

KI-gestützte Überwachung von Unterlassungserklärungen im Verbraucherrecht – Potenziale und rechtliche Grenzen am Beispiel von „KIVEDU“

Von Zina Al-Washash, Prof. Dr. Steffen Kroschwald und Prof. Dr. Thomas Schuster, Pforzheim*

Einrichtungen, die regelmäßig Verstöße gegen Verbraucherschutzrecht im digitalen Raum abmahnen, stoßen bei der manuellen Nachverfolgung erhaltener Unterlassungserklärungen an organisatorische Grenzen. Das Projekt „KIVEDU – Künstlich-intelligente Verbraucherdurchsetzung“ setzt hier an. Entwickelt wurde ein KI-gestütztes System, das Unterlassungserklärungen strukturiert erfasst, gezielt Webinhalte prüft und potenzielle kerngleiche Verstöße automatisiert identifiziert und dokumentiert. Der Beitrag beleuchtet die technischen Grundlagen dieses Systemansatzes und ordnet die datenschutz-, urheber- und KI-rechtlichen Rahmenbedingungen ein, unter denen KI ein wirksames Monitoring von Unterlassungspflichten im Verbraucherrecht unterstützen kann.

I. Einleitung und Problemstellung

Die effektive Durchsetzung verbraucherschützender Normen ist ein zentraler Bestandteil des Verbraucherrechts.¹ Neben der staatlichen Rechtsdurchsetzung kommt dem sogenannten „Private Enforcement“², insbesondere durch strafbewehrte Unterlassungserklärungen (einschließlich vertraglicher Unterlassungsvereinbarungen), erhebliche praktische Bedeutung zu. Qualifizierte Einrichtungen, Wettbewerbsverbände und Mitbewerber können damit Rechtsverstöße effizient außergerichtlich unterbinden, in dem sie den Schuldner abmahnen und ihn im Rahmen einer Unterlassungserklärung dazu verpflichten, die beanstandete Handlung künftig zu unterlassen sowie für den Fall der Zuwiderhandlung eine Vertragsstrafe zu zahlen.³

In der Praxis zeigt sich jedoch ein strukturelles Vollzugsdefizit. Zwar werden Unterlassungsansprüche regelmäßig erfolgreich initial durchgesetzt, die anschließende Kontrolle ihrer dauerhaften Einhaltung bleibt jedoch häufig lückenhaft.⁴ Insbesondere im digitalen Raum ist die Überwachung von Unterlassungsansprüchen ressourcenintensiv und technisch anspruchsvoll. Verstöße treten in großer Zahl, dynamisch und in vielfältigen Erscheinungsformen auf.

Hinzu kommt, dass Unterlassungserklärungen regelmäßig nicht nur identische, sondern auch sogenannte „kerngleiche“ Handlungen erfassen. Darunter fallen Verhaltensweisen, die zwar nicht wort- oder bildgleich sind, in denen jedoch das Charakteristische der ursprünglichen Verletzungshandlung zum Ausdruck kommt.⁵ Die Herausforderung besteht daher nicht allein in der Identifikation identischer Verstöße, sondern insbesondere in der Erkennung und rechtlichen Einordnung vergleichbarer Erscheinungsformen. Die hierfür erforderliche kontinuierliche Prüfung verlangt eine wertende Analyse des Unterlassungsgehalts sowie dessen Übertragung auf neue, häufig vari-

ierende Sachverhalte. Sie wird bislang weitgehend manuell durchgeführt und ist folglich mit erheblichem Aufwand verbunden. Angesichts begrenzter personeller und technischer Ressourcen bleiben zahlreiche Verstöße unentdeckt, sodass die präventive Wirkung von Unterlassungserklärungen teilweise abgeschwächt wird.

Vor diesem Hintergrund rücken digitale Technologien und insbesondere Systeme der Künstlichen Intelligenz (KI) in den Fokus. Sie bieten die Möglichkeit, wiederkehrende Prüfprozesse zu automatisieren, große Datenmengen auszuwerten und potenzielle Verstöße frühzeitig zu identifizieren. Das im Rahmen des Invest-BW-Programms durchgeführte Projekt „KIVEDU – Künstlich-intelligente Verbraucherdurchsetzung“⁶ setzt hier an. Ziel war die Entwicklung eines KI-gestützten Systems, das wesentliche Prüfschritte automatisiert: vom Einlesen der Unterlassungserklärungen über das gezielte Web-Crawling bis hin zur Identifikation und gerichtsfesten Dokumentation potenzieller Verstöße.

Der Einsatz solcher Technologien wirft zugleich grundlegende rechtliche Fragen auf. Zu berücksichtigen sind insbesondere datenschutzrechtliche Anforderungen, urheberrechtliche Grenzen des Web-Crawlings und -Scrapings sowie die Vorgaben der europäischen KI-Verordnung.

Der Beitrag untersucht, inwieweit KI bei der Überwachung der Einhaltung von Unterlassungserklärungen und -vereinbarungen im Verbraucherrecht effektiv unterstützen kann. Am Beispiel des Projekts KIVEDU werden die technischen Grundlagen dargestellt und die damit verbundenen rechtlichen Herausforderungen exemplarisch aufgezeigt. Ziel ist es, Potenziale und

* Zina Al-Washash, LL.M., war bis Ende 2025 akademische Mitarbeiterin am Institut für Verbraucherforschung und nachhaltigen Konsum (vunk) an der Hochschule Pforzheim u.a. im Projekt KIVEDU und befasste sich insbesondere mit rechtlichen Fragestellungen der Digitalisierung und des Verbraucherschutzes. Prof. Dr. Steffen Kroschwald, LL.M., lehrt Europäisches und Internationales Wirtschaftsrecht und ist Direktor des Instituts für Verbraucherforschung und nachhaltigen Konsum (vunk) an der Hochschule Pforzheim. Prof. Dr. Thomas Schuster ist Professor für Datenbanken und Softwaretechnik an der Hochschule Pforzheim, Leiter des futureLAB sowie wissenschaftlicher Koordinator der Campus-IT. Das Autorenteam dankt Vincent Goetze, LL.B., herzlich für die wertvolle Unterstützung bei der Endredaktion des Manuskripts.

1 Brönneke/Tonner, in: Kenning/Oehler/Reisch Verbraucherwissenschaften, 2. Aufl. 2021, S. 148.

2 Begriff zum Beispiel bei BeckOK Datenschutzrecht/Schröder, DGA Art. 12 Rn. 88.

3 Einführend BeckOK UWG/Scholz, UWG § 13 Rn. 4.

4 So bereits als Problemstellung des KIVEDU-Projekts beschrieben bei Waidelich et al., Using large language models for the enforcement of consumer rights in Germany, Lecture Notes in Business Information Processing (LNBI, volume 495), 2023.

5 U.a. BGH 6.2.2013 – I ZB 79/11, RUR 2013, 1071 (1072 Rn. 14).

6 Gefördert im Rahmen des Invest-BW-Programms des Ministeriums für Wirtschaft, Arbeit und Tourismus, Förderkennzeichen BW1/3092/03 gem. Bescheid vom 2.2.2023, geändert durch Bescheid vom 30.10.2024.

Grenzen KI-gestützter Verbraucherrechtsdurchsetzung im Kontext des Private Enforcement einzuordnen.

II. Rechtlicher Rahmen: Unterlassungserklärungen im Verbraucherrecht

Das Verbraucherrecht ist durch eine Vielzahl spezialgesetzlicher Regelungen geprägt, die das Marktverhalten von Unternehmen im Interesse der Verbraucher steuern. Diese finden sich insbesondere im Bürgerlichen Gesetzbuch sowie in zahlreichen spezialgesetzlichen Vorschriften. Für die Durchsetzung von Unterlassungsansprüchen kommt dem Lauterkeitsrecht eine zentrale Bedeutung zu.⁷ Das Gesetz gegen den unlauteren Wettbewerb (UWG) untersagt unlautere geschäftliche Handlungen gegenüber Verbrauchern und Mitbewerbern. Nach § 3a UWG sind auch Verstöße gegen solche gesetzlichen Vorschriften unlauter, die dazu bestimmt sind, im Interesse der Marktteilnehmer das Marktverhalten zu regeln. Auf diese Weise fungiert das Lauterkeitsrecht als Durchsetzungsinstrument für eine Vielzahl verbraucherschützender Normen.

Verstöße gegen diese Vorschriften begründen nach § 8 Abs. 1 UWG Unterlassungsansprüche, die im Wege der Abmahnung und strafbewehrten Unterlassungserklärung geltend gemacht werden können. Die Reichweite der Unterlassungsverpflichtung erstreckt sich dabei regelmäßig nicht nur darauf, den konkreten Verstoß nicht zu wiederholen, sondern auch auf kerngleiche Verstöße, die als solche vom Unterlassungsgläubiger identifiziert und bewertet werden müssen.⁸ Anspruchsberechtigt sind insbesondere Mitbewerber, qualifizierte Wirtschaftsverbände sowie nach dem Unterlassungsklagengesetz eingetragene Einrichtungen. Die praktische Durchsetzung erfolgt damit maßgeblich im Wege des „Private Enforcement“.

III. KI als Lösungsansatz – das KIVEDU-System im Überblick

KIVEDU automatisiert wesentliche Prozessschritte bei der Dokumentation und Nachverfolgung von Unterlassungsansprüchen. Das System unterstützt mit KI-basierter Texterkennung bereits bei der Erfassung und Verwaltung von Vorgängen im Zusammenhang mit Abmahnungen, insbesondere der Unterlassungserklärung. Es übernimmt sodann die regelmäßige Kontrolle auf mögliche Folgeverstöße und versendet im Falle erneuter Verstöße Benachrichtigungen an Unterlassungsgläubiger.⁹

Die technische Umsetzung von KIVEDU folgt dem Ziel, den nachgelagerten manuellen Prüfprozess durch eine modulare Systemarchitektur zu digitalisieren und zu skalieren. Der Gesamtprozess wird durch die Anwender (zB potenziell Nutzende in Verbraucherzentralen) initiiert, die die Unterlassungserklärung als PDF-Dokument über das Frontend in das System hochladen. Von dort aus wird das Dokument an die KIVEDU-Mikroservices zur weiteren Verarbeitung übergeben. Die Prüfung erfolgt dabei in mehreren Schritten: Zunächst werden relevante Textpassagen extrahiert und in Bezug zur Unterlassungsverpflichtung gesetzt. Anschließend erfolgt eine semantische Bewertung, bei der das System prüft, ob eine inhaltliche Übereinstimmung oder funktionale Gleichartigkeit vorliegt. Die Ergebnisse werden priorisiert und für eine rechtliche Nachprüfung aufbereitet.

Nach dem Durchlaufen der „Analyse-Pipeline“ schließt sich hier auch wieder der Kreis, indem die aufbereiteten Ergebnisse im Frontend zur Sichtung und Prüfung bereitgestellt werden. Maßgebend sind folgende Funktionen:

- **Wissensbasierte Datenstrukturierung:** Ausgangspunkt ist die Unterlassungserklärung als rechtliches Referenzdokument. Diese wird durch Verfahren der automatisierten Texterkennung und -strukturierung (Large Language Model) in eine maschinenlesbare Form überführt. Dabei werden insbesondere die untersagten Verhaltensweisen sowie deren charakteristische Merkmale extrahiert und als Prüfmaßstab aufbereitet.
- **Zielgerichtete Untersuchung (Web-Crawling):** Zur Identifikation potenzieller Verstöße scannt das System die relevanten digitalen Präsenzen des Schuldners (zB Online-Shops, Produktauftritte auf Online-Marktplätze). Dies erfolgt über Web-Crawling- und Scraping-Verfahren, die relevante Inhalte auffinden und für die weitere Analyse verfügbar machen. Die Herausforderung besteht dabei nicht allein in der Datenerhebung, sondern insbesondere in der inhaltlichen Bewertung der erfassten Informationen.
- **KI gestützte Verstoßidentifikation:** Hier setzt der Einsatz von KI-gestützten Analyseverfahren an, insbesondere von Large Language Models (LLMs). Diese ermöglichen eine semantische Verarbeitung natürlicher Sprache und sind in der Lage, inhaltliche Zusammenhänge über reine Wortgleichheit hinaus zu erkennen. Auf dieser Grundlage kann das System nicht nur identische Verstöße identifizieren, sondern auch solche, bei denen das charakteristische Element der untersagten Handlung in abgewandelter Form fortbesteht.
- **Gerichtsfeste Beweissicherung und Dokumentation:** Wird durch die semantische Analyse ein potenzieller Verstoß detektiert, stößt das System automatisch die Sicherung und Archivierung der betroffenen Webinhalte für die Beweissicherung an. Die strukturierten Daten werden anschließend in einer Datenbank gespeichert. Wird hingegen kein potenzieller Verstoß erkannt, wird das Verfahren an dieser Stelle ohne weitere Schritte beendet.

KIVEDU versteht sich dabei nicht als autonom entscheidendes System, sondern als Assistenzsystem. Die abschließende rechtliche Bewertung verbleibt beim Menschen.

IV. Rechtliche Herausforderungen

1. Datenschutzrecht

a) *Anwendung.* Der Einsatz des KIVEDU-Systems ist mit der Verarbeitung potenziell personenbezogener Daten verbunden und unterliegt daher den Vorgaben der Datenschutz-Grundverordnung (DSGVO). Deren Anwendungsbereich ist bereits eröffnet, wenn Informationen verarbeitet werden, die sich auf identi-

7 Ausf. hierzu Brönneke/Tonner, in: Kenning/Oehler/Reisch, Verbraucherwissenschaften, 2. Aufl. 2021, S. 144 ff.

8 Zur Herausforderung, kerngleiche Verstöße im Rahmen von (festgestellten) Unterlassungsansprüchen zu identifizieren BeckOK UWG/Scholz, UWG § 12 Rn. 181.

9 Hierzu u.a. Waidelich et al., Using large language models for the enforcement of consumer rights in Germany, Lecture Notes in Business Information Processing (LNBIP, volume 495), 2023.

fizierte oder identifizierbare natürliche Personen beziehen (Art. 4 Nr. 1 DSGVO).

Im Rahmen von KIVEDU können personenbezogene Daten insbesondere in zwei Konstellationen betroffen sein: Zum einen bei der automatisierten Erfassung und Analyse von Webinhalten, die etwa Impressumsangaben, Kontaktdaten oder sonstige identifizierende Informationen enthalten können. Zum anderen bei der Verarbeitung von Unterlagen aus Abmahnverfahren und Unterlassungserklärungen sowie bei der Nutzung des Systems selbst, etwa durch Protokoll- und Zugriffsdaten.

Die datenschutzrechtliche Bewertung ist dabei maßgeblich von der konkreten Ausgestaltung der Datenverarbeitung abhängig. Zu unterscheiden ist insbesondere zwischen der Entwicklungsphase des Systems und dessen späterem operativen Einsatz. Während in der Entwicklungsphase eine Verarbeitung personenbezogener Daten durch den Einsatz anonymisierter oder synthetischer Datensätze vermieden werden kann,¹⁰ ist in der Anwendungsphase regelmäßig von einer Verarbeitung personenbezogener Daten auszugehen. Dies kann einerseits Bestands- und Nutzungsdaten von Systemanwendern betreffen, aber auch die in eingelesenen Unterlassungserklärungen enthaltenen personenbezogenen Daten (etwa Namen der Parteien, wenn es sich um natürliche Personen handelt oder ihren Vertretern). Beim Crawling und Scraping können ferner im Netz befindliche Daten mit Personenbezug miterfasst und damit verarbeitet werden; etwa solche in Impressums- oder Kontaktangaben. Verantwortlich im datenschutzrechtlichen Sinne sind dabei typischerweise die anwendenden Stellen, wie beispielsweise Verbraucherzentralen oder Wettbewerbsverbände, während der Systembetrieb – je nach Ausgestaltung – als Auftragsverarbeitung einzuordnen sein kann.

b) Datenschutzrechtliche Gestaltungsanforderungen. Vor diesem Hintergrund kommt der datenschutzkonformen Ausgestaltung des Systems zentrale Bedeutung zu. Maßgeblich sind insbesondere die Vorgaben des Art. 25 DSGVO, wonach Datenschutzanforderungen bereits bei der technischen Konzeption zu berücksichtigen sind.¹¹ Ziel ist es, die Verarbeitung personenbezogener Daten von vornherein auf das erforderliche Maß zu beschränken und datenschutzrechtliche Risiken bereits auf Ebene der Systemarchitektur zu minimieren.

Dabei ist zwischen Entwicklungs- und Anwendungsphase zu differenzieren. In der Entwicklungsphase kann die Verarbeitung personenbezogener Daten weitgehend vermieden werden.¹² Im Projekt KIVEDU wurde hierfür konsequent auf anonymisierte Unterlagen und synthetische Testumgebungen zurückgegriffen.¹³ Dies ermöglicht es, Funktionsfähigkeit und Leistungsfähigkeit der eingesetzten KI-Modelle zu überprüfen, ohne reale personenbezogene Daten zu verarbeiten.

In der Anwendungsphase tritt demgegenüber die praktische Verarbeitung personenbezogener Daten in den Vordergrund. Hier ist sicherzustellen, dass die Verarbeitung auf das erforderliche Maß beschränkt bleibt (vgl. Erwägungsgrund 78 DSGVO). Dies betrifft insbesondere die Ausgestaltung von Eingabemasken, die Festlegung von Löschfristen sowie die Beschränkung von Zugriffsrechten.¹⁴

Auch bei der automatisierten Erfassung von Webinhalten sind Datenminimierung und Zweckbindung leitend. Die Datenerhebung hat sich auf solche Informationen zu beschränken, die für

die Identifikation möglicher Verstöße erforderlich sind. Nicht erforderliche personenbezogene Daten sind – soweit technisch möglich – auszublenden oder zu anonymisieren. Dies lässt sich in der Praxis zum Beispiel durch automatisierte Vorverarbeitungsschritte unmittelbar bei der Datenerfassung realisieren, etwa durch den Einsatz von Named Entity Recognition (NER) zur Maskierung unstrukturierter Identitätsdaten oder durch musterbasierte Filter für strukturierte Kontaktinformationen.¹⁵

Darüber hinaus ist die Nachvollziehbarkeit der Verarbeitung sicherzustellen. Die Ergebnisse der KI-gestützten Analyse müssen für die Anwender verständlich und überprüfbar aufbereitet werden. Nur so kann gewährleistet werden, dass die automatisierte Voranalyse in eine eigenständige rechtliche Bewertung überführt werden kann. In diesem Zusammenhang spricht aus datenschutzrechtlicher Sicht vieles dafür, bei der Auswahl des Large Language Models auf Open-Source-Modelle zurückzugreifen. Offene Architekturen erleichtern die Nachvollziehbarkeit der Datenverarbeitung und unterstützen damit die Umsetzung des Transparenzgrundsatzes (Art. 5 Abs. 1 lit. a DSGVO).¹⁶

Schließlich ist eine geschlossene und lokal abgesicherte Systemumgebung erforderlich, die unbefugte Zugriffe und unkontrollierte Datenweitergaben verhindert.¹⁷ Hierzu zählen insbesondere Zugriffsbeschränkungen, Protokollierung sowie geeignete technische und organisatorische Schutzmaßnahmen.

c) Rechtsgrundlagen der Verarbeitung. Die datenschutzrechtliche Zulässigkeit der Verarbeitung richtet sich nach Art. 6 Abs. 1 DSGVO und ist für die einzelnen Verarbeitungsschritte gesondert zu bestimmen.

Eine Einwilligung der betroffenen Person kommt nur eingeschränkt in Betracht. Sie ist insbesondere für die Verarbeitung von Daten Dritter, die im Rahmen des Crawling erfasst werden, regelmäßig nicht praktikabel.

Auch die Verarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 lit. b DSGVO ist auf Fälle beschränkt, in denen die betroffene Person selbst Vertragspartei ist. Dies betrifft im KIVEDU-Kontext primär das bestehende Schuldverhältnis zwischen Unterlassungsgläubiger und -schuldner. Dabei bemisst sich die Zulässigkeit an der zweckgebundenen Erforderlichkeit. Für darüberhinausgehende Datenverarbeitungen, insbesondere im Zusammenhang mit öffentlich zugänglichen Webinhalten, scheidet diese Rechtsgrundlage aus.

¹⁰ Vgl. BeckOK Datenschutzrecht/Schantz, 55. Ed., DSGVO Art. 5, Rn. 24 ff. zum Grundsatz der Datenminimierung.

¹¹ Paal/Pauly, 4. Aufl. 2026, DSGVO/Martini, DSGVO Art. 25 Rn. 10; Angelehnt an: DSK, Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Version 1.0, Stand: Juni 2025.

¹² Vgl. zur Datenminimierung BeckOK Datenschutzrecht/Schantz, 55. Ed., DSGVO Art. 5, Rn. 24 ff.

¹³ Vgl. DSK, Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ vom 6.5.2024, Version 1.0, S. 5 und S. 7 f.

¹⁴ Vgl. DSK, Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ vom 6.5.2024, V 1.0, S. 8 u. S. 13; EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, V 2.0, Rn. 51 ff., 83 ff.

¹⁵ Hierzu beispielsweise Li/Sun/Han/Li, A Survey on Deep Learning for Named Entity Recognition, in: IEEE Transactions on Knowledge and Data Engineering, 2022 (34, 1), S. 50 ff.

¹⁶ DSK, Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen vom Juni 2025, Version 1.0, S. 10.

¹⁷ DSK, Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ vom 6.5.2024, Version 1.0, S. 6.

Als primäre Rechtsgrundlage kommt regelmäßig Art. 6 Abs. 1 lit. f DSGVO in Betracht. Die Verarbeitung kann auf berechnete Interessen gestützt werden, wenn sie zur Durchsetzung von Unterlassungsansprüchen erforderlich ist und die Interessen der betroffenen Personen nicht überwiegen.¹⁸ Im Rahmen der hierbei gebotenen Interessenabwägung sind die konkrete Ausgestaltung der Datenverarbeitung sowie die implementierten Schutzmaßnahmen entscheidend. Für die Praxis erfordert dies den Nachweis belastbarer Lösch- und Einschränkungskonzepte, leicht zugänglicher Widerspruchskanäle sowie einer transparenten Information der Betroffenen.

d) *Keine automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO.* Der Einsatz von KIVEDU begründet regelmäßig keine automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO.¹⁹ Das System trifft keine eigenständigen, rechtlich verbindlichen Entscheidungen, sondern dient der Unterstützung bei der Identifikation potenzieller Verstöße.

Die abschließende Bewertung bleibt einer natürlichen Person vorbehalten. Voraussetzung ist allerdings, dass diese Bewertung nicht lediglich formal erfolgt, sondern auf einer eigenständigen Prüfung beruht. Hierfür ist es erforderlich, dass die vom System generierten Ergebnisse nachvollziehbar aufbereitet werden und eine eigenständige rechtliche Würdigung ermöglichen.²⁰

Damit handelt es sich bei KIVEDU um ein System der Entscheidungsunterstützung, nicht um eine automatisierte Entscheidungsfindung im datenschutzrechtlichen Sinn.

2. Urheberrechtliche Anforderungen an Crawling und Scraping

Der Einsatz von Web-Crawling- und Scraping-Technologien im Rahmen von KIVEDU wirft, neben datenschutzrechtlichen, insbesondere urheberrechtlichen Fragen auf. Das System durchsucht automatisiert Webseiten, analysiert Inhalte und erstellt im Fall eines potenziellen Verstoßes einen statischen Export der betreffenden Webseite als Beweismittel. Dabei kann nicht ausgeschlossen werden, dass urheberrechtlich geschützte Inhalte erfasst und technisch vervielfältigt werden. KIVEDU bewegt sich damit in einem Spannungsfeld zwischen effizienter Beweisgewinnung und den Grenzen des Urheberrechts, insbesondere den Schrankenregelungen und dem Schutz technischer Maßnahmen.

a) *Urheberrechtlicher Schutzgegenstand.* Das Urheberrecht schützt Werke im Sinne von § 2 UrhG, sofern diese eine persönliche geistige Schöpfung („Schöpfungshöhe“) aufweisen. Praktisch relevant sind vor allem:

- **Sprachwerke** (§ 2 Abs. 1 Nr. 1 UrhG), etwa Produktbeschreibungen, Werbetexte oder redaktionelle Inhalte, sofern sie über schlicht beschreibende Formulierungen hinausgehen und ein Mindestmaß individueller Gestaltung erreichen.²¹
- **Lichtbildwerke bzw. Lichtbilder** (§ 2 Abs. 1 Nr. 5 UrhG), insbesondere Produkt- und Werbefotos,²² die im Rahmen von Webshops oder Plattformen angezeigt werden. In der Grundversion von KIVEDU ist zwar keine eigenständige Bildanalyse vorgesehen, dennoch können Lichtbilder durch den statischen Export einer Webseite als Beweismittel erfasst werden.
- **Datenbankwerke** (§ 4 UrhG) und **Datenbanken** im Sinne des Leistungsschutzrechts (§ 87a UrhG). Webshops, Preisvergleichs- und Anzeigenportale, die primär Ziel des Systems

sind, erfüllen häufig zumindest die Anforderungen des Datenbankherstellerschutzes, da Struktur, Zusammenstellung und laufende Aktualisierung regelmäßig eine wesentliche Investition darstellen.²³

Vor diesem Hintergrund ist davon auszugehen, dass KIVEDU bei der automatisierten Erfassung regelmäßig auf urheberrechtlich relevante Inhalte trifft, auch wenn der Fokus des Systems auf der Verstoßprüfung gegenüber Unterlassungspflichten liegt und nicht auf der wirtschaftlichen Auswertung dieser Inhalte.

b) *Vervielfältigung.* Vervielfältigung bedeutet im Sinne der §§ 15 Abs. 1 Nr. 1, 16, 87b UrhG jede körperliche Festlegung eines Werkes, unabhängig vom Medium.²⁴ Bereits das temporäre Zwischenspeichern im Arbeitsspeicher kann als Vervielfältigung gelten.²⁵ Beim Crawling und Scraping werden Inhalte von Webseiten automatisiert abgerufen, verarbeitet und in der Regel zumindest vorübergehend gespeichert. Erfolgt ein statischer Export der Webseite oder wird ein Datensatz dauerhaft gespeichert, liegt eine dauerhafte Vervielfältigung vor.²⁶

Handelt es sich bei den betroffenen Inhalten um Werke oder Datenbanken im Sinne des UrhG, sind diese Vorgänge urheberrechtlich relevant. Da eine individuelle Einwilligung der Rechteinhaber typischerweise fehlt, kann sich die Zulässigkeit allein aus gesetzlichen Schranken oder aus im Einzelfall eingeräumten Nutzungsrechten ergeben.

c) *Schranken.* In Betracht kommen insbesondere §§ 44a, 44b, 45 Abs. 1 UrhG, § 60d UrhG²⁷ sowie – ergänzend – die Einräumung von Nutzungsrechten nach § 31 UrhG. Für KIVEDU sind Reichweite, Voraussetzungen und Grenzen dieser Normen zu prüfen.

aa) *§ 44a UrhG – vorübergehende Vervielfältigungen.* § 44a UrhG erlaubt flüchtige oder begleitende Vervielfältigungen, die einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen, deren alleiniger Zweck die Übertragung in einem Netz oder eine rechtmäßige Nutzung ist und die keine eigenständige wirtschaftliche Bedeutung haben.²⁸ Klassische

18 Vgl. OLG München ZVertriebsR 2018, 394 Rn. 30 zu berechtigtem Interesse gem. Art. Abs. 1 lit. f DSGVO bei der Ermittlung von Schadensersatzansprüchen; Gola/Heckmann, DSGVO/Schulz, 3. Aufl. 2022, DSGVO Art. 6 Rn. 69; Ehmann/Selmayr, DSGVO/Heberlein, 3. Aufl. 2024, DSGVO Art. 6 Rn. 40; Spindler/Schuster/Kaesling, DSGVO/Dalby, DSGVO Art. 6 Rn. 18.

19 Vgl. grundlegend zur Definition der ausschließlich automatisierten Entscheidung EuGH 7.12.2023 – C-634/21, ECLI:EU:C:2023:957, NZA 2024, 45, Rn. 42.

20 Nach entsprechender Auslegung darf die menschliche Zwischeninstanz den automatisierten Systemvorschlag nicht lediglich formal übernehmen, da andernfalls der Schutzzweck des Art. 22 Abs. 1 DSGVO unterlaufen würde, vgl. EuGH 7.12.2023 – C-634/21, ECLI:EU:C:2023:957, NZA 2024, 45, Rn. 45; zur Übertragbarkeit dieser Rechtsprechung auf KI-gestützte Vorschlagssysteme siehe HmbBfDI, Pressemitteilung vom 7.12.2023 „Auswirkungen des Schufa-Urteils auf KI-Anwendungen.“

21 BeckOK Urheberrecht/Rauer/Bibi, 49. Ed., UrhG § 2 Rn. 78.

22 LG Mannheim GRUR-RS 2021, 62027 Rn. 32.

23 Siehe auch: Wandtke/Bullinger, UrhG/Hermes, 6. Aufl. 2022, UrhG § 87a Rn. 93 ff.

24 BeckOK Urheberrecht/Götting, 49. Ed., UrhG § 16 Rn. 5a.

25 BeckOK Urheberrecht/Götting, 49. Ed., UrhG § 16 Rn. 5a.

26 Skupin GRUR-Prax 2024, 752 (752).

27 Maamar ZUM 2023, 481 (483 ff.).

28 Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 44a Rn. 1; Maamar ZUM 2023, 481 (486).

Beispiele sind Browser-Caching oder temporäre Kopien in Netzwerkkomponenten.²⁹

Übertragen auf KIVEDU können vorübergehende Kopien beim Crawling privilegiert sein, sofern sie technisch notwendig sind,³⁰ automatisch wieder gelöscht werden und der Abruf der Seite an sich rechtmäßig erfolgt. Dies setzt voraus, dass der hypothetische manuelle Abruf durch eine Person ebenfalls rechtlich zulässig wäre.³¹ Dauerhafte Vervielfältigungen – insbesondere statische Exporte, die als Beweismittel gespeichert und ggf. vor Gericht vorgelegt werden – lassen sich über § 44a UrhG allerdings nicht rechtfertigen. Die Norm bildet daher lediglich einen Baustein für den Umgang mit flüchtigen Kopien im laufenden Such- und Abgleichprozess.

bb) § 44b UrhG – Text und Data Mining. § 44b UrhG erlaubt Vervielfältigungen rechtmäßig zugänglicher Werke zum Zwecke des Text- und Data-Minings, einschließlich Datenbankwerken und Datenbanken.³² KIVEDU erfüllt mit seinen analysierenden Funktionen zentrale Merkmale eines solchen Text- und Data-Minings. Wesentliche Voraussetzungen sind:

- **Rechtmäßiger Zugang:** Die Inhalte müssen ohne Rechtsverstoß abrufbar sein, etwa frei zugängliche Webseiten ohne Zugangssperren oder Lizenzverstöße.³³
- **Löschungspflicht:** Vervielfältigungen sind zu löschen, sobald sie für das jeweilige Text- und Data-Mining-Projekt nicht mehr erforderlich sind. Eine auf Dauer angelegte Speicherung eines Trainingskorpus oder von Analyse-Datensätzen zur beliebigen späteren Wiederverwendung ist damit ausgeschlossen.³⁴
- **Kein wirksamer Nutzungsvorbehalt („Opt-out“)** des Rechteinhabers (§ 44b Abs. 3 UrhG).³⁵

Für KIVEDU folgt hieraus die Notwendigkeit eines Löschkonzepts, das etwa vorsieht, dass Trainingsdatensätze, Testkorpora oder operative Kopien nach Projektende oder nach Abschluss der jeweiligen Analysephase gelöscht werden. Zudem ist zu prüfen und zu dokumentieren, ob Nutzungsvorbehalte bestehen.

Rechteinhaber können sich Nutzungen nach § 44b Abs. 1 UrhG vorbehalten; bei online zugänglichen Werken muss der Opt-out in maschinenlesbarer Form erklärt werden.³⁶ Praktisch werden unterschiedliche Ansätze diskutiert: Erklärungen in natürlicher Sprache, technische Standards wie ein TDM-Reservation-Protocol³⁷ oder die Nutzung von robots.txt³⁸. Mangels verbindlicher Standards und gefestigter Rechtsprechung besteht Rechtsunsicherheit. KIVEDU-Anwender sind daher gut beraten, unterschiedliche Formen von Nutzungsvorbehalten zu beachten und deren Prüfung zu dokumentieren.

§ 60d UrhG regelt ergänzend Text- und Data-Mining für Zwecke der wissenschaftlichen Forschung und war in der Forschungs- und Erprobungsphase von KIVEDU relevant. Für den hier interessierenden produktiven Einsatz steht hingegen § 44b UrhG im Vordergrund.

cc) § 45 Abs. 1 UrhG – Vervielfältigung für gerichtliche Verfahren. § 45 Abs. 1 UrhG erlaubt die Herstellung einzelner Vervielfältigungsstücke von Werken „zur Verwendung in Verfahren vor einem Gericht, einem Schiedsgericht oder einer Behörde“. Die Vorschrift zielt auf die Nutzung von Werken als Beweismittel oder sonstiges Hilfsmittel im Verfahren ab.³⁹ Streitig ist, wie weit im Vorfeld eines Verfahrens diese Privilegierung reicht.

Für KIVEDU könnte § 45 Abs. 1 UrhG dann relevant werden, wenn ein Verstoß gegen eine Unterlassungspflicht bereits konkretisiert ist und die Beweissicherung mit Blick auf ein absehbares Verfahren erfolgt.⁴⁰ Rein vorsorgliche, breit angelegte Scans des Internets ohne konkreten Verfahrensbezug werden von der Schranke hingegen eher nicht erfasst.⁴¹ Die Norm kann daher punktuell zur Rechtfertigung bestimmter Vervielfältigungen beitragen, ersetzt jedoch keine allgemeine urheberrechtliche Grundlage des Betriebs.

dd) § 31 UrhG – Einräumung von Nutzungsrechten. Unabhängig von Schranken können Rechteinhaber Nutzungsrechte nach § 31 UrhG einräumen. Denkbar ist etwa, dass Unterlassungsschuldner im Rahmen der Unterlassungserklärung ihr Einverständnis mit einem Crawling und Scraping ihrer eigenen Inhalte zu Kontrollzwecken erklären. Dies kann die Nutzung eigener Werke durch den Unterlassungsschuldner legitimieren.

Für KIVEDU greift diese Lösung jedoch nur begrenzt, weil häufig auch Werke Dritter (zB Produktbilder anderer Urheber oder fremde Rezensionstexte) betroffen sind, deren Rechteinhaber weder bekannt noch erreichbar sind. § 31 UrhG ist deshalb eher als ergänzende Option in Sonderkonstellationen zu verstehen, nicht als tragende Grundlage des Standardbetriebs.

ee) Zwischenergebnis. Eine potentiell rechtswidrige Vervielfältigung im Rahmen des Crawling und Scraping kann durch §§ 44a, 44b und – in Einzelfällen – § 45 Abs. 1 UrhG privilegiert sein; § 31 UrhG eröffnet punktuell zusätzliche Nutzungsmöglichkeiten. In allen Fällen sind Zweckbindung, Löschpflichten, Nutzungsvorbehalte (Opt-outs) und technische Schutzmaßnahmen zu beachten. KIVEDU muss daher technisch und organisatorisch so ausgelegt sein, dass flüchtige und dauerhafte Kopien kontrolliert, zeitlich begrenzt und dokumentiert werden und Nutzungsvorbehalte sowie Schutzmechanismen respektiert werden.

d) § 95a UrhG – Schutz technischer Maßnahmen. § 95a UrhG verbietet die Umgehung wirksamer technischer Maßnahmen zum Schutz von Werken oder sonstigen Schutzgegenständen

29 Wandtke/Bullinger, UrhG/Welser, 6. Aufl. 2022, UrhG § 44a Rn. 5.

30 EuGH 5.6.2014 – C-360/13, ECLI:EU:C:2014:1195, GRUR Int. 2014, 694 Rn. 28.

31 Ein Argument ließe sich hier aus Analogie zum zulässigen Medienstreaming herleiten. Hier wird argumentiert, dass eine begleitende Vervielfältigung zulässig sei, wenn auch die Nutzung sich erlaubt sei: BeckOK Urheberrecht/Schulz, 49. Ed., UrhG § 44a Rn. 13.

32 Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 44b Rn. 6.

33 Maamar ZUM 2023, 481 (483); Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes v. 9.3.2021, BT-Drs. 19/27426, 88.

34 Maamar ZUM 2023, 481 (483).

35 Maamar ZUM 2023, 481 (483).

36 Pukas/Nordmann GRUR-Prax 2024, 639 (639); Welser NJW 2024, 3383 (3390); LG Hamburg MMR 2024, 973 mAnm Hoeren/Matras/Groschmann MMR 2024, 979.

37 Bomhard InTeR 2023, 174 (179).

38 Maamar ZUM 2023, 481 (484); Heine GRUR-Prax, 87, 88.

39 BT-Drs. IV/270, 63 (zu § 45).

40 LG Düsseldorf GRUR-RR 2007, 139 (194); so wohl auch einhellig die Meinung in der Literatur, etwa BeckOK Urheberrecht/Schulz/Poththast, 49. Ed., UrhG § 45 Rn. 8 ff.; Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 45 Rn. 6; Schricker/Loewenheim, UrhG/Melichar/Stieper, 6. Aufl. 2020, UrhG § 45 Rn. 6; Wandtke/Bullinger, UrhG/Lüft, 22. Aufl. 2022, UrhG § 45 Rn. 3; Ulrich DS 2011, 352 (356).

41 Wandtke/Bullinger, UrhG/Lüft, 6. Aufl. 2022, UrhG § 45 Rn. 3.

ohne Zustimmung des Rechtsinhabers.⁴² Im KIVEDU-Betrieb dürfen daher Schutzmechanismen – etwa Captchas, Bot-Sperren, Zugriffsbeschränkungen oder besondere Anti-Scraping-Technologien – nicht umgangen werden, wenn sie zumindest auch dem Schutz urheberrechtlich geschützter Inhalte dienen.⁴³

Ob allgemeine Anti-Bot-Mechanismen als technische Maßnahmen im Sinne des § 95a UrhG einzuordnen sind, ist nicht abschließend geklärt. Die Rechtsprechung zur Umgehung technischer Schutzmaßnahmen und zur Einbindung fremder Inhalte (etwa beim Framing) deutet jedoch darauf hin, dass Gerichte schon das Umgehen technischer Zugangsschranken als relevante Umgehungshandlung werten können.⁴⁴ Für KIVEDU führt dies dazu, dass der Einsatz auf Webseiten mit erkennbar technischen Schutzmaßnahmen gegen automatisierte Zugriffe unterbleiben oder – soweit rechtlich eröffnet – auf ein Mindestmaß beschränkt bleiben muss.

§ 95b UrhG gewährt privilegierten Nutzern (etwa für Text- und Data-Mining nach § 44b UrhG) unter bestimmten Voraussetzungen einen Anspruch auf Bereitstellung der zur Nutzung notwendigen Mittel, begrenzt aber die Befugnis zur Umgehung nicht generell.⁴⁵ In der Praxis wird sich KIVEDU daher primär an der Vermeidung der Umgehung technischer Schutzmaßnahmen ausrichten müssen.

e) Fazit Urheberrecht. Web-Crawling und -Scraping im Rahmen von KIVEDU können urheberrechtlich geschützte Inhalte (Texte, Bilder, Datenbanken) erfassen und vervielfältigen. Ohne Zustimmung der Rechteinhaber bedarf es hierfür einer gesetzlichen Schranke oder einer konkreten Nutzungsrechtseinräumung. § 44b UrhG bildet eine zentrale Grundlage für Text- und Data-Mining-Vorgänge; er setzt rechtmäßigen Zugang, Löschung nach Abschluss des jeweiligen Projekts und das Fehlen wirksamer Opt-outs voraus. § 44a UrhG kann flüchtige, technisch bedingte Vervielfältigungen privilegieren, § 45 Abs. 1 UrhG Vervielfältigungen mit konkretem Verfahrensbezug. § 95a UrhG begrenzt die Zulässigkeit, soweit technische Schutzmaßnahmen betroffen sind; deren Umgehung ist unzulässig.

Die urheberrechtliche Zulässigkeit hängt damit maßgeblich von der Einhaltung der Schrankenregelungen, der Beachtung von Nutzungsvorbehalten, der Respektierung technischer Schutzmaßnahmen und einem belastbaren Lösch- und Dokumentationskonzept ab. In vielen Standardfällen – etwa bei schlichten Produktangaben mit niedriger Schöpfungshöhe – wird das Urheberrecht faktisch nicht berührt oder verbleibt im Bereich des Risiko-Minimus; rechtliche Zweifelsfragen lassen sich jedoch nicht vollständig eliminieren und sollten durch entsprechende Governance-Strukturen minimiert werden.

3. KI-Verordnung

a) Anwendungsbereich. Die KI-Verordnung (KI-VO) schafft einen unionsweiten Rechtsrahmen für Entwicklung, Inverkehrbringen und Betrieb von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck. Persönlich erfasst sind insbesondere Anbieter, Betreiber, Importeure, Händler und Bevollmächtigte (Art. 2 Abs. 1 KI-VO).⁴⁶ Anbieter ist, wer ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter eigenem Namen oder eigener Marke in Verkehr bringt oder in Betrieb nimmt (Art. 3

Nr. 3 KI-VO). Betreiber ist, wer ein KI-System in eigener Verantwortung verwendet (Art. 3 Nr. 4 KI-VO); beide Rollen könnten im Kontext von KIVEDU von unterschiedlichen Akteuren besetzt werden.

KIVEDU erfüllt die Definition eines KI-Systems nach Art. 3 Nr. 1 KI-VO: Es handelt sich um ein maschinengestütztes System, das zumindest teilweise autonom arbeitet und aus Eingaben (Unterlassungserklärungen, Webseiten, Parameter für die Verstoßprüfung) Ausgaben (Hinweise, Bewertungen, Risikoscores) generiert, die Entscheidungen über weitere Maßnahmen beeinflussen können. Kernelement ist die KI-gestützte Textanalyse, die auf einem eingebundenen Sprachmodell basiert. Dieses Sprachmodell kann zugleich die Kriterien eines KI-Modells mit allgemeinem Verwendungszweck erfüllen; insoweit richten sich einschlägige Pflichten primär an dessen Anbieter außerhalb des Projekts.

Territorial gilt die KI-VO, sobald KI-Systeme in der Europäischen Union in Verkehr gebracht, in Betrieb genommen oder ihre Ergebnisse in der Union verwendet werden (Art. 2 Abs. 1 KI-VO). Da KIVEDU auf EU-basierte Akteure wie Verbraucherorganisationen zielt und innerhalb der EU betrieben wird, ist der sachliche und territoriale Anwendungsbereich grundsätzlich eröffnet. Ausnahmen – etwa für rein private Nutzung – sind vorliegend nicht einschlägig; denkbar ist lediglich, dass bestimmte quelloffene Komponenten unter speziellen Erleichterungen stehen, soweit sie nicht selbst als Hochrisikosysteme eingesetzt werden.

b) Risikoklassifizierung und Folgen. Die KI-VO ordnet KI-Systeme risikobasiert ein: in verbotene Praktiken (inakzeptables Risiko), Hochrisikosysteme sowie in Systeme mit geringem oder minimalem Risiko.⁴⁷ Je nach Einstufung ergeben sich unterschiedlich weitreichende Pflichten.⁴⁸

Nach Art. 5 KI-VO verbotene Praktiken – etwa Systeme, die Personen in unzulässiger Weise manipulieren, spezifische Schwächen ausnutzen oder eine sozialschädliche Verhaltenssteuerung bezwecken – werden durch KIVEDU nicht verwirklicht. KIVEDU dient der Unterstützung zivilrechtlicher Unterlassungsdurchsetzung und ist weder auf die Ausnutzung schutzbedürftiger Gruppen noch auf verdeckte Beeinflussung angelegt.

Eine Einstufung als Hochrisiko-System nach Art. 6 ff. KI-VO setzt grundsätzlich voraus, dass das System entweder als Sicherheitsbauteil bestimmter Produkte fungiert (Art. 6 Abs. 1 KI-VO) oder in einem der in Anhang III genannten besonders sensiblen Bereiche eingesetzt wird (zB Zugang zu Bildung, Beschäftigung, grundlegenden Diensten, Strafverfolgung, Rechtspflege).⁴⁹ KIVEDU ist nicht darauf angelegt, Entscheidungen in diesen Kernbereichen zu treffen oder unmittelbare Zugangsentschei-

42 Dreier/Schulze, UrhG/Specht-Riemenschneider/Raue, 8. Aufl. 2025, UrhG § 95a Rn. 1; Wandtke/Bullinger, UrhG/Wandtke/Ohst, 6. Aufl. 2022, UrhG, § 95a Rn. 2.

43 EuGH 9.3.2021 – C-392/19, ECLI:EU:C:2021:181, GRUR 2021, 706 Rn. 55.

44 BGH 30.4.2014 – I ZR 224/12, BeckRS 2014, 12115 Rn. 37; BGH 22.6.2011 – I ZR 159/10, Beck RS 2011, 22670 Rn. 69; EuGH 9.3.2021 – C-392/19, ECLI:EU:C:2021:181, GRUR 2021, 3582.

45 Bisges/Dittl/Freys et al., Handbuch Urheberrecht, 2. Aufl. 2022, Rn. 734.

46 Borges CR 2024, 497 (505).

47 Schwenke DB 2024, 205 (205).

48 Schwenke DB 2024, 205 (205).

49 von Welser GRUR-Prax 2024, 485 (486 f.).

dungen zu grundlegenden Leistungen zu steuern. Es unterstützt vielmehr den Vollzug bereits bestehender zivilrechtlicher Unterlassungspflichten durch Recherche und Dokumentation. Bei bestimmungsgemäßem Gebrauch liegt daher eine Hochrisikoeinordnung fern; weite Teile des streng regulierten Hochrisikoregimes (etwa umfassendes Risikomanagementsystem, Konformitätsbewertung, CE-Kennzeichnung) sind nicht einschlägig.

Gleichwohl können einzelne allgemeine Pflichten, insbesondere Transparenzanforderungen nach Art. 50 KI-VO,⁵⁰ relevant sein: KIVEDU soll gegenüber den natürlichen Personen, die das System bedienen, transparent machen, dass sie mit einem KI-System interagieren und welche Rolle dessen Ergebnisse im Entscheidungsprozess spielen. Da es sich um eine interne Fachanwendung für geschulte Mitarbeitende handelt, ist der Umfang dieser Transparenzpflichten begrenzt und deckt sich weitgehend mit ohnehin gebotenen Informationspflichten nach Datenschutz- und Organisationsrecht.

Unabhängig von der Risikoklasse gilt Art. 4 KI-VO: Alle Akteure haben für ein angemessenes Maß an KI-Kompetenz zu sorgen.⁵¹ Für KIVEDU bedeutet dies, dass Betreiber sicherstellen müssen, dass zuständige Mitarbeitende die Funktionsweise, Grenzen und Risiken des Systems verstehen, insbesondere den unterstützenden Charakter der KI-Auswertung und die Eigenverantwortung bei der rechtlichen Einordnung der Ergebnisse.

c) *Fazit KI-VO.* KIVEDU fällt in den Anwendungsbereich der KI-VO, wird aber bei regelgerechter Nutzung nicht als Hochrisiko-System eingestuft und verwirklicht keine verbotenen Praktiken.⁵² Für Anbieter und Betreiber resultieren damit vor allem:

- **Transparenz- und Informationspflichten** gegenüber Systemnutzern, die klarstellen, dass sie mit einem KI-System arbeiten und wie die Ergebnisse in Entscheidungsprozesse einfließen.
- **Anforderungen an KI-Kompetenz** des beteiligten Personals (Art. 4 KI-VO), die in der Praxis mit Schulungen, internen Leitlinien und Dokumentation der Systemgrenzen umgesetzt werden können.
- **Dokumentations- und Governance-Pflichten** in einem Umfang, der deutlich unterhalb der Hochrisiko-Regulierung liegt und weitgehend mit den aus Datenschutz- und Berufsrecht bekannten Anforderungen harmoniert.

Insgesamt fungiert die KI-VO für KIVEDU eher als ergänzender Ordnungsrahmen, der bestehende Compliance-Strukturen (insbesondere aus Datenschutz und IT-Sicherheit) systematisiert, ohne zusätzliche, schwergewichtige Zertifizierungs- oder Konformitätslasten auszulösen.

V. Ergebnis

KIVEDU setzt bei einem praktischen Vollzugsdefizit des Verbraucherrechts an: der systematischen Kontrolle strafbewehrter Unterlassungspflichten im digitalen Raum. Der Ansatz, Unterlassungserklärungen strukturiert zu erfassen, mit Hilfe eines LLM gestützt durch Crawling und Scraping gegen laufende Webangebote zu spiegeln und mögliche Verstöße mit statischer Dokumentation zu sichern, eröffnet Verbraucherverbänden und ähnlichen Akteuren eine Form der Überwachung, die in der bisherigen, primär manuellen Praxis regelmäßig an Ressourcen- und Skalierungsgrenzen scheitert. Die im Projekt entwickelte

Architektur zeigt, dass eine technisch belastbare, revisionsfreundliche Umsetzung dieses Ansatzes möglich ist.

Rechtlich lassen sich drei zentrale Erkenntnislinien festhalten:

1. **Datenschutzrechtlich** trägt ein phasenbezogener Zuschnitt: In der Entwicklungsphase lässt sich der Einsatz realer personenbezogener Daten weitgehend vermeiden; Anonymisierung bzw. Nutzung synthetischer Daten kann hier Standard sein, nicht Ausnahme. In der Anwendungsphase rückt demgegenüber die konkrete Ausgestaltung einzelner Verarbeitungsschritte in den Vordergrund – insbesondere beim Einlesen von Unterlassungserklärungen, beim Crawling und Scraping und bei der KI-gestützten Bewertung. Die Analyse zeigt, dass sich diese Vorgänge – bei strenger Datenminimierung und technischer Abschottung – in den bekannten Kategorien der DSGVO verorten lassen, ohne neue dogmatische Brüche zu erzeugen. Art. 22 DSGVO wird durch das vorgesehene Entscheidungsmodell (KI-gestützte Voranalyse, menschliche Letztentscheidung) regelmäßig nicht eröffnet.
2. **Urheberrechtlich** ist das Projekt keine „Grauzone auf Vorrat“, sondern lässt sich entlang der bestehenden Schrankenstruktur verorten. § 44b UrhG erweist sich als zentrale Norm für das Text- und Data-Mining-Element des Systems, setzt aber ein ernst zu nehmendes Löschoption und Opt-out-Management voraus. Für die eigentliche Beweisführung kommen § 45 Abs. 1 UrhG und – in Einzelfällen – vertragliche Erlaubnisse in Betracht. Praktisch bedeutsam ist zudem, dass technische Schutzmaßnahmen und Nutzungsvorbehalte nicht als bloßes „Störgeräusch“ des Systems begriffen werden dürfen, sondern systemseitig als harte Stopps zu behandeln sind. Die rechtliche Bewertung zeigt: KIVEDU ist urheberrechtlich nicht grenzenlos einsetzbar, aber gestaltbar einbettbar, wenn diese Begrenzungen zum Ausgangspunkt der technischen Konzeption gemacht werden.
3. **Im Lichte der KI-Verordnung** bewegt sich KIVEDU in einem von der KI-VO erfassten, aber nicht hochregulierten Segment. Das System fällt in den Anwendungsbereich der Verordnung, ohne nach der derzeitigen Ausgestaltung als Hochrisiko-System einzuordnen zu sein. Die KI-VO verlangt daher keine eigene „Regulierungsarchitektur“ neben Datenschutz- und Urheberrecht, sondern ergänzt diese vor allem um Anforderungen an Nachvollziehbarkeit, Dokumentation und Kompetenzen derjenigen, die das System anwenden. Für mögliche Nutzungsadressaten wie Verbraucherorganisationen bedeutet das: Die Einführung eines Systems wie KIVEDU bleibt auch aus KI-rechtlicher Sicht handhabbar, benötigt aber eine klare Zuweisung von Verantwortlichkeiten, Dokumentationsroutinen und Schulungsstrukturen.

Für die Praxis der Verbraucherdurchsetzung lässt sich daraus folgern: Ein KI-gestütztes Monitoring von Unterlassungspflichten ist nicht nur technisch machbar, sondern rechtlich in die bestehenden Strukturen einbindbar – allerdings um den Preis einer bewussten, transparenten Begrenzung dessen, was das System

⁵⁰ Schwenke DB 2024, 205 (205).

⁵¹ Schwenke DB 2024, 205 (208).

⁵² Hierzu Schuster/Waidelich/Falk/Schneider/Lambert, Risk Classification and Compliance of AI Systems under the EU AI Act, AMCIS 20025 Proceedings. 17.

tun darf. Gerade darin liegt sein Potenzial: Es kann Organisationen bei ihrer Arbeit in der (Verbraucher-)Rechtsdurchsetzung in die Lage versetzen, bekannte Instrumente der Abmahnung und

Unterlassungserklärung in einem digitalen Marktumfeld wirkungsvoller zu nutzen, ohne die grundlegende Rollenverteilung zwischen Technik und juristischer Bewertung umzukehren.

Entwicklungen im europäischen Passagierrecht 2025-2026

Von Jasmin Reininger, Wien*

Von März 2025 bis Mai 2026 ergingen sechs Entscheidungen zur Fluggastrechte-VO, eine Entscheidung zur EuGVVO im Zusammenhang mit der Abtretung von Ansprüchen aus einem Luftbeförderungsvertrag sowie zwei Entscheidungen zum Übereinkommen von Montreal. Die Revision der Fluggastrechte-VO hat im Berichtszeitraum Fahrt aufgenommen und steht zum Ende des Berichtszeitraums im Stadium des Vermittlungsverfahrens.¹

I. Entwicklungen im Passagierrecht auf EU-Ebene

Zu den im vorangegangenen Beitrag² erwähnten Vorschlägen für eine Verordnung über Fahr- bzw. Fluggastrechte im Zusammenhang mit multimodalen Reisen³ sowie für eine Verordnung zur Änderung der Verordnungen Nr. 261/2004, Nr. 1107/2006, Nr. 1177/2010, Nr. 181/2011, Nr. 2021/782 in Bezug auf die Durchsetzung der Fahr- und Fluggastrechte in der Union⁴ läuft noch das ordentliche Gesetzgebungsverfahren; zum Ende des Berichtszeitraums dauerten die Trilogverhandlungen zu diesen beiden Dossiers noch an.⁵

Betreffend den Vorschlag zur Änderung der Verordnung 261/2004 und der Verordnung Nr. 2027/97⁶, der bereits seit März 2013 auf dem Tisch liegt, veröffentlichte der Rat am 2.10.2025 seinen Standpunkt.⁷ Im Jänner 2026 fand die Abstimmung im zuständigen Ausschuss des Europäischen Parlaments statt, in der Zweiten Lesung wurden am 21.1.2026 Änderungsanträge zur Ratsposition angenommen. Die Europäische Kommission gab am 12.3.2026 eine Stellungnahme zu den Parlamentsänderungen ab.⁸ Am 24.3.2026 lehnte der Rat der Europäischen Union die Parlamentsänderungen ab. Strittige Punkte betreffen u.a. die Höhe der Ausgleichszahlungen, die Schwellenwerte bei Verspätungen sowie die Definition der außergewöhnlichen Umstände. Somit wurde das Vermittlungsverfahren nach Art 294 AEUV eingeleitet. Am 20.4.2026 hat die formelle Sitzung des Vermittlungsausschusses begonnen und zum Ende des Berichtszeitraums, Mai 2026 noch angedauert.

II. Flugpassagierrechte

1. Fluggastrechte-VO vor dem EuGH

Von März 2025 bis Mai 2026 entschied der EuGH in sechs Rechtssachen zur Fluggastrechte-VO⁹. Die Entscheidungen werden in der Folge thematisch abgehandelt.

a) *Bordkarte für Flug im Rahmen einer Pauschalreise als bestätigte Buchung.* Mit Urteil vom 6.3.2025 entschied der EuGH in

der Rechtssache C-20/24 – Cymdek.¹⁰ Im Ausgangssachverhalt schloss ein Luftfahrtunternehmen als Anbieter von Charterflügen einen Vertrag mit einem Reiseunternehmen ab, aufgrund dessen dieses Luftfahrtunternehmen Flüge für das Reiseunternehmen durchführte, für die das Reiseunternehmen Flugscheine an Fluggäste verkaufte. Das Reiseunternehmen zahlte dabei das Entgelt für die Flüge an das Luftfahrtunternehmen. Im gegenseitigen Sachverhalt hatte ein im Rahmen einer Pauschalreise gebuchter Flug eine große Ankunftsverspätung, für die eine Ausgleichsleistung begehrt wurde. Der zugrunde liegende Pauschalreisevertrag wurde zwischen dem erwähnten Reiseunternehmen und einem dritten Unternehmen zugunsten der Fluggäste abgeschlossen. Die betroffenen Fluggäste konnten lediglich Bordkarten vorweisen; das Luftfahrtunternehmen verweigerte in der Folge mangels Nachweises über eine bestätigte und bezahlte Buchung die Zahlung der Ausgleichsleistung. Das vorlegende Gericht wollte nun geprüft wissen, ob es sich bei der Bordkarte um einen anderen Beleg im Sinne des Art. 2 lit. g der Fluggastrechte-VO handelt, wonach die Buchung akzeptiert und registriert wurde und ob die Fluggäste damit im Sinne des Art. 3 Abs. 2 der Fluggastrechte-VO über eine bestätigte Buchung für den betreffenden Flug verfügten. Schließlich stellte das vorlegende Gericht die Frage, ob der Flug gemäß Art. 3 Abs. 3 der Fluggastrechte-VO als entgeltlich zu betrachten ist, wenn der Fluggast eine Pauschalreise beim Reiseunternehmen erworben hat, welches dem Luftfahrtunternehmen den Flug bezahlt hat sowie ob die Fluggäste zu einem reduzierten Tarif reisen.

Die ersten beiden Fragen zum Begriff der „Buchung“ sowie zur Auslegung des Art. 3 Abs. 2 lit. a der Fluggastrechte-VO im Hinblick auf das Vorliegen einer „bestätigten Buchung“ behandelte der EuGH in einem. Er führte dazu aus, dass der Begriff

* Mag. Jasmin Reininger ist Mitarbeiterin der Abteilung Konsumentenpolitik der Arbeiterkammer Wien.

1 Hinweis der Redaktion: Das Vermittlungsverfahren über eine neue Fluggastrechte-VO wurde inzwischen erfolgreich abgeschlossen. Bei Redaktionsschluss dieses Heftes fehlte lediglich noch die formelle Zustimmung von Rat und Parlament sowie die Veröffentlichung im Amtsblatt.

2 Reininger VuR 2025, 250.

3 COM(2023) 752 final.

4 COM(2023) 753 final.

5 Siehe EUR-Lex – 52023PC0753 – DE – EUR-Lex (abgerufen am 19.6.2026).

6 COM(2013) 130 final.

7 Siehe Search in the register – Consilium (abgerufen am 19.6.2026).

8 COM(2026) 129.

9 ABL 2004 L 46, 1; im Folgenden Fluggastrechte-VO.

10 EuGH 6.3.2025 – C-20/24, ECLI:EU:C:2025:139 – Cymdek.