Thesenpapier
Juni 2026

Generative KI
Innovation und Recht in Arbeitsprozessen

Thema:

Zwischen Hype und Hybris: Zehn Thesen zu KI-kompatiblem Datenschutz

Wer zukunftstauglichen Datenschutz will, darf nicht nur Felder wie Bürokratieabbau oder Innovationsförderung betrachten. Es braucht einen mutigen Blick für das große Ganze – gerade auf generative KI.

iRights.Lab
Lösungen für Recht, Technologie, Politik & Gesellschaft

GenKI

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt

1 Eine Neufassung des EU-Datenschutzrechts – weil wir dazu gelernt haben

Seit Einführung der DSGVO im Jahr 2018 hat der europäische Datenschutz große Aufmerksamkeit erhalten. Meist jedoch stand er in der Kritik. Häufig wurde eine Reform gefordert, entweder zur Innovationsförderung oder als Beitrag zum Abbau vermeintlich überflüssiger Bürokratie. Überzeugender ist, das bestehende Datenschutzrecht im Sinne guten rechtsstaatlichen Handelns („good governance“) weiterzuentwickeln: Dafür ist einerseits die Einbeziehung aller gewonnenen Erfahrungen aus Unternehmens-, Aufsichts- und Gerichtspraxis wichtig, um bisherige Problemstellungen, Unklarheiten und Nachschärfungsbedarfe gemeinsam anzugehen. Andererseits müssen aber auch jene Personen zu Wort kommen, die sich intensiv mit dem zukünftigen Verhältnis von generativer KI und Datenschutz auseinandersetzen.

2 Maschinelles Lernen und Big Data stellen den Wert einzelner Datenpunkte grundsätzlich in Frage

Wer einen zukunftstauglichen und KI-kompatiblen Datenschutz möchte, muss sich der Größe der Aufgabe bewusst sein. Die realen und vermeintlichen Potenziale generativer KI-Systeme haben das Grundkonzept der DSGVO unter existenziellen Druck gesetzt. Darüber, ob einzelne Datenpunkte auch in Zukunft noch Bedeutung und auch Wert zugeschrieben bekommen sollten, gibt es gegensätzliche Ansichten. Wo die DSGVO noch Lösch- und Korrekturpflichten in Bezug auf einzelne Daten aufstellt, setzt die KI-Entwicklung auf heuristische Auswertung und stochastische Zusammenhänge in kaum mehr zu erfassenden Datenmengen. Es scheint, als entzögen Qualität und Quantität der für die KI-Entwicklung erforderlichen Daten dem datenschutzrechtlichen Konzept zunehmend den Boden.

3 Bei einem KI-kompatiblen Datenschutz muss das gesamte Datenrecht mitgedacht werden

Dass der Wert einzelner Datenpunkte unklar geworden ist, ist kein reines Datenschutzproblem:
Die urheberrechtliche TDM-Schranke– eine gesetzliche Ausnahmeregelung zum „Text und Data Mining“ - wurde als Innovationsförderung angekündigt und von KI-Anbieter*innen als Erlaubnis zur genehmigungsfreien Nutzung urheberrechtlicher Werke beim KI-Training verstanden. Schließlich komme es für die KI-Entwicklung auf das einzelne Werk gar nicht an.

Auch das Marken- und Designrecht verhindert KI-Training mit geschützten Bild- oder Wortmarken nicht. Eine Angleichung dieser und weiterer gesetzlichen Rahmenbedingungen erscheint sinnig und zweckmäßig, um Umsetzungsprobleme durch fragmentierte Rechtsrahmen zu verhindern.

4 Politik und Gesetzgebung können sich von innovationsfreundlichen Konzepten aus Wissenschaft, Wirtschaft und Zivilgesellschaft inspirieren lassen

In Wissenschaft, Wirtschaft und Zivilgesellschaft finden sich längst Ansätze, die den vermeintlich verringerten Wert und die womöglich abnehmende Bedeutung einzelner Datenpunkte ins Datenschutzrecht übertragen wollen. So könnte man die Rechtmäßigkeit einer großen Datenverarbeitung nicht mehr von jedem Teildatum abhängig machen. Und auch Betroffenenrechte könnten in Bezug auf solche Verarbeitungsschritte ausgenommen werden, wenn es bei ihnen gar nicht um spezifische Einzeldaten gehen soll. Datenschutz wäre also als Sorgfaltspflicht gegenüber einer Datenmehrheit zu verstehen und nicht als Schutz individuell zuzuordnender Informationen. Diese Ansätze schließen an verschiedene etablierte Fachdiskurse an – zum Beispiel an die vom EuGH angestoßene Diskussion zum Begriff des „personenbezogenen Datums“.

5 Der Wert einzelner Datenpunkte hängt mit dem Verständnis von Datenschutz als Menschenrechtsschutz in einer digitalisierten Welt zusammen

Ein Datenschutzrecht, dass zwar systematische Rechtsgutsverletzungen in den Blick nimmt, aber die Rechtschutzmöglichkeiten von Individuen beschränkt, etwa im Sinne eines digitalen Verbraucherschutz- und Ordnungsrechts, ist durchaus denkbar. Es lässt sich sogar argumentieren, dass ein solches System vergleichsweise leicht zu handhaben und womöglich sogar effizienter wäre. Über eine entsprechende Rechtsanpassung müsste dann aber auch im Bereich von zum Beispiel Hate Speech, Deep Fakes und Social Bots diskutiert werden: Schließlich ist auch der individuelle Schutz von Meinungsfreiheit, Religionsfreiheit und Identität ist vom Schutz und der Bedeutung individualisierbarer Datenpunkte abhängig. Bei ganzheitlicher Betrachtung lassen sich damit in der aktuellen datenschutzrechtlichen Reformdebatte Tendenzen wahrnehmen, die den Charakter des europäischen Grund- und Menschenrechtsschutz insgesamt (unbewusst) in Frage zu stellen scheinen.

6 Ein KI-kompatibler Datenschutz der Zukunft muss als Teil digitaler Menschenrechte verstanden werden

Gerade in einer Gegenwart, in der Smartphones zentrale Hilfsmittel für die Bewältigung des Alltags sind, KI-Systeme im beruflichen Kontext bei wichtigen Arbeitsschritten unterstützen und einem demografischen Wandel mit mehr Technik und Automatisierung begegnet werden soll, muss ein zukunftsfähiges, KI-kompatibles Datenschutzrecht individueller Menschenrechtsschutz bleiben. Politik, Wissenschaft, Wirtschaft und Zivilgesellschaft müssen den Wert, die Bedeutung und die Vorteile dieses Grundansatzes hervorheben und auf diese Weise zu einem neuen, positiveren Image beitragen – etwa durch gemeinsame Werbekampagnen von Bundesministerien und der Industrie, durch aufeinander Bezug nehmende Interviews und Pressemitteilungen, oder durch die Hervorhebung von Best Practices aus Wissenschaft und Wirtschaft. Dazu gehören aber auch Reformen, die die datenschutzrechtlichen Regelungen risikobasiert weiterentwickelt: Vereine und Unternehmen, die keine risikorelevanten Verarbeitungen vornehmen, sollten einerseits entlastet werden, und global agierende Digitalunternehmen andererseits höheren Auflagen entsprechen müssen.

7 Es braucht klare Rechtsgrundlagen für Entwicklung und Einsatz von KI

Das gilt gerade für generative KI: Ihre Entwicklung und ihr Einsatz müssen rechtskonform möglich sein, ohne hierfür übermäßigen Haftungsrisiken ausgeliefert zu sein. Bisher müssen Organisationen und Unternehmen prüfen und sicherstellen, dass in jedem KI-Verarbeitungskontext die eigenen Verarbeitungsinteressen überwiegen. Das überfordert gerade kleine Organisationen und Unternehmen. Statt den einzelnen Verantwortlichen eine komplizierte Interessensabwägung aufzuerlegen, muss der europäische Gesetzgeber hier selbst vorangehen. Er muss die einzustellenden Interessen und Argumente abwägen und eine präzise gefasste, neue Rechtsgrundlage schaffen – auch und gerade in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Das schafft Rechtssicherheit, von der vor allem nicht-digitalspezifische Organisationen und Unternehmen profitieren.

8 Keine Chatbot-DSGVO: Agentic & Public AI als relevante Szenarien für zukunftstauglichen Datenschutz berücksichtigen

Wer das Datenschutzrecht reformieren will, darf nicht bei heutigen KI-Modellen wie LLMs oder generativen KI-Systemen (wie Chatbots) stehen bleiben. Daten, auf die KI-Agenten zugreifen müssen, um zum Beispiel als persönliche Assistenz von Privatpersonen zu funktionieren, sollten schon heute mitgedacht werden. Dasselbe gilt für gemeinschaftlich organisierte KI-Systeme des öffentlichen Informationsmanagements, die in ganz Europa unter dem Begriff „Public AI“ immer öfter gefordert werden. Beide Entwicklungen sind bei datenschutzrechtlichen Reformüberlegungen zu bedenken und einzubeziehen, und könnten durch passgenaue Erleichterungen und Voraussetzungen im Datenrecht gezielt gefördert oder gesteuert werden.

9 Public AI als Beleg: Datenpunkte haben weiterhin einen Wert – im KI-Output

Gerade Konzepte wie Public AI zeigen zudem: Mag der Wert einzelner Datenpunkte im Rahmen des KI-Trainings in Zweifel stehen – für den KI-Output bleibt er unbestritten. Anders würden Ansätze zu einem KI-basierten Wissens- und Informationsmanagement – sei es proprietär oder gemeinwohlbasiert – nicht tragen. Diese setzen unverändert auf Präzision, Vollständigkeit, Nachvollziehbarkeit und Korrigierbarkeit von Informationen und Daten, die vom System ausgegeben werden. Eine Reform des Daten(schutz)rechts muss daher den Output wesentlich anders behandeln als die KI-Entwicklung.

10 Handeln statt abwarten – zwischen “best practice” und “failing forward”

Parallel zu Reformbemühungen in Brüssel sollten auch andere Akteur*innen als EU mit Mitgliedstaaten zu einem zukunftsfähigeren Datenschutz beitragen. Besonders gefördert werden sollten Maßnahmen zum aktiven Wissensaustausch zu best und worst practices in Wissenschaft, Wirtschaft und Zivilgesellschaft – auch unter Einbeziehung der nationalen Aufsichtsstellen. Einen Beitrag könnten hier auch freiwillige Register leisten, in denen staatliche und privatwirtschaftliche KI-Nutzer*innen ihre Dokumentationen, Datenschutzfolgenabschätzungen und Abwägungserläuterungen öffentlich einsehbar hinterlegen. Diese und weitere Maßnahmen können dabei helfen, praxisnahe Anwendungen zu etablieren, Kosten zu senken und gerade durch den Austausch mit Fachbehörden auch Rechtsunsicherheiten zu verringern.

Impressum

Ein Thesenpapier im Rahmen des iRights.Lab-Forschungsprojekts
Generative KI – Innovation und Recht in Arbeitsprozessen (GenKI-IR)

Grundlage des Thesenpapiers waren die Arbeiten der Zukunftslabore
zu dem Thema „KI-DSGVO“. Wir danken allen Teilnehmer*innen der Zukunftslabore.

iRights.Lab GmbH
Oranienstr. 185
D-10999 Berlin
Telefon: +49 (0)30 40 36 77 230
Fax: +49 (0)30 40 36 77 260
E-Mail: kontakt@irights-lab.de

Geschäftsführer: Philipp Otto
Projektleitung: Solvejg Gunkel
Autor: Dr. Matthieu Binder

Redaktion: Lena Biskup, Solvejg Gunkel, Dr. Till Kreutzer,
Merlin Münch, Henry Steinhau
Illustration und Gestaltung: Gustav Berneburg
Lektorat: Kathrin Maurer
Juni 2026

Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 185640 B
Finanzamt für Körperschaften II
USt-IdNr.: DE311181302
Inhaltlich Verantwortlicher i.S.d.§18 Abs.2 MStV:
Philipp Otto (Anschrift siehe oben)

iRights.Lab
Lösungen für Recht, Technologie, Politik & Gesellschaft

GenKI

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt