Erkenntnisse zur Verbesserung von Datenschutz in Plattformökonomien: Transparenz, Intervenierbarkeit und User Experience im Fokus

Lennart Kiss, Rachelle Sellung, Björn Hanneke und Lorenz Baum

Zusammenfassung
Transparenz und Intervenierbarkeit sind zentrale Prinzipien der DSGVO, doch ihre praktische Umsetzung bleibt herausfordernd. In diesem Beitrag wird untersucht, wie Datenschutz durch gezielte Gestaltung von technischen Hilfssystemen in Plattformökonomien effektiver gestaltet werden kann, um Nutzerrechte verständlich und anwendbar zu machen. Dieses Ziel wird fortlaufend als Datenschutzinitiative bezeichnet. Im Rahmen des PERISCOPE-Projekts wurden interdisziplinäre Methoden aus User Experience, Recht und Ökonomie kombiniert, um Datenschutzmaßnahmen aus verschiedenen Perspektiven zu bewerten. Empirische Studien mit Endnutzern und Plattformbetreibern zeigen, dass bestehende Datenschutzlösungen oft schwer verständlich sind und Nutzerrechte durch komplexe Prozesse eingeschränkt werden. Die Forschung hebt hervor, dass eine transparente Kommunikation, nutzerfreundliche Gestaltung und gezielte Interaktivität entscheidend für die Akzeptanz und Wirksamkeit von Datenschutzinitiativen sind. Zudem werden wirtschaftliche Faktoren analysiert, die Unternehmen zur Implementierung datenschutzfreundlicher Modelle motivieren können. Dieser Beitrag leitet konkrete Handlungsempfehlungen für die Weiterentwicklung nutzerzentrierter Datenschutzstrategien ab und betont die Notwendigkeit einer ganzheitlichen Integration von Regulierung, Technologie und Nutzererwartungen.

1. Einleitung: User Experience und Datenschutz

Datenschutz ist zu einem zentralen Anliegen von Nutzenden, Unternehmen und Gesetzgebern geworden. Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union setzt mit ihren Anforderungen an Transparenz und Intervenierbarkeit wesentliche Standards für einen nutzerfreundlichen Datenschutz. Trotz der formalen Vorteile dieser Grundsätze bleibt ihre praktische Umsetzung eine Herausforderung. Dieser Beitrag stammt aus der Forschung des vom Bundesministerium für Bildung und Forschung, Technologie und Raumfahrt geförderten PERISCOPE-Projekts[1], das datenschutzfreundliche Lösungen für kleine und mittelständische Unternehmen (KMUs) entwickelte.

1 Die Forschung des PERISCOPE-Projekts wurde vom Bundesministerium für Bildung und Forschung, Technologie und Raumfahrt gefördert. https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/periscope.

Zwei der wichtigsten Ergebnisse des PERISCOPE-Projekts sind ein Privacy Friendly Business Model Recommender Tool[2] und ein Personal Rights Management System.

Das Privacy Friendly Business Model Recommender Tool von PERISCOPE wurde entwickelt, durch Forschung validiert und im PERISCOPE-Projekt implementiert. Ziel dieses Demonstrators ist es, Geschäftsmodelle von Plattformanbietern mit einem Privacy-Score zu bewerten und Verbesserungsvorschläge zu liefern. Dieses Tool hilft, die Privatssphärenfreundlichkeit von Geschäftsmodellen zu messen und zu vergleichen und quantifiziert das Engagement für Privatsphäre in Geschäftsmodellen. Die Methodik dieser Anwendung ist durch verschiedene Studien des Projekts validiert[3]. Darüber hinaus entwickelte PERISCOPE ein Personal Rights Management System als Demonstrator, das sowohl für den Plattformanbieter als auch für den Verbraucher konzipiert wurde. Das Tool kann genutzt werden, um den Nutzern mehr Transparenz über ihre Datennutzung und Möglichkeiten zur Intervenierbarkeit zu bieten, sowie um die Bearbeitung der ausgeübten Betroffenenrechte für die Plattformbetreiber zu erleichtern. Die Ergebnisse des PERISCOPE-Projekts sind auf der Projektwebsite veröffentlicht[4]. Die Entwicklung des Demonstrators basiert auf den verschiedenen Zwischenergebnissen und der Forschung des Projekts[5].

Durch einen interdisziplinären Forschungsansatz untersucht die Studie, wie Datenschutzinitiativen aus der Sicht von User Experience, dem Recht und der Ökonomie verbessert werden können. Die Ergebnisse dieser Untersuchung liefern Erkenntnisse für die Gestaltung effektiver Datenschutzmaßnahmen und präsentieren konkrete Implikationen zur Weiterentwicklung datenschutzfreundlicher Technologien.

---

2 https://privacy.wiim-research.de

3 *Hanneke/Baum/Schnuck/Hinz*, DuD 2024; Tool siehe https://aisel.aisnet.org/icis2024/security/security/3/.

4 Für die Ergebnisse des PERISCOPE Projekts siehe: https://websites.fraunhofer.de/periscope-projekt/?page_id=490 (zuletzt abgerufen am 23.05.2025).

5 Näher *Hanneke/Baum/Schlereth/Hinz*, ICIS 2023.; *Hanneke/Baum/Hinz*, ECIS 2023.; *Astfalk/Schunck*, LNI, Open Identity Summit 2023.; *Pfeiffer/Astfalk/Baum/Haneke/Schunck/Winterstetter*, in: Friedewald u.a. (Hrsg.), Daten-Fairness in einer globalisierten Welt, Nomos, 2023, S. 117–144.; *Pfeiffer*, Datenzugang in der Plattformökonomie: *Regulierungsinstrumente in P2B-VO, DMA und DSA*, in: Buchheim u.a. (Hrsg.), Plattformen. Grundlagen und Neuordnung des Rechts digitaler Plattformen, 2024, S. 53–76.; *Schmitt/Schunck/Lo Iacono*, Ökosysteme – Neue Herausforderungen für den Datenschutz, 2024.; *Pfeiffer*, in: Augsberg u.a. (Hrsg.), Datenzugangsregeln. Zwischen Freigabe und Kontrolle, 2024, S. 101–136.

Diese Forschungsarbeit umfasste mehrere Studien mit einer diversifizierten Nutzergruppe, darunter Tiefeninterviews, Usability-Tests und quantitative Online-Umfragen mit realen Anwendern. Die Teilnehmer repräsentierten verschiedene demografische Gruppen, um unterschiedliche Perspektiven zu gewährleisten. Das Projekt konzentrierte sich auf mehrere Schlüsselaspekte, die durch die Studien untersucht werden sollten. Als erstes wurde die (1) Wahrnehmung von Betroffenenrechten untersucht, also wie Endnutzer, die ihnen durch die DSGVO gewährten Rechte wahrnehmen und verstehen. Ein weiteres zentrales Thema war (2) die Transparenz der Plattformen und Intervenierbarkeit durch Endnutzer. Es wurde die Rolle von Transparenz bei der Vermittlung von Datenschutzinformationen und dessen Einfluss auf die Nutzererfahrung untersucht. Darüber hinaus wollten wir herausfinden, wie einfach es für Nutzer ist, ihre Rechte durchzusetzen und in Datenschutzprozesse einzugreifen. Schließlich betrachteten wir auch (3) die Perspektive weiterer Stakeholder, insbesondere die Sichtweisen der Plattformbetreiber auf Datenschutz und ihre Bereitschaft, Lösungen zu adaptieren, bei denen Transparenz und Intervenierbarkeit im Vordergrund stehen.

Im Folgenden werden die Erkenntnisse aus den verschiedenen Studien, Anforderungsdefinitionen und Bewertungen sowie die Erkenntnisse aus den Demonstrationsumsetzungen des PERISCOPE-Projekts dargelegt und reflektiert. Die nachfolgenden Abschnitt stellen die zentralen Ergebnisse dieser Untersuchungen dar: Abschnitt 2 eröffnet mit einem theoretischen Hintergrund zu den Aspekten der Transparenz und Intervenierbarkeit, Abschnitt 3 erläutert das Forschungsdesign und die durchgeführten Studien, Abschnitt 4 präsentiert interdisziplinäre Erkenntnisse aus der Perspektive der User Experience (UX), des Rechts und der Ökonomie, Abschnitt 5 leitet konkrete Implikationen für die Gestaltung künftiger Datenschutzinitiativen ab, Abschnitt 6 diskutiert die Limitationen der Forschung sowie potenzielle zukünftige Forschungsansätze, und Abschnitt 7 fasst die zentralen Erkenntnisse zusammen und zieht ein abschließendes Fazit.

2. Theoretischer Hintergrund: Transparenz und Intervenierbarkeit als Schlüssel für nutzerfreundlichen Datenschutz

Transparenz und Intervenierbarkeit werden allgemein als wesentliche Bestandteile eines nutzerzentrierten Datenschutzes anerkannt, doch ihre

praktische Umsetzung ist nach wie vor mit Herausforderungen verbunden. Zwar sind Transparenz (Art. 5 Abs. 1 lit. a DSGVO) und Intervenierbarkeit (Art. 15–21 DSGVO) in der Datenschutz-Grundverordnung formell verankert, doch ist es alles andere als einfach, sicherzustellen, dass diese Rechte zu einer wirkungsvollen Kontrolle für die Betroffenen führen. Verantwortliche sind verpflichtet, Informationen in „präziser, transparenter, verständlicher und leicht zugänglicher Form" bereitzustellen (Art. 12 Abs. 1 DSGVO), aber in der Praxis bleiben Datenschutzhinweise schwer verständlich,[6] Einwilligungsmechanismen beruhen oft auf sogenannten „Dark Patterns"[7] und das Volumen der Datentransaktionen erschwert die Übersicht für die Betroffenen.

Die Möglichkeit der Intervention ist nicht nur eine Frage der gesetzlichen Rechte, sondern auch der technischen Machbarkeit. Während die DSGVO das Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) und Datenübertragung (Art. 20 DSGVO) vorschreibt, haben viele Organisationen mit fragmentierten Datenarchitekturen und Altsystemen zu kämpfen, die eine rasche Umsetzung dieser Rechte erschweren.[8] Plattformen verarbeiten große Mengen an Benutzerdaten in Echtzeit, und die Beantwortung von Anfragen innerhalb der vorgeschriebenen einmonatigen Frist (Art. 12 Abs. 3 DSGVO) kann logistisch anspruchsvoll sein. Darüber hinaus ist die Wirksamkeit der Intervenierbarkeit begrenzt, wenn datengesteuerte Geschäftsmodelle auf personenbezogene Daten als Kernbestandteil angewiesen sind. Einige Verantwortliche schrecken auf subtile Weise Nutzer von Löschanfragen ab, indem sie bewusst Reibungspunkte einführen – mehrstufige Prozesse, Verzögerungen oder unvollständige Datenlöschungen –, was Bedenken aufwirft, ob die Datenschutz-Grundverordnung immer wirksam ausgeübt wird.

Über die Einhaltung von Vorschriften hinaus erschwert die sich entwickelnde technologische und rechtliche Landschaft diese Grundsätze zusätzlich. Automatisierte Personalisierung, algorithmische Entscheidungsfindung und Echtzeit-Datenhandel stellen traditionelle Vorstellungen von Transparenz und Benutzerkontrolle in Frage. Regulierungsbehörden und

6 *Tesfay* u.a., Privacy Guide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation, 2018, S. 15-21.

7 *Nouwens* u.a., in ACM (Hrsg.), Proceedings of the CHI Conference on Human Factors in Computing Systems, 2020, 1–13.

8 *Shah* u.a., in USENIX (Hrsg.), Proceedings des 11th Workshop on Hot Topics in Storage and File Systems (HotStorage), 2019.

Wissenschaftler setzen sich zunehmend für Technologien zur Verbesserung der Transparenz (*Transparency enhancing Technologies*, TETs) und automatisierte Datenschutz-Tools ein, aber die Akzeptanz dieser Lösungen ist uneinheitlich, insbesondere bei KMU, denen die Ressourcen für robuste Compliance-Infrastrukturen fehlen.[9]

Daher geht es nicht mehr primär darum, ob Transparenz und Intervenierbarkeit gesetzlich verankert sind, sondern vielmehr darum, wie sichergestellt werden kann, dass sie in einer zunehmend komplexen, datengesteuerten Ökonomie wirkungsvoll umgesetzt werden. Die Diskrepanz zwischen rechtlichen Vorgaben und praktischer Umsetzung wirft zentrale Fragen auf: Sind Nutzer tatsächlich in der Lage, informierte Entscheidungen zu treffen, oder führen Transparenzpflichten lediglich zu einer Flut juristischer Offenlegungen? Lässt sich Intervenierbarkeit in einem Umfeld effektiv skalieren, in dem personenbezogene Daten kontinuierlich verarbeitet, analysiert und weitergegeben werden? Um diesen Herausforderungen zu begegnen, bedarf es nicht nur einer konsequenten Durchsetzung regulatorischer Anforderungen, sondern auch technologischer Innovationen und bewährter branchenweiter Ansätze, die nicht nur dem Wortlaut, sondern auch dem Geist der DSGVO gerecht werden.

3. Forschungsdesign: Nutzererfahrungen mit Datenschutz-Tools

Dieser Beitrag untersucht, wie verschiedene Stakeholdergruppen das PERISCOPE-System wahrnehmen und nutzen. Um ein umfassendes Verständnis über die Nutzererfahrungen mit Datenschutz-Tools zu gewinnen, wurden verschiedene empirische Untersuchungen durchgeführt. Dabei lag der Fokus insbesondere auf den Aspekten Transparenz, Intervenierbarkeit und User Experience. Ziel war es, herauszufinden, wie unterschiedliche Stakeholder das Tool wahrnehmen, welche Herausforderungen sie bei der Ausübung von Betroffenenrechten erleben und inwiefern entworfene Lösungen ihre Erwartungen erfüllen. Die erhobenen Daten liefern Erkenntnisse über multidisziplinäre Aspekte solcher Initiativen, insbesondere im Hinblick auf die User Experience, rechtliche Rahmenbedingungen und ökonomische Einflussfaktoren.

Um verschiedene Perspektiven auf Datenschutzinitiativen zu erfassen, wurde ein Methodenmix eingesetzt, der qualitative und quantitative An-

9 *Kergroach*, SMEs Going Digital, 2021.

sätze kombiniert. Die Endnutzerperspektive wurde durch Usability-Tests und eine Online-Umfrage untersucht, während die Sichtweise der Stakeholdergruppe der Plattformbetreiber anhand qualitativer Tiefeninterviews erfasst wurde. Durch diese methodische Herangehensweise konnten sowohl praktische Nutzungshürden als auch strategische Herausforderungen bei der Implementierung und Anwendung des PERISCOPE-Tools identifiziert werden.

Die Usability-Tests wurden mit Endnutzern des PERISCOPE-Tools durchgeführt, um deren Interaktion mit dem System systematisch zu analysieren. Im Rahmen dieser Tests wurden Fragen zur Wahrnehmung von Datenschutzpräferenzen, zu auftretenden Hürden sowie zur empfundenen Schwierigkeit einzelner Testaufgaben gestellt. Zusätzlich kamen standardisierte Messinstrumente wie die System Usability Scale und das User Experience Questionnaire zum Einsatz, um die Benutzerfreundlichkeit und Nutzererfahrung des Systems in einem vergleichbaren Rahmen zu bewerten. Zusätzlich wurde die allgemeine Zufriedenheit der Teilnehmenden untersucht, insbesondere im Hinblick auf die Erfüllung ihrer Erwartungen an die Funktionen des Tools, mögliche Verbesserungsvorschläge sowie potenzielle Anwendungsgebiete.

Die Perspektive der Plattformbetreiber wurde durch leitfadengestützte Tiefeninterviews erfasst, die sich an dem Design-Science-Ansatz orientierten. In diesem Zusammenhang diente das PERISCOPE-System als Artefakt, um spezifische Herausforderungen und Anforderungen an Datenschutzinitiativen aus Sicht der Betreiber zu identifizieren. Der Fokus lag auf Erfahrungen mit der Umsetzung von Transparenz- und Intervenierbarkeitsfunktionen, auf strategischen Überlegungen zur Einführung solcher Maßnahmen sowie auf Hürden bei der praktischen Umsetzung. Die Interviews wurden inhaltsanalytisch nach den Prinzipien von Mayring[10] ausgewertet, um wiederkehrende Themen, Herausforderungen und Potenziale systematisch zu erfassen.

Ergänzend wurde eine Online-Umfrage mit realen Nutzern des PERISCOPE-Projektpartners Gohobi, ein Onlineplattformbetreiber, durchgeführt. Diese Untersuchung zielte darauf ab, allgemeine Wahrnehmungen und Nutzungsgewohnheiten im Umgang mit Datenschutzinitiativen zu erfassen. Die Teilnehmenden bewerteten ihre ersten Eindrücke in Bezug auf die Benutzerfreundlichkeit des Tools und gaben Auskunft über ihre persönlichen Datenschutzpräferenzen und ihr generelles Verhalten im Umgang

10 *Mayring*, Qualitative Content Analysis, 2021.

mit Datenschutzoptionen. Darüber hinaus wurde untersucht, inwiefern sie mit Betroffenenrechten vertraut sind und in welchem Maße sie diese in Anspruch nehmen. Zusätzlich wurde erfasst, ob die Teilnehmer bereit wären, eine datenschutzfreundliche Plattform aktiv weiterzuempfehlen und inwiefern das Vertrauen in die Plattform durch Transparenz- und Intervenierbarkeitsfunktionen beeinflusst wird. Abschließend wurde ein allgemeines Feedback zur Nutzung des Systems eingeholt, um weiterführende Erkenntnisse zur praktischen Anwendbarkeit zu gewinnen.

Durch die Kombination dieser methodischen Ansätze konnte eine fundierte Grundlage für die Analyse der Nutzererfahrungen mehrerer Stakeholdergruppen mit Datenschutzinitiativen geschaffen werden. Während die Usability-Tests praxisnahe Nutzungshürden offenlegten, ermöglichten die Tiefeninterviews eine differenzierte Betrachtung der Herausforderungen und Strategien der Plattformbetreiber. Die Online-Umfrage diente dazu, diese hauptsächlich qualitativen Erkenntnisse durch eine größere empirische Basis zu ergänzen.

4. Erkenntnisse aus der Nutzerforschung

Die empirischen Untersuchungen im Rahmen des PERISCOPE-Projekts liefern praktische Erkenntnisse darüber, wie verschiedene Nutzergruppen Datenschutzinitiativen wahrnehmen und welche Faktoren deren Akzeptanz und Nutzung beeinflussen. Dabei zeigte sich, dass Datenschutz nicht nur aus technischer oder regulatorischer Sicht betrachtet werden kann, sondern entscheidend davon abhängt, wie verständlich, zugänglich und anwendungsfreundlich entsprechende Maßnahmen gestaltet sind. Die Forschungsergebnisse verdeutlichen, dass insbesondere die User Experience, die rechtlichen Rahmenbedingungen, sowie die wirtschaftlichen Implikationen eine wesentliche Rolle für die erfolgreiche Umsetzung datenschutzfreundlicher Technologien spielen. Die folgenden Abschnitte beleuchten die zentralen Erkenntnisse aus diesen drei Perspektiven.

4.1 User Experience Erkenntnisse

Die Studien zur Nutzung des PERISCOPE-Systems verdeutlichen zentrale Herausforderungen und Gestaltungsmöglichkeiten für eine verbesserte User Experience im Kontext von Datenschutzinitiativen. Die Studien in

diesem Abschnitt basieren auf den Erkenntnissen aus mehreren Runden von User Experience-Tests, die mit einem Mix aus Methoden durchgeführt wurden, sowie auf Interviews mit Plattformanbietern und einer Umfrage unter Endnutzern. Insbesondere wurden vier Schlüsselfaktoren identifiziert, die maßgeblich zur Benutzerfreundlichkeit und Nutzererfahrung von Datenschutztools beitragen: unmittelbares Feedback und Unterstützung, Reduktion von Komplexität, visuelle Hilfsmittel und interaktive Elemente zur Förderung der Nutzerkontrolle.

4.1.1 Unmittelbares Feedback und Unterstützung

Die Analyse der Nutzerinteraktion mit dem PERISCOPE-System zeigte, dass eine fehlende Rückmeldung während der Nutzung erhebliche Unsicherheiten hervorrufen kann, insbesondere wenn es um die Wahrnehmung und Ausübung von Betroffenenrechten geht. Nutzer benötigen eine unmittelbare Bestätigung darüber, ob ihre Anfragen oder Teilschritte der Prozesse erfolgreich waren oder welche weiteren Schritte erforderlich sind, um ihre Datenschutzanliegen effektiv zu verfolgen. Unklare oder ausbleibende Rückmeldungen können zu Frustration und im schlimmsten Fall zu einem Vertrauensverlust gegenüber dem Tool führen.

Ein Ansatz zur Verbesserung der Nutzererfahrung ist die Bereitstellung von Echtzeit-Feedback, welches den Nutzern signalisiert, ob ihre Datenschutzanfragen – beispielsweise eine Datenlöschung – erfolgreich bearbeitet wurden oder ob noch weitere Aktionen erforderlich sind. Darüber hinaus können kontextbezogene Anleitungen und Tutorials integriert werden, die Nutzern schrittweise erklären, wie sie ihre Betroffenenrechte durchsetzen können. Diese Art der Unterstützung erweist sich insbesondere für weniger rechtsaffine Nutzer als essenziell, da sie eine strukturierte und verständliche Hilfestellung für komplexe Datenschutzprozesse bietet.

Neben automatisierten Hilfestellungen zeigte sich in den Untersuchungen auch, dass Nutzer in bestimmten Fällen auf direkte menschliche Unterstützung angewiesen sind. Wenn Echtzeit-Feedback und Tutorials nicht ausreichen, können persönliche Support-Optionen dabei helfen, individuelle oder komplexe Probleme effizient zu lösen. Die Möglichkeit, eine direkte Ansprechperson zu konsultieren, beeinflusst die Ausübbarkeit von Betroffenenrechten positiv.

4.1.2 Reduktion von Komplexität

Ein zentrales Ergebnis der Nutzerforschung ist, dass die Verständlichkeit von Datenschutztools maßgeblich darüber entscheidet, ob und in welchem Umfang Nutzer ihre Betroffenenrechte wahrnehmen. Die Komplexität rechtlicher und technischer Sachverhalte stellt eine signifikante Barriere dar, die dazu führt, dass Nutzer Datenschutzoptionen nur eingeschränkt oder gar nicht nutzen. Besonders problematisch ist der häufige Einsatz juristischer Fachterminologie, die für viele Nutzer schwer zugänglich ist.

Die Reduktion von Komplexität erfordert jedoch mehr als nur eine Vereinfachung von Begrifflichkeiten. Vielmehr sollte die gesamte Sprach- und Interaktionsgestaltung eines Datenschutztools darauf ausgerichtet sein, eine intuitive Nutzung zu ermöglichen. Dies umfasst die Verwendung eines verständlichen Vokabulars sowie einer klaren und strukturierten Informationsaufbereitung, die es auch weniger datenschutzaffinen Nutzern erleichtert, ihre Rechte durchzusetzen. Die Herausforderung besteht darin, eine Balance zu finden: Während die Inhalte zugänglich und verständlich sein müssen, dürfen essenzielle rechtliche und technische Details nicht verloren gehen.

Die Ergebnisse zeigen, dass eine gezielte sprachliche Vereinfachung nicht nur zu einer erhöhten Nutzerfreundlichkeit führt, sondern auch die allgemeine Akzeptanz von Datenschutzinitiativen steigert. Eine benutzerzentrierte Gestaltung der Informationsvermittlung trägt dazu bei, dass Datenschutztools als verständlich, zugänglich und somit als verlässlich wahrgenommen werden. Besteht diese Hürde weiterhin, kann nicht von informierten Entscheidungen der Nutzer ausgegangen werden.

4.1.3 Visuelle Unterstützung als Vermittlungsstrategie

Visuelle Darstellungen spielen eine wesentliche Rolle bei der Vermittlung komplexer Datenschutzinhalte. Die Studien zeigten, dass Nutzer von Infografiken, Schritt-für-Schritt-Anleitungen und weiteren visuellen Hilfsmitteln profitieren, da diese abstrakte Datenschutzkonzepte in einer leicht verständlichen Weise präsentieren. Besonders bei der Entscheidungsfindung, beispielsweise zur Ausübung eines Betroffenenrechts, erweisen sich visuelle Elemente als hilfreich, da sie strukturierte Orientierung bieten und so die kognitive Belastung der Nutzer reduzieren.

Der Einsatz von Diagrammen, Icons und interaktiven Visualisierungen kann dazu beitragen, dass Nutzer schneller erfassen, welche Datenschutz-

optionen ihnen zur Verfügung stehen und welche Konsequenzen ihre Entscheidungen haben. Durch die Reduktion textlastiger Erklärungen und die gezielte Einbindung visueller Unterstützung wird das System insgesamt benutzerfreundlicher und zugänglicher.

4.1.4 Interaktive Elemente zur Förderung der Nutzerkontrolle

Interaktivität stellt einen weiteren zentralen Faktor für eine positive Nutzererfahrung im Bereich datenschutzfreundlicher Technologien dar. Nutzer müssen das Gefühl haben, aktiv in die Verwaltung ihrer Daten eingebunden zu sein, um Vertrauen in die Funktionsweise des Systems zu entwickeln. Die Untersuchungsergebnisse zeigen, dass interaktive Funktionen wie eine dynamische Einwilligungsmanagementkomponente oder ein dialogbasierter Assistent maßgeblich dazu beitragen, dass Nutzer sich als souveräne Akteure im Datenschutzprozess wahrnehmen.

Im konkreten Fall des PERISCOPE-Systems wurde eine Chatbot-ähnliche Struktur implementiert, die Nutzern eine schrittweise Unterstützung bei der Durchsetzung ihrer Betroffenenrechte bietet. Durch diesen interaktiven Ansatz erhalten Nutzer eine gezielte Anleitung und können ihre Entscheidungen zur Datennutzung in Echtzeit anpassen. Die Möglichkeit, direkt Einfluss auf die eigenen Daten zu nehmen, förderte das Gefühl der Eigenverantwortung und zu Teilen die Motivation sich der Datenschutzthematik anzunehmen. Nutzer, die aktiv in den Datenschutzprozess eingebunden sind, zeigen eine höhere Bereitschaft, Datenschutzinitiativen nachhaltig zu nutzen und weiterzuempfehlen.

4.1.5 Zusammenfassung der User Experience Erkenntnisse

Zusammenfassend ist zu sagen, dass die Gestaltung der User Experience maßgeblich über die Akzeptanz und Wirksamkeit von Datenschutzinitiativen entscheidet. Vier zentrale Faktoren wurden als besonders relevant identifiziert: Die Bereitstellung von unmittelbarem Feedback in Form von Echtzeit-Rückmeldungen, Tutorials oder direktem Support steigert die Nutzerzufriedenheit und reduziert Unsicherheiten. Die Reduktion von Komplexität durch eine verständliche Sprache und eine intuitive Struktur senkt Nutzungshürden und fördert eine breitere Akzeptanz. Visuelle Unterstützung erleichtert die Informationsaufnahme und steigert die Effizienz bei der Entscheidungsfindung. Schließlich fördern interaktive Elemente das

Gefühl der Kontrolle und Eigenverantwortung der Nutzer, wodurch Datenschutzinitiativen als transparenter und vertrauenswürdiger wahrgenommen werden.

4.2 Rechtliche Erkenntnisse

Die rechtlichen Analysen im Rahmen des PERISCOPE-Projekts haben zentrale Herausforderungen bei der Umsetzung datenschutzrechtlicher Anforderungen innerhalb einer technischen Datenschutzinitiative offenbart. Besonders deutlich wurde, dass die späte Integration rechtlicher Vorgaben in technische Systeme zu unnötigen Anpassungskosten und ineffizienten Implementierungsprozessen führen kann. Im Fall des PERISCOPE-Projekts wurde hingegen ein Ansatz verfolgt, bei dem von Beginn an eine rechtskonforme Gestaltung im Fokus stand. Ziel war es, Plattformbetreibern, insbesondere kleinen und mittelständischen Unternehmen, ein System bereitzustellen, das sie bei der Einhaltung relevanter datenschutzrechtlicher Verpflichtungen unterstützt.

4.2.1 Fokus auf relevante rechtliche Anforderungen

Ein zentraler Aspekt bei der Entwicklung von Datenschutzinitiativen ist die frühzeitige und präzise Definition rechtlicher Anforderungen, um sicherzustellen, dass diese nicht nur theoretisch, sondern auch praktisch relevant sind. Erfahrungen aus dem PERISCOPE-Projekt zeigen, dass viele anfänglich formulierte rechtliche Vorgaben im späteren Verlauf keine unmittelbare Umsetzung erforderten oder sich als überflüssig erwiesen. Um ineffizienten Mehraufwand zu vermeiden, ist es daher essenziell, bereits zu Beginn eines Projekts einen gezielten Fokus auf diejenigen rechtlichen Anforderungen zu legen, die für die praktische Implementierung tatsächlich von Bedeutung sind. Dies betraf beispielsweise spezifische Vorgaben zur Einwilligung von Minderjährigen gemäß Art. 8 DSGVO oder regulatorische Anforderungen aus der Platform-to-Business-Verordnung und dem Digital Services Act. Eine selektive Priorisierung relevanter rechtlicher Fragestellungen kann somit nicht nur den Entwicklungsaufwand reduzieren, sondern auch die Integration rechtlicher Mechanismen in digitale Anwendungen effizienter gestalten.

4.2.2 Bedeutung der frühzeitigen Klärung der datenschutzrechtlichen Verantwortlichkeit

Eine weitere zentrale Herausforderung bestand darin, dass die datenschutzrechtliche Einordnung des späteren Bereitstellers des PERISCOPE-Systems zu Beginn des Projekts nicht eindeutig geklärt war. Unklar blieb, ob dieser als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter oder als Softwarehersteller agieren würde. Diese Unsicherheit führte dazu, dass bestimmte datenschutzrechtliche Anforderungen in einer hohen Detailtiefe analysiert wurden, die sich im Rückblick als teilweise ineffizient herausstellte. Eine frühzeitige Festlegung der datenschutzrechtlichen Rolle des Systemanbieters hätte diesen Mehraufwand verringert und die Implementierung rechtlicher Anforderungen zielgerichteter gestaltet.

Die Ergebnisse des Projekts zeigen, dass es für die Entwicklung datenschutzkonformer Systeme essenziell ist, rechtliche Zuständigkeiten so früh wie möglich zu definieren. Insbesondere die Rolle des Anbieters eines Datenschutztools bestimmt maßgeblich, welche rechtlichen Anforderungen erfüllt werden müssen. Eine unklare Verantwortlichkeitsverteilung kann dazu führen, dass unnötige Ressourcen in rechtliche Detailanalysen investiert werden, die letztlich nicht relevant für die praktische Umsetzung sind.

4.2.3 Zusammenfassung der rechtlichen Erkenntnisse

Die im PERISCOPE-Projekt gewonnenen rechtlichen Erkenntnisse verdeutlichen, dass eine selektive Priorisierung zentraler datenschutzrechtlicher Anforderungen essenziell ist, um eine effiziente und praxisnahe Umsetzung zu ermöglichen. Anstatt von Beginn an einen umfassenden Anforderungskatalog zu entwickeln, der später in Teilen nicht relevant ist, sollte der Fokus auf wenige, aber praxisrelevante juristische Kernaspekte gelegt werden. Darüber hinaus zeigt sich, dass eine frühzeitige Klärung der datenschutzrechtlichen Verantwortlichkeit die Effizienz der Systementwicklung erheblich steigern kann. Diese Erkenntnisse tragen dazu bei, zukünftige datenschutzrechtliche Implementierungsstrategien zielgerichteter zu gestalten und unnötigen Mehraufwand in der rechtlichen Analyse zu vermeiden.

4.3 Ökonomische Erkenntnisse

Die zunehmende Bedeutung von Datenschutzinitiativen in digitalen Geschäftsmodellen offenbart nicht nur regulatorische und ethische Anforde-

rungen, sondern auch substanzielle ökonomische Potenziale. Insbesondere Transparenz über Datennutzung und Intervenierbarkeit, verstanden als die Möglichkeit der Nutzenden, aktiv Kontrolle über ihre Daten auszuüben, entwickeln sich zu zentralen Differenzierungsmerkmalen im Wettbewerb. Basierend auf drei empirischen Studien wird im Folgenden herausgearbeitet, welche ökonomischen Implikationen sich aus Transparenz- und Intervenierbarkeitsmechanismen für Konsumierende, Plattformbetreibende und Anbietende von Privacy Management Systems (PMS) ergeben.

4.3.1 Privatsphärenfreundliche Plattformgeschäftsmodelle

In einer ersten Studie wurden die Präferenzen der Nutzenden hinsichtlich der Ausgestaltung von Plattform-Geschäftsmodellen analysiert.[11] Hierzu wurde ein Recommender-System entwickelt, das auf einer adaptiven Choice-Based Conjoint Analyse (ACBC) basiert. Ziel war es, jene Tradeoffs zu identifizieren, die Konsumentinnen und Konsumenten zwischen unterschiedlichen Datenschutzmerkmalen von Geschäftsmodellen vornehmen, insbesondere im Hinblick auf Transparenz und Kontrolle.

Die Untersuchung erfolgte mit einer Stichprobe von 84 Teilnehmenden aus den Vereinigten Staaten. Bewertet wurden hypothetische Plattformkonfigurationen, die sich hinsichtlich der Datennutzung (personenbezogen, anonymisiert, keine Nutzung), der Transparenzmechanismen (etwa digitaler Datenzugriff über Dashboards) und der Möglichkeiten zur Nutzungssteuerung unterschieden.

Die Ergebnisse zeigen, dass Plattformen, die auf anonyme Datennutzung und digitalen, jederzeit verfügbaren Zugang zu persönlichen Daten setzen, von den Nutzenden signifikant bevorzugt werden. Transparenzmechanismen wie Dashboards, die einen einfachen und kontinuierlichen Datenzugriff ermöglichen, steigern den wahrgenommenen Wert einer Plattform erheblich. Somit kann eine datenschutzfreundliche Ausgestaltung von Plattformmodellen durch transparente Informationsangebote und verbesserte Intervenierbarkeit nicht nur regulatorische Vorgaben erfüllen, sondern auch als strategisches Differenzierungsmerkmal mit direktem Einfluss auf die Marktattraktivität dienen.

11 *Baum* u.a., A Recommender System for Privacy Friendly Platform Business Models. 2024

4.3.2 Nutzungspräferenzen und Zahlungsbereitschaft für Privacy Management Systemen

Eine zweite Studie[12] untersuchte die Präferenzen der Konsumentinnen und Konsumenten für Privacy Management Systems (PMS), die darauf abzielen, Transparenz über Datenverarbeitungspraktiken zu schaffen und Intervenierbarkeit durch flexible Kontrollmöglichkeiten zu gewährleisten. Hierzu wurde eine klassische Choice-Based Conjoint Analyse (CBC) mit einer repräsentativen Stichprobe von 589 Teilnehmenden aus der deutschen Internetbevölkerung durchgeführt. Im Fokus standen zentrale Attribute wie der Modus des Datenzugriffs (postalische Information, digitaler Einmalzugriff, kontinuierliches Dashboard), die Verwaltung von Einwilligungen (individuell, vorgefertigte Profile, vollständige Zustimmung) sowie verschiedene Arten der Datennutzung für Marketingzwecke.

Die Ergebnisse zeigen, dass Nutzende einen kontinuierlichen, digitalen Zugriff über Dashboards und die Möglichkeit zur granularen Steuerung von Einwilligungen deutlich bevorzugen. Anonymisierte Datennutzung wird signifikant positiver bewertet als personenbezogene oder umfassende Nutzung. Zudem zeigen die Analysen, dass Rabatte zwar einen Einfluss auf die Nutzung von PMS haben, jedoch Transparenz und Intervenierbarkeit als primäre Treiber der Akzeptanz zu betrachten sind.

Daraus ergibt sich ein klares wirtschaftliches Potenzial: Systeme, die Transparenz schaffen und Intervenierbarkeit ermöglichen, erhöhen nicht nur die Bereitschaft zur Nutzung, sondern stärken auch das Vertrauen in digitale Dienste. Anbieter, die in solche PMS investieren, können sowohl ihre regulatorische Konformität absichern als auch die Nutzerloyalität und Zahlungsbereitschaft steigern.

Auch monetäre Anreize wie Rabatte beeinflussen die Bereitschaft zur Nutzung von datengetriebenen Diensten: Ein Rabatt von 12 % kann die Nutzungswahrscheinlichkeit selbst für weniger datenschutzfreundliche Konfigurationen erhöhen – z. B. bei der schlechtesten Konfiguration von 16,8 % auf 43,3 %. Dennoch bleibt Transparenz über Datennutzungspraktiken und die Möglichkeit, individuelle Datenfreigaben einfach zu verwalten, der entscheidende Treiber für Akzeptanz und Zahlungsbereitschaft. Nutzer bevorzugen digitalen Zugriff auf ihre Daten (CBC-Nutzenbeitrag +0,39) gegenüber postalischer Zustellung (−0,41); Privacy-Dashboards wurden

12 *Hanneke* u.a., Consumer Preferences for Privacy Management Systems, 2023.

hingegen neutral bewertet (+0,02), was auf weiteres Optimierungspotenzial in der User Experience hinweist.

4.3.3 Nutzersegmentierung

Abschließend wurde in einer dritten Studie eine Clusteranalyse durchgeführt, um unterschiedliche Nutzersegmente hinsichtlich ihrer Datenschutzpräferenzen zu identifizieren.[13]

Grundlage der Segmentierung bildeten zwei latente Konstrukte: die subjektive Bedeutung von Datenschutz (Privacy Importance) und das Wissen über Datenschutzrechte (GDPR Knowledge), die eine Differenzierung der Nutzenden nach Datenschutzbewusstsein und Handlungskompetenz ermöglichen. Anhand der repräsentativen Stichprobe von 589 Teilnehmenden aus der deutschen Internetbevölkerung wurden vier Cluster bzw. Segmente identifiziert:

- *Fundamentalists* (34 %) zeichnen sich durch ein hohes Maß an Datenschutzbewusstsein und Schutzmotivation aus
- *Amateurs* (27 %) haben ein moderates Bewusstsein, aber geringes Wissen und handeln häufig situativ.
- *Pragmatists* (24 %) wägen Datenschutzbedenken gegen Nutzenüberlegungen ab und verhalten sich kontextabhängig.
- Die *Unconcerned* (15 %) messen Datenschutz nur eine geringe Bedeutung bei und priorisieren Bequemlichkeit und finanzielle Anreize.

Diese Segmentierung orientiert sich an bestehenden Einteilungen,[14] wird jedoch um die Gruppe der *Amateurs* erweitert, um aktuelle Entwicklungen wie Sensibilisierung bei gleichzeitig begrenztem Wissen über Datenschutzrechte abzubilden. Besonders die *Fundamentalists* und *Pragmatists*, die zusammen mehr als die Hälfte der Nutzenden ausmachen, zeigen eine hohe Affinität zu Angeboten, die Transparenz und Intervenierbarkeit gewährleisten.

13 *Hanneke* u.a., GDPR Privacy Type Clustering: Motivational Factors for Consumer Data Sharing, 2023.

14 Siehe z. B. *Westin*, Social and Political Dimensions of Privacy, 2003.

4.3.4 Zusammenfassung der Ökonomischen Implikationen

Die drei Studien verdeutlichen, dass Transparenz und Intervenierbarkeit nicht nur rechtliche Anforderungen bedienen, sondern wesentliche ökonomische Erfolgsfaktoren im digitalen Wettbewerb darstellen. Unternehmen, die in leicht zugängliche, transparente Informationsangebote und flexible Steuerungsmöglichkeiten für ihre Nutzenden investieren, können nicht nur regulatorische Risiken minimieren, sondern auch das Vertrauen stärken und dadurch ihre Marktposition verbessern. Die Zahlungsbereitschaft für datenschutzfreundliche Angebote ist insbesondere bei den datensensiblen Konsumentensegmenten hoch und kann durch intelligente Kombination mit Anreizsystemen gesteigert werden.

Somit eröffnen Transparenz und Intervenierbarkeit neue ökonomische Potenziale für Plattformanbietende, die zunehmend auch als strategische Assets im digitalen Wettbewerb betrachtet werden müssen.

5. Implikationen für die Gestaltung effektiver Datenschutzinitiativen

Die Gestaltung erfolgreicher Datenschutzinitiativen erfordert mehr als die Erfüllung regulatorischer Vorgaben. Eine effektive Umsetzung muss Nutzerbedürfnisse berücksichtigen, rechtliche Anforderungen praxisnah integrieren und wirtschaftliche Rahmenbedingungen einbeziehen. Die im PERISCOPE-Projekt gewonnenen Erkenntnisse zeigen, dass Datenschutzmaßnahmen nur dann nachhaltig wirksam sind, wenn sie verständlich, zugänglich und wirtschaftlich tragfähig gestaltet werden. Dabei spielen drei zentrale Dimensionen eine Rolle: User Experience, rechtliche Präzision und ökonomische Anreize. Die folgenden Prinzipien und Gestaltungsempfehlungen verdeutlichen, wie Datenschutzinitiativen sowohl aus Nutzer- als auch aus Unternehmensperspektive optimiert werden können.

Die User Experience Erkenntnisse zeigen, dass die Gestaltung von Datenschutzinitiativen maßgeblich durch die Wahrnehmungen und Erlebnisse der Nutzer bestimmt wird. Ein rein regulatorischer Ansatz reicht nicht aus, um Datenschutzmaßnahmen effektiv nutzbar zu machen. Stattdessen sollten Datenschutzlösungen gezielt so gestaltet werden, dass sie den Bedürfnissen und Erwartungen der Nutzer gerecht werden. Dazu sollten Entwickler und Unternehmen folgende Prinzipien berücksichtigen:

- *Unmittelbares Feedback bereitstellen*, um Unsicherheiten zu vermeiden und die Nutzung zu erleichtern. Echtzeit-Rückmeldungen und kontextbezogene Anleitungen helfen, Betroffenenrechte effektiv wahrzunehmen.
- *Komplexität reduzieren*, indem Fachbegriffe vermieden und Datenschutzoptionen klar strukturiert und verständlich präsentiert werden.
- *Visuelle Unterstützung nutzen*, um abstrakte Datenschutzinformationen leichter erfassbar zu machen. Infografiken und intuitive Symbole verbessern die Verständlichkeit.
- *Interaktive Elemente integrieren*, um Nutzern mehr Kontrolle zu geben. Dynamische Datenschutzeinstellungen und Chatbots erleichtern die Verwaltung persönlicher Daten.
- *Datenschutz als Nutzermehrwert* begreifen, indem Datenschutzoptionen aktiv zur positiven Nutzungserfahrung beitragen, statt als reine Pflichtinformationen zu erscheinen.

Die rechtlichen Analysen des PERISCOPE-Projekts zeigen, dass eine späte Integration rechtlicher Vorgaben zu ineffizienten Anpassungen führt. Ein frühzeitiger rechtskonformer Gestaltungsansatz erleichtert die Umsetzung und reduziert unnötigen Mehraufwand.

- *Relevante Anforderungen frühzeitig priorisieren:* Viele anfänglich definierte Vorgaben erwiesen sich als überflüssig oder nicht *umsetzungsrelevant*. Eine gezielte Auswahl essenzieller rechtlicher Aspekte verbessert die Effizienz der Implementierung.
- *Datenschutzrechtliche Verantwortlichkeiten klären:* Unklarheiten über die Rolle des Systemanbieters führten zu *übermäßig* detaillierten Analysen. Eine frühzeitige Festlegung der Verantwortlichkeit optimiert den Entwicklungsprozess.

Die ökonomischen Erkenntnisse zeigen, dass ein „One-size-fits-all"-Ansatz bei der Gestaltung von Datenschutzinitiativen weder aus Nutzersicht noch aus wirtschaftlicher Perspektive optimal ist. Stattdessen sollten Unternehmen:

- *Differenzierte Datenschutzoptionen anbieten*, die verschiedenen Nutzersegmenten gerecht werden, von den *Fundamentalists* bis hin zu den *Unconcerned*.
- *Transparenz als Wettbewerbsvorteil* nutzen, indem sie verständliche und leicht zugängliche Informationen über Datennutzungspraktiken bereitstellen.

- *Anonymisierungstechnologien* einsetzen, um sowohl Wertschöpfungspotenziale zu realisieren als auch Nutzervertrauen zu stärken.
- *Rabattstrukturen und monetäre Anreize strategisch* einsetzen, um die Bereitschaft zur Datenfreigabe zu erhöhen, dabei jedoch die unterschiedlichen Präferenzen der Nutzersegmente berücksichtigen.
- *Intervenierbarkeit und Kontrolle* als *wesentliche* Faktoren für die Nutzerzufriedenheit und -bindung erkennen und entsprechende Funktionen implementieren.

Die wirtschaftlichen Implikationen der Untersuchung verdeutlichen, dass datenschutzfreundliche Geschäftsmodelle nicht zwangsläufig im Widerspruch zu ökonomischen Interessen stehen, sondern bei intelligenter Gestaltung sogar zu einem Wettbewerbsvorteil werden können[1]. Durch das Verständnis der unterschiedlichen Nutzerpräferenzen und die entsprechende Anpassung von Geschäftsmodellen können Plattformunternehmen sowohl regulatorische Anforderungen erfüllen als auch wirtschaftliche Ziele erreichen.

6. Limitationen und zukünftige Arbeit

Die im PERISCOPE-Projekt gewonnenen Erkenntnisse liefern interdisziplinäre Impulse für die Gestaltung datenschutzfreundlicher Technologien und zeigen, wie Transparenz und Intervenierbarkeit effektiv umgesetzt werden können. Gleichzeitig eröffnen sie neue Fragestellungen, die in zukünftiger Forschung weiter vertieft werden sollten, um die Anwendbarkeit und den langfristigen Nutzen dieser Prinzipien weiter zu optimieren.

Ein zentraler Aspekt zukünftiger Untersuchungen ist die langfristige Wirkung von Datenschutzmaßnahmen. Während die Studie die unmittelbare Wahrnehmung und Nutzung der Datenschutzinitiative analysiert, bleibt offen, wie sich diese Maßnahmen über einen längeren Zeitraum auf das Verhalten und das Vertrauen der Nutzer auswirken. Eine Langzeitbetrachtung könnte aufzeigen, inwiefern wiederholte Nutzungserfahrungen die Akzeptanz stärken und ob es effektive Mechanismen gibt, um eine nachhaltige Einbindung der Nutzer zu fördern.

Darüber hinaus bietet die Skalierbarkeit der Erkenntnisse ein wichtiges Forschungsfeld. Die im Projekt getesteten Maßnahmen wurden in einem definierten Anwendungskontext evaluiert. Zukünftige Arbeiten sollten untersuchen, wie sich die entwickelten Lösungen auf groß angelegte Plattformen mit heterogenen Nutzergruppen übertragen lassen. Besonders

relevant ist hierbei die Frage, wie sich Nutzer mit unterschiedlichem Vorwissen und verschiedenen Datenschutzpräferenzen in größeren Systemen orientieren und inwiefern sich die identifizierten UX-Prinzipien unter Bedingungen hoher Nutzerzahlen bewähren.

7. Fazit: Wege zu einem effektiveren und nutzerfreundlicheren Datenschutz

Dieser Beitrag liefert eine interdisziplinäre Perspektive auf die Gestaltung und Wirksamkeit von Datenschutzinitiativen und verknüpft Erkenntnisse aus den Bereichen User Experience, Recht und Ökonomie. Im Rahmen des PERISCOPE-Projekts wurden zentrale Herausforderungen und Potenziale datenschutzfreundlicher Technologien analysiert, wobei die Perspektiven verschiedener Stakeholdergruppen der Plattformökonomie berücksichtigt wurden. Durch die Kombination qualitativer und quantitativer Methoden konnten gezielte Implikationen für die Entwicklung effektiver Datenschutzmaßnahmen abgeleitet werden.

Drei empirische Studien – Usability-Tests, Tiefeninterviews und eine Online-Umfrage – ermöglichten eine umfassende Analyse der Nutzererfahrungen mit der Datenschutzlösung des Projekts. Während die Usability-Tests spezifische Nutzungshürden offenlegten, gaben die Tiefeninterviews detaillierte Einblicke in die Herausforderungen und Erwartungen der Plattformbetreiber. Die Online-Umfrage ergänzte diese Erkenntnisse um quantitative Daten zur Wahrnehmung und Akzeptanz von Datenschutzmaßnahmen unter realen Nutzern.

Die Untersuchungsergebnisse zeigen, dass Datenschutzinitiativen nicht nur regulatorische Anforderungen erfüllen, sondern konsequent an den Bedürfnissen der Nutzer ausgerichtet sein müssen. Unmittelbares Feedback, eine klare Informationsstruktur, visuelle Unterstützung und interaktive Elemente spielen eine entscheidende Rolle für die Akzeptanz und Nutzung von Datenschutztechnologien. Gleichzeitig wurde deutlich, dass eine frühzeitige und präzise rechtliche Einordnung notwendig ist, um ineffiziente Anpassungen im Entwicklungsprozess zu vermeiden. Darüber hinaus verdeutlichen die ökonomischen Erkenntnisse, dass datenschutzfreundliche Gestaltung nicht im Widerspruch zu wirtschaftlichen Interessen steht, sondern bei intelligenter Integration sogar zu einem Wettbewerbsvorteil werden kann.

Die gewonnenen Erkenntnisse tragen dazu bei, die Gestaltung von Datenschutzinitiativen zielgerichteter und nutzerfreundlicher zu machen. Die

interdisziplinäre Herangehensweise dieses Projekts zeigt, dass Datenschutz mehr ist als eine regulatorische Notwendigkeit – er kann als integraler Bestandteil digitaler Dienste gestaltet werden, um sowohl User Experience als auch wirtschaftliche Aspekte zu fördern.

Literatur

Astfalk, Stefanie; Schunck, Christian H. (2023): Balancing Privacy and Value Creation in the Platform Economy: The Role of Transparency and Intervenability. In: Roßnagel, H.; Schunck, C. H.; Günther, J. (Hrsg.): Open Identity Summit 2023. Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn: 2023, S. 135.

Baum, Lorenz; Hanneke, Björn und Hinz, Oliver (2024): A Recommender System for Privacy Friendly Platform Business Models. In: Proceedings der International Conference on Information Systems (ICIS) 2024. Bangkok, Thailand. Best Design Science Paper Nominee. Online verfügbar unter: https://aisel.aisnet.org/icis2024/security/security/3/.

Bundesministerium für Forschung, Technologie und Raumfahrt (o. D.): Periscope. Online verfügbar unter: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/periscope (besucht am 23.05.2025).

Hanneke, Björn; Baum, Lorenz und Hinz, Oliver (2023): GDPR Privacy Type Clustering: Motivational Factors for Consumer Data Sharing. In: Proceedings der European Conference on Information Systems (ECIS) 2023. Kristiansand, Norway. Online verfügbar unter: https://aisel.aisnet.org/ecis2023_rp/409/.

Hanneke, Björn; Baum, Lorenz; Schlereth, Christian und Hinz, Oliver (2023): Consumer Preferences for Privacy Management Systems. In: Proceedings der International Conference on Information Systems (ICIS) 2023. Hyderabad, India. Online verfügbar unter: https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/12/.

Kergroach, Sylvain (2021): SMEs Going Digital: Policy Challenges and Recommendations. In: OECD Going Digital Toolkit Notes, Nr. 15. Paris: OECD Publishing.

Mayring, Philipp (2021): Qualitative Content Analysis: A Step-by-Step Guide. London: Sage.

Nouwens, Maarten; Liccardi, Ilaria; Veale, Michael; Karger, David und Kagal, Lalana (2020): „Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence". In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. New York: ACM, S. 1–13.

Periscope Project (2025): Periscope Ergebnisse. Online verfügbar unter: https://websites.fraunhofer.de/periscope-projekt/?page_id=490 (besucht am 23.05.2025).

Pfeiffer, Lars (2024): Datenzugang in der Plattformökonomie: Regulierungsinstrumente in P2B-VO, DMA und DSA. In: Buchheim, Bernd; Kraetzig, Lars; Mendelsohn, David; Steinrötter, Matthias (Hrsg.): Plattformen. Grundlagen und Neuordnung des Rechts digitaler Plattformen. Baden-Baden: Nomos, S. 53–76.

Pfeiffer, Lars (2024): Big-Tech-Data: Zugangsnotwendigkeit und Zugangsausgestaltung nach dem Digital Markets Act. In: Augsberg, Arndt; Düwell, Thomas; Müller, Christian (Hrsg.): Datenzugangsregeln. Zwischen Freigabe und Kontrolle. Frankfurt a. M.: Campus Verlag, S. 101–136. Online verfügbar unter: https://www.campus.de/e-books/wissenschaft/philosophie/datenzugangsregeln-18409.html

Pfeiffer, Lars; Astfalk, Stefanie; Baum, Lorenz; Hanneke, Björn; Schunck, Christian; Winterstetter, Matthias (2023): Anforderungen an die automatisierte Protokollierung von Datenverarbeitungstätigkeiten in einem Transaktionsjournal: Eine Multi-Stakeholder-Perspektive auf Motivation und Umsetzung. In: Friedewald, Frauke; Roßnagel, Rainer; Neuburger, Marion; Bieker, Anika; Hornung, Thilo (Hrsg.): Daten-Fairness in einer globalisierten Welt. Baden-Baden: Nomos, S. 117–144.

Privacy Recommender (2023): Privacy Recommender. Online verfügbar unter: https://privacy.wiim-research.de (besucht am 23.05.2025).

Schmitt, Hartmut; Schunck, Christian H.; Lo Iacono, Luigi (2024): Datenökonomie in digitalen Ökosystemen – Neue Herausforderungen für den Datenschutz. In: Datenschutz und Datensicherheit – DuD, 48 Online verfügbar unter: https://www.springerprofessional.de/datenschutz-und-datensicherheit-dud-2-2024/26674164.

Shah, Akshat; Banakar, Varad; Shastri, Sambit; Wasserman, Mark und Chidambaram, Vijay (2019): „Analyzing the impact of GDPR on storage systems". In: Proceedings des 11th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage 19). Berkeley: USENIX Association.

Tesfay, Weldegebriel B.; Hofmann, Philipp; Nakamura, Takeshi; Kiyomoto, Shinsaku und Serna, Juan (2018): „PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation". In: Proceedings des vierten ACM International Workshop on Security and Privacy Analytics. New York: ACM, S. 15–21.

Westin, Alan F. (2003): „Social and Political Dimensions of Privacy". Journal of Social Issues, 59(2), S. 431–453.