Die Verarbeitung personenbezogener Daten zum Training von KI-Systemen aufgrund „berechtigter Interessen" gemäß Art. 6 Abs. 1 lit. f DSGVO: im Zweifel für die informationelle Selbstbestimmung

Konstantinos Tsakiliotis[*]

A. Einführung

In jeder Phase eines KI-Projekts – vom Sammeln und Bewerten relevanter (Trainings-)Daten über das Training algorithmischer Modelle bis hin zu deren Überprüfung – finden unterschiedliche Verarbeitungen personenbezogener Daten statt, unter anderem werden mittels Scraping online bzw. öffentlich verfügbare personenbezogene Daten aus verschiedenen Quellen gesammelt und für das KI-Training benutzt. Personenbezogene Daten sind dabei von grundlegender Bedeutung, da sie als unverzichtbarer „Treibstoff" für die Leistungsfähigkeit und Effektivität dieser Systeme dienen.[1] Art. 6 Abs. 1 lit. f DSGVO stellt die Rechtsgrundlage dar, worauf Verantwortliche Datenverarbeitungen im Kontext des KI-Trainings am häufigsten stützen. Als Grund wird unter anderem angeführt, dass ansonsten die Transaktionskosten für das Einholen der Einwilligung jeder in den Trainingsdaten vertretenen betroffenen Person oft zu hoch wären. Gemäß Art. 6 Abs. 1 lit. f DS-GVO ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Dieser Beitrag analysiert den Abwägungsvorgang des Art. 6 Abs. 1 lit. f DS-GVO unter Einbeziehung der Stellungnahmen des EDSA sowie der einschlägigen Rechtsprechung des EuGH. Die Konzeption des Abwägungsvorgangs wird aus rechtspolitischer Perspektive kritisch hinterfragt. Der

* M.A. Science & Technology Studies (TU München), Rechtsanwalt und Doktorand an der TU Dresden. Sämtliche Internetverweise wurden zuletzt abgerufen am 25.7.2025. Der Verfasser dankt Tristan Radtke für die kritische Durchsicht des Manuskripts und die wertvollen Anmerkungen.

1 *Kramcsák* Computer Law & Security Review 48 (2023), Article 105765 (2 f.) <https://doi.org/10.1016/j.clsr.2022.105765>.

Beitrag warnt davor, den politisch umstrittenen Begriff der „Innovation" als Panazee im Rahmen der Auslegung des Art. 6 Abs. 1 lit. f DSGVO heranzuziehen, und plädiert stattdessen im Interesse der informationellen Selbstbestimmung dafür, die Einwilligung der Betroffenen einzuholen, wenn dies ohne unverhältnismäßigen Aufwand möglich ist. Abschließend wird ein Ausblick de lege ferenda unter anderem auf regulatorische Instrumente gegeben, mit denen eine demokratische Gesellschaft die Richtung datengetriebener Innovation mitgestalten kann.

B. Entstehungsgeschichte des Art. 6 Abs. 1 lit. f DSGVO

Der datenschutzrechtliche Erlaubnistatbestand „berechtigte Interessen" reicht von der Datenschutz-RL 95/46/EG bis zur DSGVO und behält über all diese Jahre hinweg das Kernprinzip einer Abwägung zwischen den Interessen des Verantwortlichen und den Interessen der betroffenen Person bei.[2] In Ermangelung der bezweckten Harmonisierung bezüglich Art. 7 lit. f RL 95/46/EG unter den Mitgliedstaaten aufgrund des abstrakten Wortlauts der Norm (mangels relevanter Erläuterung hinsichtlich des Abwägungsvorgangs etwa in den Erläuterungsgründen) erkannte die Kommission einen entsprechenden Reformbedarf.[3] Im Zuge der Arbeiten an der DSGVO schlug die Europäische Kommission im Jahr 2012 zunächst vor, die berechtigten Interessen Dritter ganz aus dem Anwendungsbereich zu entfernen und sich auf das berechtigte Interesse des Verantwortlichen zu beschränken.[4] Außerdem sollten delegierte Rechtsakte der Kommission die Rahmenbedingungen für das berechtigte Interesse weiter spezifizieren, etwa in Bezug auf unterschiedliche Branchen oder hinsichtlich der Verarbeitung von Daten von Kindern.[5] Dieser Ansatz stieß auf Kritik, da man grundlegende Fragen zur Auslegung nicht einem Exekutivorgan mit begrenztem Auftrag überlassen wollte, stattdessen sollte die Arbeit der Datenschutzgruppe WP29 bei der Erläuterung des europäischen Datenschutz-

2 Vgl. Art. 7 lit. f RL 95/46/EG; *Kamara/De Hert*, Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach, in: Selinger/Polonetsky/Tene, The Cambridge Handbook of Consumer Privacy, 2018, S. 321 (326 f.).

3 KOM(2003) 265 endgültig.

4 *Kamara/De Hert*, in: The Cambridge Handbook of Consumer Privacy, S. 321 (326 ff.).

5 *Kamara/De Hert*, in: The Cambridge Handbook of Consumer Privacy, S. 321 (326 ff.).

rechts vom Europäischen Datenschutzausschuss fortgeführt werden.[6] Im sogenannten Albrecht-Bericht[7] wurde zudem eine Positivliste vorgeschlagen, die bestimmte Anwendungsfälle des berechtigten Interesses explizit erfassen sollte, zum Beispiel die Datenverarbeitung im Kontext von Medien und Kunst. Allerdings lehnte man eine solche feste Aufzählung überwiegend ab, weil sie als zu eng und nicht zukunftsfähig galt.[8]

Bereits 2014 merkte die Artikel-29-Datenschutzgruppe (WP29) – die Vorgängerin des kraft Art. 68 Abs. 1 DSGVO am 25. Mai 2018 eingerichteten Europäischen Datenschutzausschusses – in ihrer Stellungnahme 06/2014 an, dass Art. 7 lit. f RL 95/46/EG nicht als „letztes Mittel" für seltene oder unerwartete Situationen verstanden werden sollte, in denen andere Rechtsgrundlagen nicht greifen.[9] Ebenso wies sie darauf hin, dass Art. 7 lit. f RL 95/46/EG nicht automatisch gewählt oder sein Anwendungsbereich fälschlicherweise erweitert werden darf, nur weil es vermeintlich weniger einschränkend ist als andere Rechtsgrundlagen.[10] Weiterhin betonte die Arbeitsgruppe, dass eine korrekte Prüfung gemäß Art. 7 lit. f RL 95/46/EG keine bloße Gegenüberstellung zweier leicht messbarer „Gewichte" darstellt, sondern eine unter Umständen skalierbare und je nach Komplexität variierende umfassende Berücksichtigung verschiedener Faktoren erfordert, die allerdings nicht übermäßig belastend sein müsste („unduly burdensome").[11] Die Datenschutzgruppe beklagte, dass obwohl die Vorgängernorm des Art. 6 Abs. 1 lit. f DSGVO eine fundierte Interessenabwägung vorschrieb, „betrachten manche ihn fälschlicherweise als ‚offene Tür' für jede Datenverarbeitung, die sich nicht auf andere Rechtsgrundlagen stützen lässt".[12]

6 *Kuner*, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy & Security Law Report 11 (2012), PVLR 06.

7 PE-CONS 76/24 <https://data.consilium.europa.eu/doc/document/PE-76-2024-INIT/en/pdf>.

8 *Kamara/De Hert*, in: The Cambridge Handbook of Consumer Privacy, S. 321 (326 ff.).

9 *Kamara/De Hert*, in: The Cambridge Handbook of Consumer Privacy, S. 321 (326 ff.).

10 Article 29 Working Party, Opinion 06/2014, S. 4.

11 Article 29 Working Party, Opinion 06/2014, S. 4.

12 Article 29 Working Party, Opinion 06/2014, S. 5.

C. Art. 6 Abs. 1 lit. f DSGVO de lege lata

De lege lata ist gemäß Art. 6 Abs. 1 lit. f DS-GVO eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Dafür müssen die drei folgenden kumulativen Voraussetzungen erfüllt sein: (i) dass von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen wird; (ii) dass die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich ist; und (iii) dass die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen.[13]

I. „Berechtigte Interessen" des Verantwortlichen oder eines Dritten

Auf der ersten Stufe muss der KI-Entwickler ein berechtigtes Interesse nachweisen, das klar und präzise formuliert, real und gegenwärtig[14] – also nicht spekulativ – ist.[15] Das berechtigte Interesse des KI-Entwicklers an der Datenverarbeitung zum Zwecke des KI-Trainings kann tatsächlicher, wirtschaftlicher oder ideeller Art sein.[16] Der EuGH verlangt, dass ein „berechtigtes Interesse" nur dann vorliegt, wenn es selbst rechtmäßig ist;[17] der EDSA weist im Sinne der Einheit der acquis communautaire darauf hin, dass die Verantwortlichen bei der Prüfung alle einschlägigen Normen, unter anderem das Verbot zielgruppenspezifischer Werbung an Minderjährige gemäß Art. 26 Abs. 3, Art. 28 DSA und die Verbote manipulativer Praktiken gemäß Art. 5 Abs. 1–2 KI-VO, in die Beurteilung einbeziehen müssen.[18] Berechtigt ist jedenfalls das Interesse des KI-Entwicklers, das in den Schutzbereich eines Grundrechts nach der GRCh fällt, wie zB die Forschungsfreiheit unter Art. 14 GRCh, sowie die unternehmerische Freiheit gemäß Art. 16 GRCh oder der Grundsatz der kulturellen und sprachlichen Vielfalt gemäß

13 EDSA, Stellungnahme 28/2024, Rn. 68 mit den dortigen Hinweisen auf die Rspr. des EuGH.
14 EuGH BeckRS 2019, 31011 (Rn. 44).
15 EDSA, Stellungnahme 28/2024, Rn. 68.
16 *Paal* ZfDR 2024, 129 (149 ff.).
17 EuGH NJW 2024, 3769 (Rn. 49).
18 EDSA, Stellungnahme 28/2024, Rn. 68, siehe dazu Fn. 54 in der Stellungnahme.

Art. 22 GRCh.[19] Mangels einer abschließenden Definition dieses Begriffs – oder eines Beispielkatalogs – in der DSGVO kann grundsätzlich eine breite Vielfalt von Interessen als berechtigt angesehen werden.[20] Nach Ansicht des EDSA können – vorbehaltlich der beiden weiteren Prüfungsschritte – im Kontext von KI-Modellen unter anderem folgende Interessen als „berechtigt" gelten: die Entwicklung eines Konversationsagenten, der Nutzer unterstützt, der Aufbau eines KI-Systems zur Aufdeckung betrügerischer Inhalte oder Verhaltensweisen und die Verbesserung der Bedrohungserkennung in einem Informationssystem.[21]

II. Erforderlichkeit

Die Erforderlichkeit der Datenverarbeitung wird bejaht, wenn das angestrebte Ziel nicht mit weniger einschneidenden Mitteln erreicht werden kann.[22] Dies sollte sich unter anderem danach richten, ob der Verantwortliche in direkter Beziehung zu den betroffenen Personen steht und die Daten selbst erhoben hat oder ob die Daten online verfügbar waren und bspw. von Dritten erhoben wurden.[23] Zwar stehen die in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen gleichrangig nebeneinander,[24] doch gilt die informierte Einwilligung gemäß Art. 6 Abs. 1 lit. a iVm Art. 7 DSGVO im Einklang mit der Rechtsprechung des EuGH[25] auf der Erforderlichkeitsebene als weniger einschneidendes jedoch gleich effektives Mittel, soweit bereits ein Kontakt zum Betroffenen besteht. Soweit der Verantwortliche selbst die Daten erhoben hat und in direkter (Vertrags)beziehung zum Datensubjekt steht und die Datensubjekte in seiner Datenschutzerklärung nicht darüber unterrichtet hat, ist er angehalten, zunächst die Datensubjekte über den Zweck des KI-Trainings in verständlicher Sprache zu informieren und ihre Einwilligung hierzu einzuholen. Dabei kann man sich die gängige Konstellation eines Nutzers vorstellen, den der Plattformbetreiber ohne Aufwand um seine Einwilligung bitten kann. Die Rechtslage lässt

19 Vgl. *Kamara/De Hert*, in: The Cambridge Handbook of Consumer Privacy, S. 321 (330).
20 EuGH NJW 2024, 417 (Rn. 76).
21 EDSA, Stellungnahme 28/2024, Rn. 69.
22 EDSA, Stellungnahme 28/2024, Rn. 71; vgl. EuGH ZD 2018, 420 (Rn. 113).
23 EDSA, Stellungnahme 28/2024, Rn. 74.
24 EDSA, Leitlinien 1/2024, S. 4.
25 EuGH NJW 2024, 3769 (Rn. 51–53).

sich bei öffentlich zugänglichen Daten aus Drittquellen anders beurteilen, denn aufgrund des damit einhergehenden enormen Aufwands ist die Identifizierung der einzelnen Betroffenen – geschweige die Einholung deren Einwilligung – wirtschaftlich unmöglich und dieses Vorgehen wäre auch im Zusammenhang mit Art. 11 und Art. 14 Abs. 5 DSGVO im Ergebnis datenschutzfeindlich.[26]

Auf der nächsten Ebene muss darüber hinaus in den verschiedenen Verarbeitungsphasen unter Zugrundelegung des Grundsatzes der Datenminimierung geprüft werden, ob die Datenverarbeitung erforderlich ist.[27] Im Zeitalter von KI ist dies Wunschdenken, denn „einen ausgewogenen Mittelweg zwischen Datenhunger und Datendürre zu finden, wird eine echte Herausforderung sein".[28] Dennoch kann die Einhaltung des Grundsatzes der Datenminimierung in Kombination mit dem Grundsatz der Datenrichtigkeit die Qualität der Trainingsdatensätze und somit die Funktion des KI-Modells positiv beeinflussen.[29] Die Richtigkeit von KI-Trainingsdaten ist insbesondere wichtig, „um falsche, diskriminierende oder verzerrte (biased) Ergebnisse auf der Output-Ebene zu verhindern".[30] Art. 10 Abs. 3 KI-VO schreibt vor, dass Trainingsdaten von Hochrisikosystemen hinsichtlich ihrer Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sein müssen.[31] Zur Einhaltung dieser Grundsätze müssten die KI-Entwickler nachweisen, dass sie die erhobenen Rohdaten gründlich bereinigt und validiert haben, bevor sie diese in geeignete Trainingsdaten umgewandelt haben.

III. Interessenabwägung: die (un)vernünftigen Erwartungen der Betroffenen

Zuletzt ist eine umfassende Abwägung der berechtigten Interessen des KI-Entwicklers mit den – möglicherweise – entgegenstehenden Interessen und Rechten der betroffenen Personen vorzunehmen. Hierbei handelt es

26 *Hacker* Law, Innovation and Technology 13 (2021), 257 (291) <https://doi.org/10.1080/17579961.2021.1977219>.
27 *Paal* ZfDR 2024, 129 (150); EDSA, Stellungnahme 28/2024, Rn. 73.
28 Auf Deutsch übersetzt: *Solove* Florida Law Review 77 (2025), 1 (26) <https://doi.org/10.2139/ssrn.4713111>.
29 *Pesch/Böhme* MMR 2023, 917 (917); *Paal* ZfDR 2024, 129 (142).
30 *Paal* ZfDR 2024, 129 (141).
31 *Paal* ZfDR 2024, 129 (141).

sich um eine Einzelfallprüfung unter Berücksichtigung sämtlicher Umstände der konkreten Verarbeitung.[32] Der EDSA verlangt dafür eine nachvollziehbar dokumentierte Einzelfallanalyse, die alle relevanten Faktoren einbezieht.[33] Zu den wesentlichen Abwägungskriterien gehören neben den relevanten Grundrechten und Grundfreiheiten der betroffenen Person sowie der jeweiligen Eingriffsintensität unter anderem auch die Art der Daten und Status der betroffenen Person, – im Einklang mit dem Wortlaut des Art. 6 Abs. 1 lit. f DSGVO „insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt" – die Vereinbarkeit der Verarbeitung mit den Verarbeitungsgrundsätzen, sowie die ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen.[34] Die Risiken reichen von Eingriffen in die Privatsphäre, Diskriminierung oder Einschränkungen der Meinungs- und Informationsfreiheit bis hin zu Gefahren für die körperliche und geistige Unversehrtheit.[35] Der EDSA fordert, sowohl mögliche Vorteile als auch negative Effekte für die Betroffenen zu berücksichtigen.[36] Maßgeblich sind die Art der Daten, der technische und organisatorische Kontext sowie alle Folgewirkungen.[37]

Besonders kritisch sind besondere Kategorien personenbezogener Daten wie unter anderem politische Meinungen und Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO, sowie darüberhinausgehende besonders sensible Daten, wie Finanz- oder Standortangaben.[38] Der EuGH hat im Zusammenhang mit Art. 9 Abs. 1 DSGVO klargestellt, dass schon das bloße Vorhandensein auch nur eines sensiblen Elements den gesamten Datensatz in den Anwendungsbereich des Verbots rückt; ohne einschlägige Ausnahme ist die Verarbeitung damit unzulässig.[39] Für die Ausnahme des Art. 9 Abs. 2 lit. e DSGVO („offensichtlich öffentlich gemacht") verlangt der EuGH zudem den Nachweis, dass die betroffene Person ihre Daten tatsächlich bewusst und eindeutig der Allgemeinheit zugänglich machen wollte.[40] Daraus folgt,

32 Vgl. BeckOK DatenschutzR/*Albers/Veit*, 52. Ed. 1.5.2025, DS-GVO Art. 6 Rn. 71.
33 EDSA, Leitlinien 1/2024, Rn. 12 ff.; vgl. *Herfurth* ZD 2018, 514 (515 ff.), der ein handbares „3x5-Modell" vorschlägt, das aus den drei Dimensionen „Daten", „Akteure" und „Datenverarbeitung" besteht.
34 Vgl. BeckOK DatenschutzR/*Albers/Veit*, 52. Ed. 1.5.2025, DS-GVO Art. 6 Rn. 71.
35 BeckOK DatenschutzR/*Albers/Veit*, 52. Ed. 1.5.2025, DS-GVO Art. 6 Rn. 71.
36 EDSA, Leitlinien 1/2024, Rn. 39.
37 EDSA, Leitlinien 1/2024, Rn. 39.
38 EDSA, Stellungnahme 28/2024, Rn. 84.
39 EuGH GRUR 2023, 1131 (Rn. 89).
40 EuGH GRUR 2023, 1131 (Rn. 90).

dass Art. 6 Abs. 1 lit. f DSGVO für das KI-Training mit besonderen Kategorien von personenbezogenen Daten, die mittels Scraping gesammelt wurden, in der Regel keine geeignete Rechtsgrundlage darstellt.[41] Der EDSA weist ferner unter Bezugnahme auf die Rechtsprechung des EuGH darauf hin, dass auch Umfang, Häufigkeit und die Kombination verschiedener Datensätze das Risiko erhöhen.[42]

Ein weiteres Abwägungskriterium, das explizit Erwgr. 47 DSGVO vorschreibt, sind die „vernünftigen Erwartungen" der Betroffenen:[43] So heißt es, dass„[a]uf jeden Fall … das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen [wäre], wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen". Der EDSA weist darauf hin, dass dies bei komplexen KI-Systemen besonders fragwürdig ist, weil sich Nutzungsmöglichkeiten und Datenflüsse den Betroffenen häufig nicht erschließen, wobei Transparenz allein noch keine Vorhersehbarkeit begründet.[44]

Das Abwägungskriterium der „vernünftigen Erwartungen" kann auch zu unvernünftigen Ergebnissen führen, wenn die Erwartungen der Betroffenen von datenschutzrechtswidrigen Praktiken beeinflusst werden. In diesem Zusammenhang wird betont, dass Verbraucher häufig die Praktiken marktbeherrschender Anbieter als gesellschaftlichen Standard akzeptieren; so könnten diese Anbieter ihre (möglicherweise unfairen) Praktiken als „vernünftige Erwartung" deklarieren.[45] Insbesondere im Kontext von öf-

41 Vgl. *Kuru* International Data Privacy Law 14 (2024), 326 (336 ff.) <https://doi.org/10.1093/idpl/ipae013>; *Ruschemeier* DuD 2025, 349 (354).

42 EDSA, Stellungnahme 28/2024, Rn. 86.

43 Siehe dazu ausführlich *Friedl*, Reasonable Expectations of Privacy – With Special Regard to European Privacy and Data Protection Law, 2025; sowie auch zur Geschichte des Konzepts siehe *Pohle*, Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, 2018, S. 188 f. mit Hinweis auf Katz v. United States, 389 U.S. 347 (1967).

44 EDSA, Stellungnahme 28/2024, Rn. 92; vgl. EuGH GRUR 2023, 1131 (Rn. 123).

45 *Kamara/De Hert*, in: The Cambridge Handbook of Consumer Privacy, S. 321 (335) mit Hinweis unter Fn. 78 auf *Zingales*.

fentlich verfügbaren Datensätzen erlaubt die bloße Tatsache, dass personenbezogene Daten online öffentlich zugänglich sind, sowie die faktische Zugriffsmöglichkeit der KI-Entwickler bei der Datensammlung mittels Scraping nicht den Schluss, die Betroffenen hätten die Kontrolle über ihre Daten endgültig aufgegeben und somit alle denkbaren Verarbeitungszwecke „vernünftigerweise" erwarten müssen.[46] Die Abwägung aus dem Prisma dieses Kriteriums erfordert eine spezifische Prüfung der vernünftigen Erwartungen des jeweiligen Datensubjekts. Da eine solche ressourcenaufwändige Individualisierung im Kontext der Sammlung öffentlich verfügbarer Daten praktisch ausscheidet, kann dieses Abwägungskriterium nur dann in diesem Kontext überhaupt geprüft werden, wenn man alle Betroffenen, deren Daten öffentlich verfügbar sind, als Gruppe betrachtet, um sodann deren vernünftigen Erwartungen zu kollektivieren, um zu einem Ergebnis zu gelangen. Diese Prüfung führt spätestens dann ad absurdum, wenn man zum Ergebnis kommt, dass alle Datensubjekte, deren personenbezogenen Daten öffentlich verfügbar sind, ungeachtet des spezifischen Kontextes der Veröffentlichung die Verarbeitung ihrer personenbezogenen Daten zum KI-Training vernünftigerweise hätten erwarten müssen.

Auf einer weiteren Stufe sind die möglichen risikomindernden Maßnahmen bei der Abwägung zu berücksichtigen: Basierend auf einem eher konsequentialistischen Ansatz vertritt der EDSA die Ansicht, dass selbst wenn nach der Bewertung die Interessen der Betroffenen überwiegen, der Verantwortliche dennoch zur Verarbeitung gelangen kann, wenn er zusätzliche – über die DSGVO-Pflichten hinausgehende – Garantien schafft.[47] Dazu gehören technische Garantien wie Pseudonymisierung, Maskierung, „Differential Privacy" oder andere Methoden, die zwar keinen vollständigen Anonymisierungsgrad erreichen müssen,[48] aber Re-Identifizierungsrisiken messbar absenken.[49] Ergänzend empfiehlt der EDSA, den Betroffenen zusätzliche Kontrollrechte einzuräumen – etwa ein gleich vor Beginn

46 Im Ergebnis so auch *Solove* Florida Law Review 77 (2025), 1 (26) <https://doi.org/10.2139/ssrn.4713111>.

47 EDSA, Stellungnahme 28/2024, Rn. 96–98.

48 Siehe dazu *Brown/Lee/Mireshghallah/Shokri/Tramèr*, What Does it Mean for a Language Model to Preserve Privacy?, in: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22), 2022, S. 2280 (2282) <https://doi.org/10.1145/3531146.3534642>.

49 EDSA, Stellungnahme 28/2024, Rn. 100 f.

des Trainings bedingungsloses Opt-out,[50] großzügige Lösch-/Entlern-Optionen und eine angemessene Karenzzeit zwischen Datenerhebung und Nutzung.[51] Mehr Transparenz lässt sich unter anderem durch leicht zugängliche Modellkarten, FAQ-Seiten, Informationskampagnen oder freiwillige Jahresberichte herstellen, die Kriterien, Quellen und Schutzvorkehrungen des Trainingsdatensatzes offenlegen.[52] Für Datensammlungen per Web-Scraping nennt der EDSA spezifische Schutzmaßnahmen, wie unter anderem den Ausschluss riskanter Quellen oder Datenkategorien, Beachtung von robots.txt/ai.txt-Signalen, zeitliche Limitierungen sowie eine vom Verantwortlichen gepflegte Opt-out-Liste, über die Betroffene das Crawling ihrer Inhalte untersagen können.[53] In der Einsatzphase empfiehlt der EDSA technische Filter, Wasserzeichen und andere Ausgabekontrollen, um Regurgitation, unberechtigte Weiterverwendungen oder Deepfakes einzudämmen; parallel sollen beschleunigte Verfahren für Lösch- und Berichtigungsanträge zur Verfügung stehen.[54] Schließlich erhöht die Veröffentlichung der eigenen Interessenabwägung sowie die frühzeitige Einbindung des Datenschutzbeauftragten Transparenz und Fairness gegenüber Betroffenen und Aufsichtsbehörden.[55]

D. Zur Berechtigung der „berechtigten Interessen"

I. Innovationsförderung oder Regelungsmechanismus von „prozeduraler Fairness"?

Dem Art. 6 Abs. 1 lit. f DSGVO ist das Spannungsverhältnis zwischen den Rechten des Betroffenen unter anderem dem Recht auf informationelle Selbstbestimmung aus Art. 8 EMRK,[56] dem Datenschutz aus Art. 8 GRCh und dem Schutz der Privatsphäre aus Art. 7 GRCh, auf der einen Seite und

50 Das Widerspruchsrecht gem. Art. 21 DSGVO wird im Gegensatz dazu a) ex post d.h. nach Beginn der Verarbeitung ausgeübt und b) kann die Verarbeitung nur bedingt i.S.v. Art. 21 Abs. 1 S. 2 DSGVO beenden.
51 EDSA, Stellungnahme 28/2024, Rn. 102.
52 EDSA, Stellungnahme 28/2024, Rn. 103.
53 EDSA, Stellungnahme 28/2024 Rn. 104 ff.
54 EDSA, Stellungnahme 28/2024, Rn. 107.
55 EDSA, Stellungnahme 28/2024, Rn. 108.
56 Auch aus Art. 8 EMRK wird ein Grundrecht auf informationelle Selbstbestimmung abgeleitet, vgl. Calliess/Ruffert/*Kingreen*, 6. Aufl. 2022, EU-GRCharta Art. 8 Rn. 5.

der „Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten" auf der anderen Seite inhärent. Als Panazee wird oft im Kontext von KI-Training der sehr breite und philosophisch kontextabhängige Begriff der Innovation erwähnt: Aus utilitaristischer Perspektive argumentiert *Hacker*, dass durch die Nutzung vorhandener Datensätze KI-Entwickler den Aufwand und die Kosten für die erneute Einholung von Einwilligungen minimieren können, ohne dabei die Sicherheit oder den Datenschutz der betroffenen Personen wesentlich zu beeinträchtigen.[57] *Paal* argumentiert, dass KI-Entwickler in der Regel ein wirtschaftliches Interesse verfolgen, indem sie Daten für das Training ihrer Systeme verarbeiten, um diese anschließend kommerziell anzubieten.[58] Über diesen rein ökonomischen Nutzen hinaus können aber auch ideelle und gemeinwohlbezogene Interessen eine Rolle spielen – etwa wenn ein KI-System im medizinischen oder gesundheitlichen Bereich einen gesellschaftlichen Mehrwert liefern soll.[59] Insbesondere in der Forschung können Entwickler zudem auf die Freiheit von Wissenschaft und Information als relevante ideelle Interessen verweisen.[60] In diesem Kontext wird sogar vertreten, dass das KI-Training ein berechtigtes Interesse per se darstellt, wobei es sich um eine vermeidbare denklogische Tautologie handelt.[61] Diese Ansätze beantworten nicht die zentrale Frage: was passiert, wenn die damit verfolgte Konsequenz bzw. „utility" zugunsten einer Personengruppe, aber zulasten einer anderen wirkt.

Buijsman, Klenk und van den Hoven[62] betonen, dass die grundlegenden philosophischen Theorien (Utilitarismus gegen Deontologische Theorien) zwar einen guten Ausgangspunkt für die Begründung der widersprüchlichen Werte in der philosophischen Debatte bieten, ihre analytische Kraft jedoch nicht ausreicht, um den feinen Nuancen kontextabhängiger ethischer Herausforderungen gerecht zu werden. Für eine praxisnahe KI-Ethik plädieren sie deshalb für Konzepte, die sich aus mittleren philosophischen Theorien in Kombination mit technologischen Designansätzen ableiten lassen. Es wird ferner unter Bezugnahme auf den Philosophen *Norman Da-*

57 *Hacker* Law, Innovation and Technology 13 (2021), 257 (291) <https://doi.org/10.1080/17579961.2021.1977219>.
58 *Paal* ZfDR 2024, 129 (149 f.).
59 *Paal* ZfDR 2024, 129 (149 f.).
60 *Paal* ZfDR 2024, 129 (149 f.).
61 *Franke* RDi 2023, 565 (567).
62 *Buijsman/Klenk/van den Hoven*, 3 – Ethics of AI, in: Smuha, Cambridge Handbook on the Law, Ethics and Policy of AI, 2024, S. 59.

niels[63] vertreten, dass die Gesellschaft bei fehlendem Konsens zu substanziellen Werten auf prozedurale Werte konzentrieren sollte, eine Art prozeduraler „Fairness".[64] Einen solchen Mechanismus prozeduraler Fairness kann Art. 6 Abs. 1 lit. f DSGVO darstellen, der – wie seine Entstehungsgeschichte zeigt – als technologische Öffnungsklausel konzipiert worden ist, die eine ad-hoc Abwägung der widerstreitenden Interessen unter Berücksichtigung der Umstände des Einzelfalls und risikomindernden Maßnahmen ermöglicht.

II. Im Zweifel für die informationelle Selbstbestimmung

Aus rechtspolitischer Perspektive ist aber kritisch anzumerken, dass die Kehrseite der Flexibilität des Abwägungsvorgangs Willkür begünstigt und Missbrauchspotential aufweist.[65] Fast jedes nicht ausdrücklich verbotene Ziel, dass zumindest abstrakt als innovationsfördernd rechtfertigen lässt, wird als „berechtigt" deklariert: Dabei darf der Begriff „Innovation" nicht pauschal als Totschlagargument dienen; nicht jede inkrementelle Produktverbesserung überwiegt die Interessen der Betroffenen so deutlich, dass ihre Einwilligung entbehrlich wäre.[66] Dem falschen Narrativ, EU-Bürger müssten aufgrund geopolitischen Drucks seitens USA und China und mangels einer wettbewerbsfähigen Wirtschaft im Namen eines politisch umstrittenen Innovationsbegriffs zugunsten der KI-Entwicklung auf ein hohes Datenschutzniveau verzichten, ist jedoch eine ungesunde Dosis Technosolutionismus und – hinsichtlich der blinden Nachahmung ausländischer Wirtschaftsmodelle – Provinzialismus zu attestieren. Chronische Unterinvestitionen in zukunftsweisende Technologien, fragmentierte Märkte und die starke Abhängigkeit von ausländischer Technologieinfrastruktur stellen weitaus gravierendere Bedrohungen für die Wettbewerbsfähigkeit der EU als der Wortlaut der DSGVO dar.[67]

63 *Daniels* Hastings Center Report 26 (1996), 6 (10, 11).

64 *Bak/Madai/Fritzsche/Mayrhofer/McLennan* Frontiers in Genetics 13 (2022), 929453 <https://doi.org/10.3389/fgene.2022.929453>.

65 Vgl. *Ferretti* Common Market Law Review 51 (2014), 843 (859); *Roßnagel* ZD 2014, 545.

66 Vgl. EuGH GRUR 2023, 1131 (Rn. 123); *Ruschemeier* DuD 2025, 349 (352); aA *Paal* ZfDR 2024, 129 (150 f.).

67 Vgl. *Csernatoni* The EU's AI Power Play: Between Deregulation and Innovation, 2025, S. 21 f.

Ebenfalls überzeugt das Argument der Kostenersparnisse nicht, wenn diese mit strukturellen Rechtsverstößen einhergehen.[68] Die Willkür liegt zudem in der frei wählbaren Steuerung des Blickwinkels auf die Abstraktionsebene des „berechtigten Interesses": Auf einer abstrakten Ebene wird das KI-Training mit übergeordneten Zielen wie öffentlicher Sicherheit und dem Schutz des Lebens begründet. Auf einer konkreteren Ebene könnte es jedoch faktisch darum gehen, ein KI-System mit wahlloser Überwachungstechnologie zu entwickeln, die in autoritären oder defizitär demokratischen Staaten zur politischen Unterdrückung eingesetzt werden kann. Dabei sind die vom KI-Entwickler verfolgten Ziele und geplanten Einsatzfelder des KI-Systems transparent anzugeben und im Abwägungsvorgang zu berücksichtigen. Solche Interessen, die auf verbotene KI-Praktiken im Sinne des Art. 5 KI-VO hinauslaufen, sind als keinesfalls berechtigt anzuerkennen.[69]

„Dark Patterns" unter anderem „Roach Motel" bzw. „false hierarchy" beim Design der Widerspruchsmöglichkeit, die Nutzern die Einlegung des Widerspruchs unter Verstoß gegen Art. 25 DSGVO de facto erschweren, stellen ebenso eine unerwünschte Folge des Opt-Out-Mechanismus des Art. 6 Abs. 1 lit. f DSGVO dar.[70] Der Vergleich der Regelungsmechanismen von Art. 6 Abs. 1 lit. a DSGVO und Art. 6 Abs. 1 lit. f DSGVO zeigt einerseits eine ex-ante Opt-in-Regelung mit bedingungsloser Widerrufsmöglichkeit und andererseits eine Opt-out-Regelung mit bedingter Widerspruchsmöglichkeit i.V.m. Art. 21 Abs. 1 DSGVO. Wie nutzerfreundlich der KI-Entwickler das Opt-out-Verfahren gestaltet, bestimmt maßgeblich, wie viele Nutzer tatsächlich Widerspruch einlegen, die Zahl sollte aber erfahrungsgemäß niedrig sein.[71] Damit wird Art. 6 Abs. 1 lit. f DSGVO – im Gegensatz zur informierten Einwilligung – zur besonders vorteilhaften Rechtsgrundlage für KI-Entwickler. Wie aber die Datenschutzgruppe bereits 2014 betonte: „Artikel 7(f) soll nicht zu einem einfachen Ausweg werden [Englisch:

68 *Ruschemeier* DuD 2025, 349 (352).

69 Vgl. EDSA, Stellungnahme 28/2024, Rn. 68, siehe dazu Fn. 54 in der Stellungnahme; zur aA, die den Abwägungsvorgang auf die Risiken des KI-Trainings im Input-Bereich beschränken möchte, siehe *Hacker* Law, Innovation and Technology 13 (2021), 257 (291) <https://doi.org/10.1080/17579961.2021.1977219>; *Paal* ZfDR 2024, 129 (156).

70 *Kyi/Shivakumar/Roesner/Santos/Zufall/Biega*, Investigating deceptive design in GDPR's legitimate interest, in: CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, 2023, S. 1 (12 f.) <https://doi.org/10.1145/3544548.3580637>.

71 *Kyi/Shivakumar/Roesner/Santos/Zufall/Biega*, in: CHI '23, S. 1 (12 f.).

an easy way out], um den Anforderungen des Datenschutzrechts zu entgehen".[72]

Ebenfalls kritisch zu betrachten ist der ergebnisorientierte Ansatz, der dem Abwägungsvorgang zugrunde liegt: Zum einen belässt der Regelungsmechanismus des Art. 6 Abs. 1 lit. f DSGVO den KI-Entwicklern die Entscheidung, ob ihre eigenen „berechtigten Interessen" überwiegen.[73] Auch wenn eine solche Entscheidung widerspruchsfähig und gerichtlich überprüfbar ist, lässt sich die rechtspolitische Frage stellen, ob der Abwägungsvorgang eine Übung der Rechenschaftspflicht *per se* oder eher eine Übung in rechtlicher Argumentation seitens des KI-Entwicklers darstellt, der ex post eine bereits gefällte Geschäftsentscheidung rechtfertigt, um zu einem bestimmten Abwägungsergebnis zu gelangen. Zum anderen bleibt zweifelhaft, ob ein Übermaß an risikomindernden Maßnahmen eine zuvor zugunsten der Betroffenen getroffene Abwägung wieder zugunsten des KI-Entwicklers verschiebt: Kompensieren Maßnahmen zur Datensicherheit Defizite bei der informationellen Selbstbestimmung?

De lege lata ist im Rahmen des Art. 6 Abs. 1 lit. f DSGVO der Einwilligung der Betroffenen als wenig einschneidendes Mittel bereits auf der Erforderlichkeitsebene Vorrang zu gewähren, soweit deren Einholung nicht aufwändig ist, d.h. immer dann, wenn der Verantwortliche bereits im Kontakt zum Betroffenen steht.[74] Im Ergebnis kann die Rechtsgrundlage des Art. 6 Abs. 1 lit. f DSGVO eine eingeschränkte Relevanz für Konstellationen des KI-Trainings aufweisen, wo die Einholung der Einwilligung der Betroffenen wirtschaftlich unmöglich ist, nämlich bei öffentlich verfügbaren personenbezogenen Daten aus Drittquellen. Selbst dann muss sichergestellt werden, dass keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO verarbeitet werden. Der Nachweis einer Ausnahme gemäß Art. 9 Abs. 2 DSGVO wird den KI-Entwicklern unter Berücksichtigung der Rechtsprechung des EuGH nämlich schwer gelingen: es ist faktisch kaum automatisiert zu prüfen, ob der Ausnahmetatbestand der offensichtlichen Veröffentlichung seitens des Betroffenen gemäß Art. 9 Abs. 2 lit. e DSGVO im Einzelfall eingreift.[75] Im Ergebnis heißt das, dass wenn die Daten vom KI-Entwickler selbst erhoben wurden, aber auch öffentlich zugänglich sind, er trotzdem (faktisch) die Einwilligung des Daten-

72 Article 29 Working Party, Opinion 06/2014, S. 5.
73 Vgl. bereits die Kritik zum risikobasierten Ansatz: *Rost* vorgänge Nr. 221/222 (2018), 79 (84).
74 EuGH NJW 2024, 3769 (Rn. 51–53).
75 EuGH GRUR 2023, 1131 Rn. 89 f.

subjekts und zugleich Nutzers als weniger einschneidendes Mittel einholen müsste.

Die Betroffenen haben in Ausübung ihrer unter Art. 8 GRCh gewährleisteten informationellen Selbstbestimmung ein ausgeprägtes Interesse daran, die Kontrolle über ihre Daten zu behalten. *Floridi*[76] weist darauf hin, dass gerade die zentrale Rolle von personenbezogenen Daten in modernen, datengetriebenen Anwendungen die ethischen Herausforderungen hinsichtlich des Datenschutzes verstärkt. Angesichts dieser Problematik sollte der Schutz der Privatsphäre und die Einhaltung klar definierter Einwilligungsstandards bei der Entwicklung und Anwendung von KI-Systemen oberste Priorität haben.[77] Das Argument, eine erneute Einwilligung könne den Betroffenen aufgrund ihrer „consent fatigue" nicht zugemutet werden,[78] überzeugt insbesondere dann nicht, wenn gerade die intransparente Datenerhebung zuvor zu dieser Ermüdung beigetragen hat. Die faktische Zugriffsmöglichkeit auf personenbezogene Daten rechtfertigt ferner keinesfalls die Schlussfolgerung, die Betroffenen hätten auf diese Kontrolle verzichtet oder sie hätten eine Verarbeitung ihrer Daten für das KI-Training zu verschiedenen Zwecken ‚vernünftigerweise' erwarten müssen. Eine solche Argumentation ist in der historisch als überholt geltenden binären Unterscheidung zwischen Öffentlichkeit und Privatheit gefangen und reduziert somit den Datenschutz lediglich auf Schutz der Privatheit.[79] Wie aber *Pohle* stattdessen plädiert: „Datenschutz heißt, informationell begründete soziale Macht in der Informationsgesellschaft unter Bedingungen zu stellen, sie zu zwingen, sich zu verantworten, und sie damit (wieder) gesellschaftlich verhandelbar zu machen."[80]

76 *Floridi*, The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities, Oxford: Oxford University Press 2023, S. 161.

77 *Floridi*, The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities, Oxford: Oxford University Press 2023, S. 161.

78 Siehe dazu *Paal* ZfDR 2024, 129 (148 f.).

79 *Rost* vorgänge #221/222 (2018), 79 (79 ff.).

80 *Pohle*, Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, 2018, S. 253; vgl. Schulz ZPTh Zeitschrift für Politische Theorie, 12 (2021), 84 (87). <https://doi.org/10.3224/zpth.v12i1.06>.

E. „Berechtigte Interessen" de lege ferenda?

De lege ferenda wird für ein konsequent risikobasiertes Modell plädiert, das die Pflichten der DSGVO graduell an das tatsächliche Gefährdungsniveau der betroffenen Personen anpasst und zugleich die Datenteilungsziele jüngerer EU-Instrumente – etwa des Data Act – reflektiert.[81] In diesen Kontext fügt sich der wissenschaftliche Diskussionsentwurf für eine künftige „KI-Datenschutz-Verordnung" ein, der für einen Workshop an der Universität Wien Anfang Dezember 2024 erarbeitet und von *Wendehorst* sukzessive in der KIR publiziert wurde.[82] Art. 11 des Entwurfs stellt eine neue Rechtsgrundlage für das KI-Training und andere Formen der Massendatenverarbeitung dar. Im Ergebnis erlaubt er Verantwortlichen, bei großskaligen Datenverarbeitungen wie KI-Training pauschal auf eine einzige Rechtsgrundlage nach Art. 6 oder 9 DSGVO zu verweisen, wenn (1) die Prüfung jeder einzelnen Datengrundlage „unverhältnismäßigen Aufwand" erfordern würde und (2) der Verantwortliche „angemessene Garantien" einsetzt.[83] Praktisch eröffnet Art. 11 damit eine pauschale Rechtfertigung gerade dort, wo Art. 9 DSGVO bislang Einwilligung oder andere eng auszulegende Ausnahmetatbestände fordert. Der Entwurf führt folglich zu einer faktischen Aushöhlung des Einwilligungserfordernisses und ist zumindest in Bezug auf Art. 11 abzulehnen. Im direkten Vergleich zeigen sich die Stärken des umfassenden einzelfallbezogenenAbwägungsvorgangs des Art. 6 Abs. 1 lit. f DSGVO, der aufeinanderprallende Interessen und die jeweiligen Risiken für die Betroffenen berücksichtigt und dabei das Ergebnis der Abwägung offen lässt.

Statt eines pauschalen Erlaubnistatbestandes für eine Datenverarbeitung zum Zwecke des KI-Trainings könnte man alternativ nur bestimmte Arten von datenbasierter Wertschöpfung privilegieren.[84] Dabei stellt sich das Dilemma, ob man durch die Privilegierung bestimmter Anwendungsfelder die Entwicklung bestimmter Technologien bremst, obwohl sie – sogar besser – geeignet wären, Wohlstand und andere erwünschte politische Ziele zu erreichen, auch wenn dies im Zeitpunkt der Gesetzgebung unabsehbar

81 *Bartels* GRUR Int. 2024, 526 (537).
82 *Wendehorst* KIR 2025, 142; *Wendehorst* KIR 2025, 174.
83 Vgl. *Wendehorst* KIR 2025, 174.
84 Vgl. dazu die Entstehungsgeschichte des Art. 6 Abs. 1 lit. f DSGVO: Im sogenannten Albrecht-Bericht wurde eine Positivliste vorgeschlagen, die bestimmte Anwendungsfälle des berechtigten Interesses explizit erfassen sollte, zum Beispiel die Datenverarbeitung im Kontext von Medien und Kunst.

ist. In diesem Zusammenhang wird die Unvorhersehbarkeit des Outputs generativer KI betont, das sich in unzähligen Kontexten und Anwendungsfeldern wiederverwenden lässt, zumal diese Systeme kontext-agnostisch trainiert werden.[85] Eine starre enge Aufzählung mittels einer Positivliste könnte legitime, gesellschaftlich wünschenswerte Anwendungen blockieren und gleichzeitig versäumen, neu entstehende Risikoszenarien abzudecken. Ebenso verfehlt ist die alternative Unterscheidung zwischen primär kommerziellen Interessen und gesellschaftlichen Interessen, denn dies missachtet solche forschungsgetriebenen Unternehmen etwa im Bereich der Biotechnologie, die kommerziell erfolgreich sein müssen, um der Gesellschaft einen effektiven Beitrag zu leisten. Wenn aber diese Positivliste breit und in Kombination mit anderen Rechtsgrundlagen, wie zB der informierten Einwilligung des Art. 6 Abs. 1 lit. a DSGVO und einer restriktiven Auslegung des Art. 6 Abs. 1 lit. f DSGVO konstruiert wird, könnte dies zugleich eine Privilegierung gesellschaftlich erwünschter Anwendungsbereiche bewirken und zugleich Innovation in unvorhersehbaren Anwendungsfeldern ermöglichen. Um der einwilligungsbezogenen Ermüdung entgegenzuwirken, muss der demokratisch legitimierte Gesetzgeber eine Grundsatzentscheidung darüber treffen, in welchen Anwendungsfeldern eine Datenverarbeitung als „berechtigt" anzusehen ist – und darf diese Entscheidung nicht den Verantwortlichen selbst überlassen, die den Abwägungsvorgang im Zweifel zugunsten ihrer eigenen Interessen auslegen.

Ein Vorbild für eine Ausgestaltung des Art. 6 Abs. 1 lit. f DSGVO de lege ferenda und zugleich ein geeignetes Rechtsinstrument zur gezielten politischen Förderung von Datenprojekten de lege lata ist die Datenverarbeitung gemäß Art. 59 KI-VO im Rahmen von KI-Reallaboren:[86] Art. 59 KI-VO normiert mit den sog. „KI-Reallaboren" einen Experimentierraum, in dem bereits erhobene personenbezogene Daten – unter Einhaltung strenger Dokumentations-, Transparenz- und Aufsichtsvorgaben – zweckgeändert zu Forschungs-, Trainings- und Testzwecken verarbeitet werden dürfen. Die Verarbeitungsgrundlage des Art. 59 Abs. 1 lit. a KI-VO setzt die Wahrung eines erheblichen öffentlichen Interesses in den enumerativ aufgelisteten

85 Vgl. *Solove* Artificial Intelligence and Privacy, Florida Law Review 77 (2025), 1 (25) <https://doi.org/10.2139/ssrn.4713111>; *Helberger/Diakopoulos*, ChatGPT and the AI Act, Internet Policy Review 12 (2023), 1 (2).

86 Vgl. dazu LfDI BW, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz – Diskussionspapier, Version 2.0 vom 17.10.2024 <https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/>.

Bereichen unter anderem öffentliche Sicherheit und öffentliche Gesundheit, Klimaschutz, nachhaltige Energie, Mobilität, kritischen Infrastrukturen und Netzen sowie effiziente öffentliche Verwaltung voraus.[87] Gemäß Art. 57 Abs. 9 KI-VO, Erwgr. 139 KI-VO sollen KI-Reallabore die Rechtssicherheit verbessern, Innovation und Wettbewerbsfähigkeit fördern, einen Beitrag zum evidenzbasierten regulatorischen Lernen leisten sowie den Zugang von KI-Systemen zum Unionsmarkt erleichtern und beschleunigen.[88] Somit wird ein synergetischer Wissenstransfer zwischen akademischen Forschungseinrichtungen, datengetriebenen Start-ups, regionalen KMU und zuständigen Aufsichtsbehörden ermöglicht. Erstere erhalten Zugriff auf qualitativ hochwertige Datensätze, um prototypische KI-Systeme realitätsnah zu validieren; letztere gewinnen zugleich frühzeitige Einblicke in technologische und datenschutzrechtliche Risikopotenziale und können so adaptive Regulierungsstandards entwickeln, was zur nachhaltigen Stärkung lokaler Innovationsökosysteme beiträgt. Das wäre eine Möglichkeit, wie wir als demokratische Gesellschaft, die informationelle Selbstbestimmung kollektiv ausüben und die Richtung der datenbasierten wirtschaftlichen Entwicklung mitbestimmen können – und zwar aufgrund berechtigter Interessen.

87 Martini/Wendehorst/*Botta*, 1. Aufl. 2024, KI-VO Art. 59 Rn. 16.
88 *Göbel/von Kruedener* GRUR-Prax 2024, 755 Rn. 12.