

# *Mehr Rechtssicherheit durch Verbots- und Erlaubnistarbestände*

Louisa Specht-Riemenschneider, Niko Härtling & Linda Bienemann

Arbeitsgruppe DSGVO am TUM Think Tank

## 1. Kontext

Die DSGVO arbeitet mit unbestimmten Rechtsbegriffen und Abwägungsklauseln in zentralen Erlaubnistarbeständen. Dies führt dazu, dass in der Praxis verstärkt auf das Instrument der Einwilligung gesetzt wird. Damit obliegt es in erster Linie den Betroffenen selbst, sich gegen Risiken bei der Verarbeitung von personenbezogenen Daten zu schützen.

Die „informierte Einwilligung“ ist allerdings vielfach nicht mehr als eine Fiktion. Aufgrund von Entscheidungsermüdung und Informationsüberlastung können und wollen Betroffene häufig keine informierten Entscheidungen treffen (s. Reformvorschlag der Arbeitsgruppe „Der Consent-Fatigue entgegenwirken“). Die Legitimationswirkung der Einwilligung ist daher beschränkt. In besonders grundrechtssensiblen Bereichen sollte der Gesetzgeber daher entscheiden, welche Datenverarbeitungen erlaubt und welche verboten sind („grüne“ und „rote“ Bereiche). Außerhalb dieser beiden Bereiche – in einem „gelben“ Bereich – kann es dabei bleiben, dass auch die Einwilligung Datenverarbeitungen legitimieren kann, wenn gesetzgeberisch die Voraussetzungen für tatsächlich selbstbestimmte Entscheidungen getroffen werden.

Um „grüne“, „rote“ und „gelbe“ Bereiche abzutrennen (Ampelkonzept), bieten sich – kumulativ – folgende Maßnahmen an:

- Formulierung expliziter Erlaubnisfälle innerhalb und außerhalb der DSGVO – gesetzgeberisch klare Entscheidungen für gesellschaftlich erwünschte Datenverarbeitungen;
- eine Konkretisierung der berechtigten Interessen nach Artikel 6 Abs. 1 Buchstabe f DSGVO;
- ein Blacklisting gesellschaftlich inakzeptabler Datenverarbeitungen entsprechend § 3 UWG;
- ein „gelber“ Bereich, bei dem es neben den weiteren Rechtfertigungstatbeständen auch bei der einwilligungsbasierten Verarbeitung von personenbezogenen Daten bleibt. Hier muss der Gesetzgeber aber die Voraussetzungen für tatsächliche Selbstbestimmung schaffen.

Die neu vorgeschlagene Gesetzesystematik des Ampelkonzepts eröffnet darüber hinaus die Möglichkeit, das bislang in Wissenschaft und Praxis vernachlässigte Verhältnis zwischen Art. 9 und Art. 6 DSGVO aufzulösen. Zwar ist Art. 9 DSGVO de lege lata als lex specialis gegenüber Art. 6 DSGVO konzipiert, entfaltet jedoch keine tatsächliche Verdrängungswirkung. Ganz im Gegenteil muss bei einem Rechtfertigungsgrund nach Art. 9 DSGVO stets auch ein Rechtfertigungsgrund nach Art. 6 DSGVO einschlägig sein (EuGH Rs. C 667/21). Dasselbe gilt für eine Sekundärnutzung nach Art. 6 Abs. 4 DSGVO. Art. 9 DSGVO enthält aber z.T. Rechtfertigungsgründe, die hinter den Voraussetzungen des Art. 6 DSGVO zurückbleiben

(z.B. Art. 9 Abs. 2 lit. e DSGVO), sodass de lege lata gerade kein ausreichender Schutz sensibler Daten besteht.

Gleichzeitig führt die Aufspaltung in zwei verschiedene Erlaubnistatbestände gerade für Mischdatensätze und Zweifelsfälle (z.B. mit mittelbar gesundheitsrelevanten Daten wie Ernährungsgewohnheiten, die auf einen pathologischen Zustand hinweisen können) zu großer Rechtsunsicherheit und Praktikabilitätsproblemen. Die Normenkonzeption des Art. 9 DSGVO zeigt weder Vollständigkeit noch bildet die Norm die individuellen und systemischen Risiken ab, die mit der jeweiligen Datenverarbeitung einhergehen.

Es sollten daher Verbots- und Erlaubnistatbestände geschaffen werden, die auch tatsächlich und nicht nur auf dem Papier ein hohes Schutzniveau für Betroffene gewährleisten und gleichzeitig mehr Rechtssicherheit in die Praxis tragen. Differenziert werden muss dabei zwar weiterhin zwischen besonderen Kategorien und anderen personenbezogenen Daten, es kann allerdings für kein Datum pauschal festgestellt werden, ob es sich um ein solch sensibles Datum handelt oder nicht, da Daten kontextabhängig zu sensiblen Daten werden können. Die individuellen und systemischen Risiken einer Datenverarbeitung müssen daher bereits bei der Formulierung von Erlaubnistatbeständen und bei der Abwägungsentscheidung sehr viel stärker berücksichtigt werden.

## 2. Reformvorschlag

Vor diesem Hintergrund hat die Arbeitsgruppe den folgenden Vorschlag zu einer gesetzlichen Neufassung von Artikel 6 und 9 DSGVO entwickelt.

### **Rechtmäßigkeit der Verarbeitung**

- (1) Die Verarbeitung ist rechtswidrig, wenn sie unter **Anhang 1** dieser Verordnung fällt.
- (2) Die Verarbeitung ist rechtmäßig, wenn sie unter **Anhang 2** dieser Verordnung fällt oder mindestens eine der nachstehenden Bedingungen erfüllt ist:
  - a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
  - b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
  - c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
  - d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
  - e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
  - f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern das berechtigte Interesse des Verantwortlichen oder eines Dritten die

Grundrechte und Grundfreiheiten der betroffenen Personen überwiegt, wobei den Grundrechten und Grundfreiheiten von Kindern ein besonderes Gewicht zukommt. Im Falle sensibler Daten [tbd: Definition in Art. 4 DSGVO einzufügen], ist ein erhebliches Überwiegen des Verarbeitungsinteresses erforderlich.

- g) Die Verarbeitung wird zur Wahrung eines anerkannten berechtigten Interesses i.S.v. **Anhang 3** vorgenommen und der Verarbeitung stehen keine besonderen Einzelfallumstände entgegen.
- (3) Absatz 2 Unterabsatz 1 Buchstabe f und g gelten nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(4) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 2 Buchstabe c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(5) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 2 Buchstaben c und e wird festgelegt durch

- a) Unionsrecht oder  
b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 2 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung

enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(6) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

- a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,  
b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

- c) ob durch die Umstände der Verarbeitung oder den Verarbeitungskontext, den Informationsinhalt des Datums oder den Empfänger der Daten erhebliche Risiken für die Grundrechte und Grundfreiheiten der betroffenen Person oder unserer Gesellschaft herbeigeführt werden,
- d) die möglichen Folgen sowie konkreten Auswirkungen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- e) das Vorhandensein geeigneter Schutzmaßnahmen, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

(7) Ist die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar, so ist die Weiterverarbeitung zu diesem anderen Zweck zulässig.

Evaluierung einer Anonymisierungsmaßnahme, oder

- die De-Anonymisierung ist notwendig, um lebenswichtige Interessen des Betroffenen oder einer anderen natürlichen Person zu schützen, oder
- die De-Anonymisierung wird durch das Unionsrecht oder das Recht eines Mitgliedsstaats erlaubt, sofern zugleich angemessene Maßnahmen zum Schutz der Rechte und Freiheiten des Betroffenen vorgesehen sind;

d. die Verarbeitung von Daten, zu denen sich der Verantwortliche unter Umgehung von technischen und organisatorischen Maßnahmen Zugang verschafft hat;

e. die Verarbeitung von Daten, die sich der Verantwortliche verschafft hat durch irreführende, aggressive oder andere unlautere Praktiken, insbesondere durch eine Gestaltung und Organisation von Online-Schnittstellen, die nach Artikel 25 der Verordnung (EU) 2022/2065 rechtswidrig ist;

f. die Verarbeitung personenbezogener Daten durch einen Verantwortlichen auf der Grundlage einer vermeintlichen Einwilligung der betroffenen Person, obwohl der Verantwortliche weiß oder vernünftigerweise wissen kann, dass die betroffene Person oder ein Dritter infolge dieser Verarbeitung erheblichen Schaden erleiden wird, und der Verantwortliche nicht vernünftigerweise annehmen kann, dass die betroffene Person ihre Einwilligung erteilt hätte, wenn sie dieses Risiko vorhergesehen hätte;

g. die Übermittlung personenbezogener Daten an einen Dritten oder die Förderung bzw. wesentliche Erleichterung der Verarbeitung personenbezogener Daten durch einen Dritten, obwohl der Verantwortliche oder Auftragsverarbeiter weiß

## Anhang 1: Verbotsfälle

(1) Soweit keine gesetzliche Verpflichtung zur Datenverarbeitung für den Verantwortlichen oder Auftragsverarbeiter besteht, ist eine Verarbeitung personenbezogener Daten zu folgenden Zwecken stets rechtswidrig:

- a. Profiling bei Kindern und Jugendlichen unter 18 Jahren zum Zwecke der Verhaltensbeobachtung oder der direkten Werbeansprache;
- b. eine Verarbeitung zum Zwecke einer nach den Richtlinien 2000/43/EG, 2000/78/EG, 2004/113/EG und 2006/54/EG unzulässigen Diskriminierung;
- c. die Verarbeitung zum Zwecke der De-Anonymisierung, es sei denn
  - eine vorherige Anonymisierung wurde als lediglich vorübergehende Maßnahme durch den Verantwortlichen vorgenommen, oder
  - eine De-Anonymisierung erfolgt allein zur Entwicklung, Verbesserung oder

oder vernünftigerweise wissen kann, dass der Dritte durch diese Verarbeitung seine Pflichten gegenüber der betroffenen Person in erheblichem Maße verletzen und dadurch voraussichtlich erheblichen Schaden verursachen wird.

(2) Dem Hersteller eines datenverarbeitenden Systems ist es untersagt, einem Verantwortlichen oder Auftragsverarbeiter ein datenverarbeitendes System anzubieten oder bereitzustellen, wenn er in Kenntnis des Umstandes handelt, dass der Verantwortliche oder Auftragsverarbeiter bei der Nutzung des datenverarbeitenden Systems datenschutzrechtliche Pflichten gegenüber der betroffenen Person verletzen wird oder verletzen will.

(3) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 92 zu erlassen, um die in Anhang 1 Abs. 1 stets rechtswidrige Verarbeitung personenbezogener Daten im Einvernehmen mit dem Europäischen Datenschutzausschuss zu ändern, weitere stets rechtswidrige Verarbeitungen hinzuzufügen oder einzelne Verarbeitungen zu streichen. Für die Ausübung der Befugnisübertragung gilt Art. 92 Abs. 6 DSGVO.

## Anhang 2: Erlaubnisfälle

1) Vorbehaltlich geeigneter Schutzmaßnahmen für die Grundrechte und die Interessen der betroffenen Person ist die Verarbeitung personenbezogener Daten zu folgenden Zwecken stets zulässig:

- a. die Verarbeitung und die Weiterverarbeitung bereits erhobener personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken;
- b. die Verarbeitung und die Weiterverarbeitung bereits erhobener personenbezogener Daten zu statistischen Zwecken;
- c. die Verarbeitung und die Weiterverarbeitung bereits erhobener personenbezogener Daten zu historischen Forschungszwecken;
- d. die Verarbeitung und die Weiterverarbeit-

ung bereits erhobener personenbezogener Daten zu im öffentlichen Interesse liegenden anderen wissenschaftlichen Forschungszwecken;

- e. die Verarbeitung erfolgt, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit oder des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren Pflichten nach dem Unionsrecht oder dem Recht der Mitgliedstaaten nachkommen kann;
- f. die Verarbeitung erfolgt zum Schutz einer natürlichen Person vor erheblicher Vernachlässigung oder vor erheblicher körperlicher, geistiger oder seelischer Schädigung oder zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben;
- g. die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden;
- h. die Verarbeitung erfolgt zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit;
- i. die Verarbeitung erfolgt auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem

Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses;

j. die Verarbeitung erfolgt für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs;

k. die Verarbeitung erfolgt aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht;

l. die Verarbeitung erfolgt für die Zwecke des Trainings, des Testens oder des Finetuning von KI-Modellen oder KI-Systemen, die den Anforderungen der Verordnung (EU) 2024/1689 genügen, wenn

1. das Trainieren, das Testen oder das Finetuning nicht in der Verantwortlichkeit eines Gatekeeper nach der Verordnung (EU) 2022/1925 vorgenommen wird

2. das Trainieren, das Testen oder das Finetuning mit bereits erhobenen Daten im Bestand desjenigen, in dessen Verantwortung das Training, Testen oder

Finetuning erfolgt und

3. das KI-Modell oder das KI-System einem gemeinwohlorientierten Zweck dient.

(2) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 92 zu erlassen, um die in Anhang 2 Abs. 1 stets zulässige Verarbeitung personenbezogener Daten im Einvernehmen mit dem Europäischen Datenschutzausschuss zu ändern, weitere zulässige Verarbeitungen hinzuzufügen oder einzelne Verarbeitungen zu streichen. Der Kommission wird die Befugnis übertragen, den Begriff des öffentlichen Interesses und der Gemeinwohlorientierung zu bestimmen und Datenverarbeitungen festzulegen, die unter diese Begriffsbestimmung fallen. Für die Ausübung der Befugnisübertragung gilt Art. 92 Abs. 6 DSGVO.

### **Anhang 3: Anerkannte Berechtigte Interessen**

(1) Ein anerkanntes berechtigtes Interesse liegt vor, wenn personenbezogene Daten zu einem der folgenden Zwecke verarbeitet werden und der Verarbeitung nicht ausnahmsweise Einzelfallumstände entgegenstehen:

a. die Verarbeitung erfolgt als Reaktion auf eine Katastrophe im Sinne des Artikels 4 Nummer 1 der Verordnung 1313/2013;

b. die Verarbeitung erfolgt zur Betrugsbekämpfung oder als Maßnahme der Sicherheit der Verarbeitung nach Artikel 32 dieser Verordnung oder zur Sicherstellung des ordnungsgemäßen Funktionierens von Geräten, IT-Systemen oder Infrastruktur;

c. die Verarbeitung erfolgt zur Gewährleistung der Netz- und Informationssicherheit (z.B. Verhinderung unbefugten Zugriffs oder von Cyberangriffen) sowie der Verhinderung der missbräuchlichen Nutzung von Diensten oder Systemen (z.B. Erkennung von Bots der Spam);

- d. die Verarbeitung erfolgt zur Meldung rechtswidriger Aktivitäten oder Gefahren für die öffentliche Sicherheit an Behörden;
- e. die Verarbeitung erfolgt zur Gewährleistung von Arbeitssicherheit und Arbeitsschutz;
- f. die Verarbeitung erfolgt ausschließlich zur Durchführung von Prozessen der Personalgewinnung oder der nachhaltigen Qualitäts sicherung;
- g. die Verarbeitung erfolgt, um personenbezogene Daten innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln;
- h. die Verarbeitung erfolgt zur Durchführung von Audits oder Compliance-Prüfungen;
- i. die Verarbeitung erfolgt innerhalb einer Organisation, die keine gewerblichen Zwecke verfolgt, zu Zwecken der Dokumentation der Tätigkeit der Organisation oder der Tätigkeit der Mitglieder oder zu Zwecken der Willensbildung innerhalb der Organisation oder zur Kommunikation der Mitglieder innerhalb der Organisation oder mit Dritten;
- j. die Verarbeitung erfolgt innerhalb von Bildungseinrichtungen oder zwischen Angehörigen der Bildungseinrichtungen oder deren Erziehungsberechtigten zu Zwecken der Gewährleistung der Funktionsfähigkeit des Unterrichts oder zu Zwecken der Kommunikation zwischen Angehörigen der Bildungseinrichtungen oder deren Erziehungsberechtigten.

(2) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 92 zu erlassen, um die nach Anhang 3 einem anerkannten berechtigten Interesse unterliegende Verarbeitung personenbezogener Daten im Einvernehmen mit dem Europäischen Datenschutzausschuss zu ändern, weitere zulässige Verarbeitungen hinzuzufügen oder einzelne Verarbeitungen zu streichen. Für die Ausübung der Befugnisübertragung gilt Art. 92 Abs. 6 DSGVO.

## 3. Einordnung

Nachfolgend findet sich eine zusammenfassende Übersicht der Vor- und Nachteile des Vorschlags zur weiterführenden Diskussion.

### Vorteile

- Der Anwendungsbereich der Einwilligung bedarf einer Einengung. Statt es überwiegend dem Betroffenen selbst zu überlassen, ob und wie er – durch eine Einwilligung – seine Personendaten stützt, bedarf es klarer roter Linien.
- Die vorgeschlagenen Verbots- und Erlaubnislisten führen zu einer Verengung des Anwendungsbereichs der Einwilligung. Hierdurch wird der Weg geebnet für eine wahrhaftig „informierte Einwilligung“ von Betroffenen.
- Die Verbote markieren klare rote Linien, die auch durch eine Einwilligung nicht durchbrochen werden können. Gleichzeitig ermöglicht die Positivliste eine effektivere und rechtssichere Datennutzung.

### Nachteile

- Dies erfordert eine grundlegende systematische Reform der DSGVO durch klare Verbotslinien und Erlaubniszonen für personenbezogene Daten.
- Der Klarstellungscharakters des Anhang 3 (Liste der anerkannten berechtigten Interessen) könnte als redundant oder verwirrend empfunden werden.



## ARBEITSGRUPPE DSGVO

Die Arbeitsgruppe DSGVO am TUM Think Tank bringt Expertinnen und Experten aus Wissenschaft, Praxis, Aufsicht und Zivilgesellschaft zur Weiterentwicklung der DSGVO zusammen. Dies ist einer von vier konkreten, rechtlich anschlussfähigen Reformbausteinen, die sowohl Datenschutz wirksamer machen als auch verantwortliche Datennutzung für Wirtschaft und Gesellschaft erleichtern.

Der TUM Think Tank bietet die organisatorische Plattform. Initiiert wurde die Arbeitsgruppe von Kai Zenner, Max Schrems, Boris Paal und Markus Siewert.

## INSTITUTION

TUM Think Tank | Hochschule für Politik München | Technische Universität München

## DISCLAIMER

Der vorliegende Reformvorschlag (Version 1.0) wird von einer Mehrheit der Arbeitsgruppe mitgetragen, auch wenn nicht alle Mitglieder allen Teilen gleichermaßen zustimmen und durchaus auch abweichende Meinungen existieren.

Die Vorschläge verstehen sich nicht als Endpunkt, sondern als Ausgangspunkt für weiterführende Diskussionen. In den kommenden Wochen und Monaten wird die Arbeitsgruppe diese Vorschläge – insbesondere vor dem Hintergrund der derzeit teilweise kontrovers geführten Debatten zum Digital Omnibus – weiterentwickeln und zusätzliche Reformbausteine ausarbeiten.

Die in diesem Bericht geäußerten Inhalte und Ansichten geben ausschließlich die Meinung der Autoren wieder und sind nicht dem TUM Think Tank als Institution oder seinen Mitgliedern zuzuschreiben.

## KONTAKT

tumthinktank@hfp.tum.de  
<https://tumthinktank.de>

## Mitglieder der Arbeitsgruppe DSGVO

**Christoph Bausewein** | Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

**Linda Bienemann** | Persönliche Referentin Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

**Franziska Boehm** | FIZ-Karlsruhe & Karlsruher Institut für Technologie (KIT)

**Stefan Brink** | Wissenschaftliches Institut für die Digitalisierung der Arbeitswelt (WIDA) / Berlin

**Thomas Fuchs** | Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit (HmbBfDI)

**Niko Härtig** | HÄRTING & Deutscher Anwaltverein

**Peter Hense** | Spirit Legal Rechtsanwaltsgesellschaft mbH

**Boris Paal** | Technische Universität München

**Frederick Richter** | Stiftung Datenschutz

**Max Schrems** | noyb

**Louisa Specht-Riemenschneider** | Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

**Christiane Wendehorst** | Universität Wien

**Michael Will** | Bayerisches Landesamt für Datenschutz (BayLDA)

**Kai Zenner** | MEP Axel Voss, Europäisches Parlament & TUM Think Tank