellschaftliche Trends – von automatisierten Entscheidungen bis zu neuen Überwachungsformen.

Ihre Ansprechpersonen

Frederick Richter, LL.M.
Vorstand

richter@stiftungdatenschutz.org

Theresa Wenzel
Referentin Stiftungskommunikation

t.wenzel@stiftungdatenschutz.org

Unser Archiv aller Stiftungsbriefe finden Sie hier

stiftungsbrief.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 und Mitarbeit
Theresa Wenzel

Redaktionsschluss
11. Dezember 2025

Agenturpartner
KING CONSULT | Kommunikation, Berlin
www.king-consult.de

Die Arbeit der Stiftung Datenschutz wird aus dem Bundeshaushalt gefördert (Einzelplan des BMJV).

Bildnachweis
Foto bei „Palantir: Big Data for Big Brother“ © BrianAJackson iStock

Bundesministerium der Justiz und für Verbraucherschutz