PROF. DR. MAX VON GRAFENSTEIN, LL.M.

Design- und Methoden-baukasten zur Entwicklung und zum Nachweis wirksamer Einwilligungs- und anderer Entscheidungsmechanismen

Unterbeauftragung im Rahmen des Forschungsprojekts Sicher im Datenverkehr (SiD)

HIIG DISCUSSION PAPER SERIES 2026-04

ABSTRACT

Der vorliegende Design- und Methodenbaukasten dient der Entwicklung und dem Nachweis wirksamer Einwilligungs- und Entscheidungsmechanismen im digitalen Raum. Er ist entlang eines strukturierten Rahmens aufgebaut, der rechtliche Anforderungen, zentrale Designfaktoren, empirische Methoden sowie einen Ausblick auf die Weiterentwicklung des Stands der Technik umfasst. Grundlage ist ein über zehnjähriger interdisziplinärer Forschungsprozess an der Schnittstelle von Datenschutzrecht, User Experience- und Interface-Design, Mensch-Maschine-Interaktion, Verhaltensökonomie und Entrepreneurship-Forschung. Ausgangspunkt ist, dass die Wirksamkeit informierter Einwilligung im Wesentlichen von drei Faktoren abhängt: dem Vorwissen und der Haltung der Nutzer*innen, dem Vertrauen in den digitalen Dienst sowie der Gestaltung der Informations- und Entscheidungsarchitektur. Der Fokus des vorliegenden Design- und Methodenbaukasten liegt auf letzterem, also der Frage, wie Einwilligungsmechanismen ausgestaltet werden können, so dass sie tatsächlich informierte und unmissverständliche Entscheidungen ermöglichen, sprich, dass die eingeholte Einwilligung wirksam und damit rechtskonform ist.

KEYWORDS

Informierte Einwilligung, Wirksamkeitsnachweis, DSGVO, User Experience Design, User Interface Design, Empirische Methoden, Designfaktoren, Dark Patterns, Bright Patterns, Nudging, Stand der Technik

CITATION

von Grafenstein, M. (2026). Design- und Methodenbaukasten zur Entwicklung und zum Nachweis wirksamer Einwilligungs- und anderer Entscheidungsmechanismen. HIIG Discussion Paper Series 2026-4. 35 pages. https://doi.org/10.5281/zenodo.21024801.

AUTOR / FÖRDERHINWEIS

Prof. Dr. Max von Grafenstein, LL.M., Regulierungswissenschaftler

Das vorliegende Gutachten wurde durch das Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG) im Rahmen des vom Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) geförderten Forschungsprojekts „Sicher im Datenverkehr: Alltagsnahe Veranschaulichung von Grundrechtsrisiken“ (SiD), Förderkennzeichen: 16KIS1968, beauftragt.

INHALT

1 EINFÜHRUNG

Der vorliegende Design- und Methodenbaukasten soll der Entwicklung und zum Nachweis wirksamer Einwilligungs- und anderer Entscheidungsmechanismen dienen. Er fasst die Ergebnisse aus einem mehr als 10-jährigen interdisziplinären Forschungsprozess an der Schnittstelle des Datenschutzrechts, der User Experience- und User Interface-Gestaltung, der Mensch-Maschine-Interaktion, Verhaltensökonomie und Entrepreneurship-Forschung zusammen.[1]

Danach gibt es drei wesentliche Faktoren, die die Wirksamkeit der informierten Einwilligung beeinflussen:[2]

1. Das Vorwissen und die Haltung der jeweiligen Internetnutzer:in;
2. das grundsätzliche Vertrauen, das eine Internetnutzer:in der besuchten Website bzw. dem genutzten Dienst entgegen bringt; sowie
3. die Art und Weise, wie ein Dienst seine Nutzer:innen darüber informiert, wie er ihre Daten verarbeiten möchte.

Der hier dargestellte Design- und Methodenbaukasten konzentriert sich auf den dritten Punkt.

Dienstanbieter, die personenbezogene Daten verarbeiten, wie zum Beispiel Websitebetreiber, stehen in einem Zielkonflikt, wenn sie ihre Nutzer:innen über die Nutzung ihrer Daten informieren. Einerseits möchten sie bei ihren Nutzer:innen Vertrauen in die Nutzung ihres Dienstes, ihre Marke und in die Preisgabe der Daten aufbauen. Andererseits streben viele Dienste nach einer formal möglichst hohen Einwilligungsrate, damit sie möglichst viele Daten verarbeiten können.[3]

---

[1] Siehe die Forschungsprojekte im Rahmen der Forschungsstelle Digitale Selbstbestimmung am Einstein Center Digital Future – Universität der Künste Berlin (https://www.ziw.udk-berlin.de/forschung/digital-self-determination/) sowie im Rahmen des Forschungsprogramms Daten, Akteure, Infrastrukturen: Governance datengetriebener Innovation und Cybersicherheit am Alexander von Humboldt Institut für Internet und Gesellschaft (https://www.hiig.de/research/daten-akteure-infrastrukturen/).

[2] Siehe etwa Dinev, Tamara/Hart, Paul, An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research 17 (2006), S. 61–80; Culnan, Mary J./Armstrong, Pamela K., Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, Organization Science 10 (1999), S. 104–115; Pavlou, Paul A., Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, International Journal of Electronic Commerce 7 (2003), S. 101–134; McDonald, Aleecia M./Cranor, Lorrie Faith, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 4 (2008), S. 543–568; Nouwens, Midas et al., Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence, Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), 2020, S. 1–13; Schaub, Florian et al., Designing Effective Privacy Notices and Controls, IEEE Internet Computing 21 (2017), S. 70–77.

[3] Siehe etwa Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on Art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924.

Bei der Frage, wie Dienste diesen Zielkonflikt auflösen, wird häufig zwischen sogenannten Bright Patterns bzw. neutralen Techniken und Dark Patterns unterschieden.[4] Der Begriff Dark Patterns meint, dass ein Dienst Techniken verwendet, die

1. seine Nutzer:innen über die konkrete Ausgestaltung der Information im Unklaren darüber lässt, welche Risiken für sie mit der Preisgabe ihrer Daten verbunden sind, und sie damit keine informierte Entscheidung über die Vorteile und Risiken der Datenpreisgabe treffen können, und/oder
2. es ihren Nutzer:innen über die konkrete Ausgestaltung der Entscheidungsarchitektur erschwert, entsprechend ihrer Vorteils-Risiko-Abwägung eine entsprechende Entscheidung zu treffen.

Die folgenden Ausführungen konzentrieren sich auf neutrale Techniken bzw. Bright Patterns, die durch eine entsprechende Ausgestaltung der Informations- und Entscheidungsarchitektur nachweisbar informierte Entscheidungen ermöglichen. Wenn auch in datenschutzrechtlicher Hinsicht irrelevant, sei doch mit Blick auf das sehr große Interesse der Wirtschaft darauf hingewiesen, dass eine nutzungsfreundliche Implementierung informierter Entscheidungsprozesse zu einer Erhöhung der Einwilligungsrate führen kann.[5]

In der bisherigen Praxis war die Verwendung solcher Techniken trotzdem keine Selbstverständlichkeit. Insbesondere auf Websites wurden Einwilligungsmechanismen, sog. Cookie Banner, bisher auf eine Weise ausgestaltet, die Nutzer:innen kaum in einer für sie verständlichen Weise über die Verwendung ihrer Daten informierte. Häufig ist es für Nutzer:innen auch schwieriger, die Einwilligungsanfrage zu verweigern, als ihr zuzustimmen. Und wenn eine Möglichkeit zum Widerspruch besteht, wird diese in aller Regel auf einer Unterseite versteckt, was es Nutzer:innen erschwert, ihr Widerspruchsrecht auszuüben. Selbst wenn Nutzer:innen die Anfrage mit einem einzigen Klick auf "Alles ablehnen", "Alles annehmen" oder "Schließen" wegklicken können, läuft die Häufigkeit der Anfragen darauf hinaus, dass das Wegklicken aufgrund der verursachten sog. Einwilligungsmüdigkeit kaum als informierte und eindeutige Entscheidung angesehen werden kann.

In Ansehung dieser Praktiken sah sich der Gesetzgeber gezwungen, gesetzliche Vorgaben zur Ermöglichung wirksamer Entscheidungsprozesse zu machen. Auf diese wird im Folgenden kurz eingegangen.

---

[4] Leiser, M. and Santos, C., Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface (April 27, 2023). Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface, Vol. 15 No. 1 (2024): BILETA Special Issue , Available at SSRN: https://ssrn.com/abstract=4431048; Bielova, N. Survey of academic studies measuring the effect of dark patterns on acceptance consent rate of users in consent banners; Graßl, P., Schraffenberger, H., Borgesius, F., and Buijzen, M., Dark and bright patterns in cookie consent requests.

[5] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894.

2 RECHTLICHE ANFORDERUNGEN

Art. 6 Abs. 1 lit. a DSGVO verlangt als eine der möglichen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten die informierte Einwilligung. Gem. Art. 4 Nr. 11 DSGVO ist eine Einwilligung

> *"jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".*

Art. 25 DSGVO stellt für die Implementierung der informierten Einwilligung weitere Anforderungen auf. Insbesondere muss die verantwortliche Stelle, also zum Beispiel ein Website-Betreiber, die informierte Einwilligung so technisch-organisatorisch umsetzen, dass der Schutz gegen die Risiken, die die Datenverarbeitung für die Grundrechte der Betroffenen verursacht, wirksam ist.

Dabei ist der **Stand der Technik** zu beachten, das heißt, die jeweils auf dem Markt verfügbare, wirksamste Umsetzung der informierten Einwilligung ("best available technology"). Der Stand der Technik stellt eine sogenannte dynamische Verweisung auf den jeweiligen Entwicklungsstand dar. Begrifflich fordert der Stand der Technik einerseits mehr als die sogenannten anerkannten Regeln der Technik (Best Practice), weil der Stand der Technik einen wissenschaftlichen Nachweis erfordert, dass es sich tatsächlich um die wirksamste Umsetzung handelt. Andererseits fordert der Stand der Technik weniger als der sogenannte Stand der Wissenschaft, weil er nicht die Umsetzung jedes Konzepts fordert, das wissenschaftlich erwiesen das wirksamere ist, sondern nur ein solches, das bereits auf dem Markt verfügbar ist. Außerdem darf die verantwortliche Stelle die Implementierungskosten berücksichtigen. Das bedeutet, dass sie den Stand der Technik nicht implementieren muss, wenn die Kosten hierfür unverhältnismäßig sind.[6]

Der Europäische Datenschutzausschuss (EDSA) stellt in seinen Guidelines 4/2019 on Article 25 Data Protection by Design and by Default entsprechend klar, dass der Wirksamkeitsnachweis das zentrale Element von Art. 25 DSGVO darstellt. Der EDSA führt hierzu aus:

> *"Zu diesem Zweck kann der Verantwortliche geeignete Leistungskennzahlen (KPI) festlegen, um die Wirksamkeit nachzuweisen. Eine Leistungskennzahl ist ein vom Verantwortlichen gewählter messbarer Wert, der aufzeigt, wie effektiv der Verantwortliche sein Datenschutzziel erreicht. Leistungskennzahlen können quantitativer Natur sein, wie beispielsweise der Prozentsatz von Fehlalarmen oder*

[6] Hansen, M. in: Datenschutzrecht – DSGVO/BDSG, Simitis, S., Hornung, G. and Spiecker genannt Döhmann, I. (Eds.), Art. 25 cip. 36/37 and Art. 32 cip. 27 et seq.; siehe zum Regulierungskonzept und seinen bezweckten Auswirkungen auf die Marktdynamik, Grafenstein, M. v. (2019). Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design, in: González-Fuster, G., van Brakel, R., & P. De Hert, Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed.. Cheltenham: Edward Elgar Publishing.

> *Falschnegativen, die Verringerung von Beschwerden oder die Verkürzung der Reaktionszeit, wenn betroffene Personen ihre Rechte ausüben; oder sie können qualitativer Natur sein, wie beispielsweise Leistungsbewertungen, die Verwendung von Bewertungsskalen oder Expertengutachten. Alternativ zu KPIs können Verantwortliche die wirksame Umsetzung der Grundsätze nachweisen, indem sie die Gründe für ihre Bewertung der Wirksamkeit der gewählten Maßnahmen und Garantien darlegen."*[7]

In der Praxis stellt die **größte Herausforderung bei der Umsetzung** einer wirksamen Einwilligung aktuell **die Informiertheit** der Einwilligung dar. Ein Wirksamkeitsnachweis wird in der Praxis bisher kaum erbracht. Im Gegenteil gibt es zahlreiche empirische Studien, die belegen, dass herkömmliche Cookie Banner Internetnutzer nicht ausreichend informieren.[8] Diesen Studien zufolge ziehen Verbraucher:innen zwar datenschutzfreundliche Dienste solchen mit höheren Risiken vor. Sie können diese aber nicht erkennen und sich deswegen auch nicht für sie entscheiden.[9]

Was in der aktuellen Praxis bestenfalls anzutreffen ist, ist die Anwendung der vorgenannten anerkannten Regeln der Technik (sog. Best Practice). Diese Best Practice-Regeln unterscheiden sich vom Stand der Technik dadurch, dass die verantwortliche Stelle keinen empirischen Wirksamkeitsnachweis erbringen muss. **Best Practice entspricht jedoch nicht** dem in **Art. 25 DSGVO** geforderten Niveau, das einen Wirksamkeitsnachweis verlangt.[10]

Es gibt zahlreiche Beiträge aus Wissenschaft und Praxis dazu, wie Einwilligungsprozesse nicht gestaltet werden sollten.[11] Selbst wo positive Vorgaben gemacht werden, stellen diese nur Best Practice-Regeln dar, aber keinen empirischen Nachweis, dass diese wirksame Entscheidungsprozesse ermöglichen. Im Gegenteil hat eine quantitative Studie ergeben, dass Internetnutzer:innen selbst nach Best Practice-Regeln gestaltete

[7] EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 7: "To do so, the controller may determine appropriate key performance indicators (KPI) to demonstrate the effectiveness. A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves their data protection objective. KPIs may be quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards."

[8] Siehe etwa Utz, C., Degeling, M., Fahl, M., Schaub, F., and Holz, T. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212.

[9] Tsai,J. Y., Egelman, S., Cranor, L., Acquisti, A. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research Vol. 22, No. 2, June 2011, pp. 254–268.

[10] Hansen, M. in: Datenschutzrecht – DSGVO/BDSG, Simitis, S., Hornung, G. and Spiecker genannt Döhmann, I. (Eds.), Art. 25 cip. 36/37 and Art. 32 cip. 27 et seq.

[11] Siehe etwa CNIL, Bielova, N. (2023). A survey of user studies as evidence for dark patterns in consent banners, unter https://linc.cnil.fr/en/survey-user-studies-evidence-dark-patterns-consent-banners.

Cookie Banner so uninformiert wegklicken, dass man kaum von einer „informierten" Einwilligung im Sinne des Gesetzes sprechen kann.[12] Die folgenden Kapitel fassen die Ergebnisse und Methoden aus einem Forschungs- und Entwicklungsprozess zusammen, den der Autor dieser Guidelines in den letzten 10 Jahren durchlaufen hat und **mit denen sich der Stand der Technik positiv bestimmen und fortentwickeln lässt.**[13]

3 DESIGNFAKTOREN ZUR ENTWICKLUNG WIRKSAMER ENTSCHEIDUNGSMECHANISMEN

Eine verständliche Gestaltung der datenschutzrechtlich relevanten Informationen trägt nicht nur erheblich zu einer besseren Informiertheit von Internetnutzer:innen über die Verarbeitung ihrer personenbezogenen Daten bei, sondern auch zu einem höheren Vertrauen in die Nutzung des Dienstes sowie in die Preisgabe bzw. Verarbeitung ihrer Daten. Eine verständliche Gestaltung hat damit auch wesentlichen Einfluss auf die Wahrscheinlichkeit, ob Internetnutzer:innen der Preisgabe ihrer Daten zustimmen oder ihr widersprechen.[14] Um wirksame Entscheidungsprozesse im Sinne von Art. 25 DSGVO zu ermöglichen, sollten sich die Betreiber von Websites und anderen digitalen Diensten auf folgende Faktoren konzentrieren. Die folgenden Faktoren sind nicht nur wissenschaftlich als wirksamste Umsetzungsfaktoren der informierten Einwilligung nachgewiesen, sondern auch auf dem Markt verfügbar.[15] Die folgende Darstellung erhebt freilich weder Anspruch auf Abschließbarkeit noch Endgültigkeit. Vielmehr wird sich der aktuelle Stand der Technik in Bezug auf die informierte Einwilligung (hoffentlich) ständig weiterentwickeln.

---

[12] Grassl, P., Gerber, N., & Grafenstein, M. v. (2024). How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights? European Data Protection Law Review, 10(1), 96–104. DOI: 10.21552/edpl/2024/1/14; ibid (longer version including all pictures and charts), available under https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5012997; siehe bereits Grafenstein, M. v., Jakobi, T., & Stevens, G. (2021). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centred UX-design methods. Computer Law & Security Review, 46. DOI: 10.1016/j.clsr.2022.105722.

[13] Siehe Fn. 1.

[14] Adjerid, I., Acquisti, A., Brandimarte, L., Loewenstein, G. Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, in: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS), 2013; Ebert, N., Pape, S., Spohr, D., Bingel, J. Bolder is Better: Raising User Awareness for Data Privacy through Visualizations. arXiv, 2021; Godinho de Matos, A., Godinho de Matos, M., Adjerid, I. Consumer Consent and Firm Targeting after GDPR: The Case of a Large Telecom Provider, Working Paper, 2022; siehe auch die Ergebnisse zweier quantitativen Nutzerstudien zum Einwilligungsverhalten in dem White "Die informierte Einwilligung als Baustein für einen fairen Wettbewerb" verfügbar unter https://tinyurl.com/Consenter-White-Paper.

[15] Siehe der mittlerweile zu einer marktreifen Lösung weiter entwickelte Forschungsdemonstrator Consenter, verfügbar unter www.consenter.eu.

3.1 Zweckspezifizierung mit Blick auf die Vorteile und Risiken der Datenverarbeitung

Die aus Nutzer:innensicht entscheidungsrelevantesten Informationen sind dabei Angaben zu den Zwecken, für die ihre Daten verarbeitet werden, und die damit jeweils verbundenen Vorteile und Datenschutzrisiken.[16] Der Fokus auf die Verarbeitungszwecke entspricht der datenschutzrechtlichen Konzeption, nach der die Verarbeitungszwecke der Dreh- und Angelpunkt der datenschutzrechtlichen Prüfung sind. Die Darstellung der Vorteile und Risiken entspricht nicht nur der Funktion des Zweckbindungsprinzips, wonach die Betroffenen anhand der Zweckspezifizierung die Folgen für sich abschätzen können müssen.[17] Sie entspricht auch verhaltensökonomischen Theorien des Privacy Calculus, wonach Laien bei Entscheidungen über die Preisgabe ihrer Daten stets die damit verbundenen Vorteile und Nachteile abwägen.[18]

Die verständliche **Darstellung der Vorteile und Risiken** in Verbindung mit dem jeweiligen Verarbeitungszweck **stellt einen der beiden entscheidenden Wendepunkte** bei der evidenzbasierten Entwicklung wirksamer Entscheidungsprozesse **dar**. Verschiedene qualitative und quantitative Studien zeigen, dass durch die Darstellung der Vorteile und Risiken das Verständnis bei Endnutzer:innen erheblich gesteigert werden kann. Die stärksten Verständnisgewinne lassen sich in Kombination mit agenten-gestützten Entscheidungsprozessen erzielen (siehe unten Punkt 3.3).[19]

Auf Basis des aktuellen Forschungs- und Entwicklungsstands empfiehlt sich die Formulierung folgender Verarbeitungszwecke (die Klammerzusätze weisen lediglich auf die rechtlich erforderlichen

---

[16] Zu den weiteren rechtlich erforderlichen Information die einschlägige juristische Literatur sowie zu den aus Nutzersicht relevanten Informationen etwa Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924.

[17] Art. 29 Working Party, Opinion 03/2013 on purpose limitation, pp. 11 et seq; siehe bereits zur ePrivacy-Richtlinie Dammann/Simitis, Art. 6, Rn. 22; siehe zur datenschutzrechtlich-dogmatischen Begründung Grafenstein, M. v. (2021). Refining the concept of the right to data protection in article 8 ECFR – Part II. European Data Protection Law Review, 7(2), 190-205. DOI: 10.21552/edpl/2021/2/8 und zur entsprechenden Nutzerperspektive sowie Klärung der Begriffe “Konsequenzen” und "Auswirkungen" Grafenstein, M. v., Jakobi, T., & Stevens, G. (2021). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centred UX-design methods. Computer Law & Security Review, 46. DOI: 10.1016/j.clsr.2022.105722.

[18] Vgl. Dinev, T., Hart, P., 2006. An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research 17, S. 61–80, 61; grundlegend bereits Culnan, M. J., Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, Organization Science 10, S. 104–115.

[19] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894; siehe in größerem Detail Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

Voreinstellungen hin):

1. Anonyme Verbesserung des Dienstes (Opt-Out)
2. Verbesserung des Dienstes (Opt-In)
3. Freischalten zusätzlicher Website-Funktionen (Opt-In)
4. Personalisierung der Website (Opt-In)
5. Unterstützung von Marketinganalysen (Opt-In)
6. Erhalte Marketingangebote (Opt-In)
7. Erhalte personalisierte Marketingangebote (Opt-In)
8. Personalisierung von Online-Werbung (Opt-In)
    a. Profilbasierte Personalisierung
    b. Erinnerungswerbung (= Re-Targeting) → noch in Diskussion
    c. Gruppenbasierte Personalisierung
    d. Kontextbasierte Werbung

Diese Zweckliste ist nicht abschließend und erhebt keinen Anspruch auf Ausschlichkeit. Weitere Verarbeitungszwecke, die von einer Entscheidung der jeweiligen Internet:nutzerin (das heißt von einem Opt-In- oder Opt-Out-Verfahren) abhängen, sind genauso möglich, wie noch verständlichere Formulierungen, soweit dies entsprechende Nachweise stützen.

Für die Formulierung ist entscheidend, dass sie einerseits Internetnutzer:innen eine hinreichend konkrete Vorstellung vermittelt, wofür und auf welche Weise ihre Daten verarbeitet werden. Andererseits muss sie so konkret sein, dass sich anhand ihrer die jeweils verursachten konkreten Grundrechtsrisiken feststellen und von anderen Verarbeitungsverfahren unterscheiden lassen.[20]

Die Zwecke können in unterschiedlichen Verhältnissen zueinander stehen. Wie die Zweckbeispiele 6 bis 8 zeigen, lassen sich auch Zweckhierarchien bilden, die sich entweder ausschließen (Beispiele 6 und 7) oder ergänzen (Beispiele 8 lit. a bis d). Unterschiedlich formulierte Zwecke, die das gleiche Verarbeitungsverfahren beschreiben und entweder die gleichen oder höhere bzw. niedrigere Vorteile und Risiken verursachen, lassen sich über eine Übersetzungsmatrix zuordnen (siehe etwa mit Blick auf die Zweckformulierungen des Transparency and Consent Frameworks des IAB Europe).[21] Die Abweichungen sind den Internetnutzer:innen gegebenenfalls entsprechend anzuzeigen (siehe hierzu unter Punkt 3.1.3).

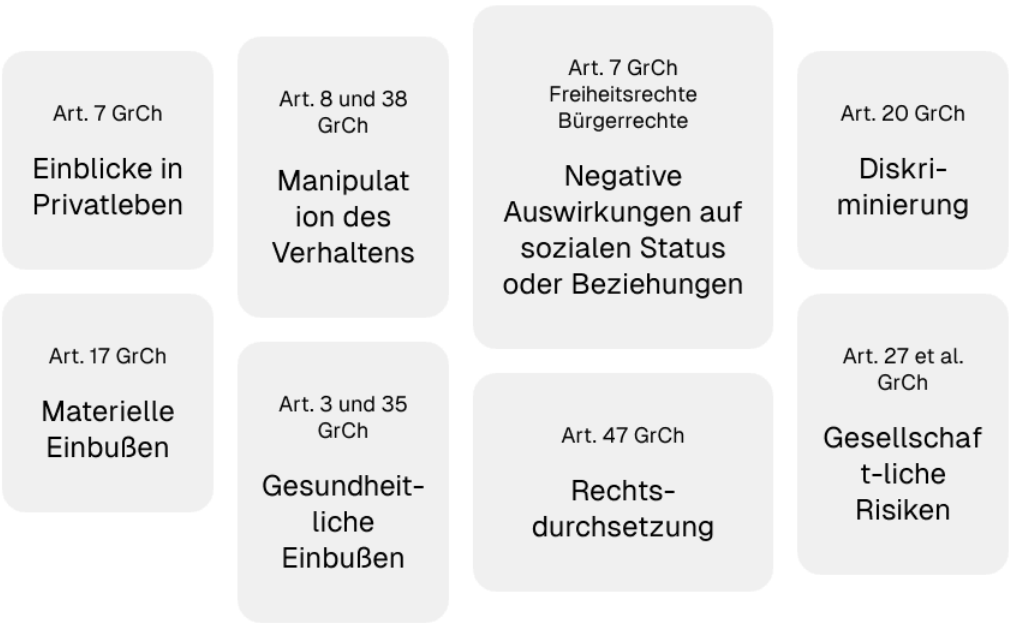
Es ist davon auszugehen, dass Zwecke noch verständlicher formuliert werden können und der Stand der Technik entsprechend fortentwickelt wird.

Für die Darstellung der Risiken kann auf die Ergebnisse mehrerer rechtlicher sowie empirischer

[20] Grafenstein, M. v. (2021). Refining the concept of the right to data protection in article 8 ECFR – part III. European Data Protection Law Review, 7(3), 373-387. DOI: 10.21552/edpl/2021/3/6 mit weiteren Nachweisen.

[21] Siehe auch Annex 1 der in Spezifikation ConStand verfügbar unter https://tinyurl.com/ConStand.

Forschungsprojekte zurückgegriffen werden. Danach entsprechen die aus Nutzersicht relevanten Risiken weitgehend den **Grundrechtsrisiken**:[22]



Diese Risiken sind dem jeweiligen Verarbeitungszweck zuzuordnen und auf einer Skala von 1-3 zu gewichten (1 = geringes Risiko; 2 = mittleres Risiko; 3 = hohes Risiko). Die Zuordnung und Gewichtung der Risiken hat auf Grundlage der etablierten Methodologien zur Feststellung der Datenschutzrisiken zu erfolgen.[23]

Für die Darstellung der Risiken gegenüber den Internetnutzer:innen sollte der Fokus auf den unmittelbar aus dem Verarbeitungszweck resultierenden Risiken für die individuellen Grundrechte der jeweils betroffenen Internetnutzer:in liegen. Das mittelbare, das heißt abstrakte Risiko, dass etwa die Daten zweckentfremdet werden könnten, wird hier als Risiko der Sicherheit der Verarbeitung gem. Art. 32 DSGVO eingeordnet. IT-Security-Risiken gem. Art. 32 DSGVO sowie gesellschaftliche Risiken, wie zum Beispiel für die Demokratie oder die Solidarität innerhalb einer Gesellschaft, werden zumindest in den hier zugrunde liegenden Forschungsdesigns bisher nicht abgebildet. Hintergrund ist, dass dies in bisherigen

[22] Grafenstein, M. v., Jakobi, T., & Stevens, G. (2021). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods. Computer Law & Security Review, 46. DOI: 10.1016/j.clsr.2022.105722, pp. 20/21.

[23] Siehe etwa das Standard-Datenschutzmodell in der jeweils aktuellsten Fassung veröffentlicht auf https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

Iterationen der Designs zu einer Überforderung der Testpersonen führte.[24]

Hier gibt es ebenfalls noch erhebliches Entwicklungspotential für den Stand der Technik, neben den konkreten individuellen Risiken auch abstrakte und gesellschaftliche Risiken abzubilden, ohne die Nutzer:innen zu überfordern.

Neben den Risiken sollten den jeweiligen Verarbeitungszwecken auch die Vorteile zugewiesen und gewichtet werden, die Internetnutzer:innen mit Preisgabe ihrer Daten erhalten. Die Zuordnung der Risiken und Vorteile hat nach aktuellem Wissensstand einen wesentlichen Einfluss auf die Informiertheit, das Vertrauen und damit die Einwilligungsrate.[25] Bei der Zuordnung und Gewichtung ist daher größte Sorgfalt anzulegen, damit kein Risiko kleiner oder größer dargestellt wird, als es tatsächlich ist. Gleiches gilt für die Darstellung der Vorteile. Die richtige Zuordnung und Gewichtung sollte daher idealerweise im Rahmen eines Multi-Stakeholder-Prozesses abgesichert werden, der neben Laien auch Experten involviert, die in verschiedenen Bereichen tätig sind, insb. im Daten- und Verbraucherschutz sowie in den verschiedenen – untereinander konkurrierenden – Wirtschaftszweigen (siehe hierzu auch unter Punkt 4.2).[26]

3.2 Layout und visuelle Darstellung / Hierarchie

Bei der visuellen Darstellung ergibt sich in der Regel ein Zielkonflikt: Aus rechtlicher Perspektive müssen die Informationen so präzise und umfassend wie möglich dargestellt werden. Aus verhaltensökonomischer Perspektive sollten die Informationen auf ihre wesentlichen Inhalte verdichtet werden, damit Laien sie aufnehmen und verstehen können.[27] Bei der Auflösung dieses Zielkonflikte können folgende

---

[24] Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924; Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

[25] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894; siehe in größerem Detail Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

[26] Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924; Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

[27] Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924 mit weiteren Nachweisen.

Designprinzipien leiten:

Die für Internetnutzer:innen entscheidungserheblichen Informationen sind jeweils durch **Visualisierungen und/oder Icons** zu unterstützen. Zumindest zu Beginn können und sollten Visualisierungen und Icons textliche Erklärungen jedoch nicht ersetzen; sie können aber über die Zeit von Internetnutzer:innen erlernt werden, so dass sie zu einem späteren Zeitpunkt die textliche Darstellung ersetzen können.[28]

Grundsätzlich gilt die Maxime, **je weniger textlich-visuelle Elemente auf einer visuellen Ebene, desto eher nehmen Laien die Information wahr und verstehen sie.** Das verschärft zwar den eingangs beschriebenen Zielkonflikt. Der Zielkonflikt lässt sich aber auflösen, indem man die Informationen auf verschiedene visuelle Ebenen verteilt.[29] Dabei ist zu gewichten: die aus Nutzersicht relevantesten Informationen sind auf der ersten visuellen Ebene anzuordnen, die weniger relevanten Informationen auf der jeweils hinteren visuellen Ebene.

Nach aktuellem Stand der Technik sollten **auf der ersten visuellen Ebene die Zwecke** mit dem jeweils verwendeten Privacy Icon dargestellt werden. In dem hier referenzierten Forschungsdemonstrator werden die jeweiligen Vorteile und Risiken auf der ersten visuellen Ebene noch nicht einzeln abgebildet, sondern nur in einem **Vorteils-/Risiko-Verhältnis** verdichtet. Das jeweils dargestellte Wert-/Risiko-Verhältnis ist für Internetnutzer:innen entscheidend und beeinflusst maßgeblich die Einwilligungsrate.[30]

Die Darstellung der einzelnen Risiken und Vorteile für jeden Verarbeitungszweck auf der ersten Ebene hat sich bisher als herausfordernd dargestellt, da es sehr viel Information auf einmal ist, was sich negativ auf das generelle Verständnis der Internetnutzer:innen auswirkt. Die **Darstellung der einzelnen Risiken und Vorteile** wird deshalb **erst auf der zweiten visuellen Ebene** dargestellt. Dies beinhaltet auch eine Liste der Risiken, die nicht eintreten. Das soll verhindern, dass Internetnutzer:innen sich Risiken "einbilden", die der jeweilige Verarbeitungszweck nicht unmittelbar verursacht.[31]

---

[28] Siehe zu den Abwägungsentscheidungen, die bei einer möglichst verständlichen textlich-visuellen Darstellung zu treffen sind, im Detail etwa bei Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924 mit weiteren Nachweisen.

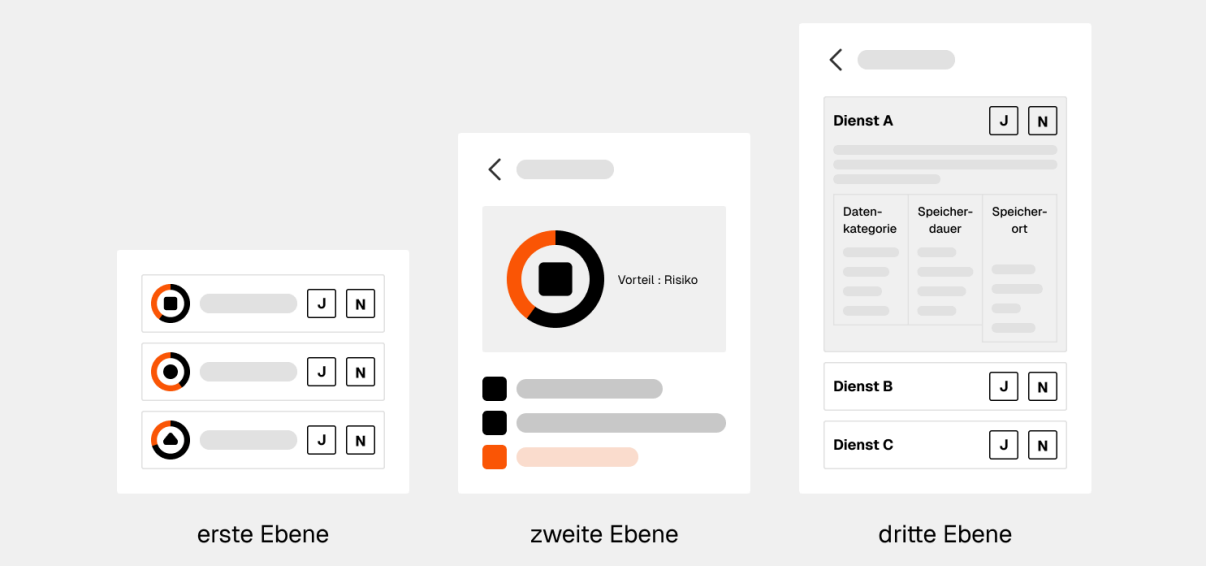
[29] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, S. 19.

[30] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894; siehe im Detail Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

[31] Vgl. die Erhöhung der falschen Negativtreffer durch mehr Transparenz in Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review) sowie der Schutz vor der "diffusen Angst" in BVerfG, 2nd March 2010, 1 BvR 256/08, 1 BvR 263/08, and 1 BvR 586/08 (Vorratsdatenspeicherung), cip. 241.

Erst **auf der dritten Ebene folgt eine Darstellung, welche Daten** konkret erhoben werden, welche eventuell **eingesetzte Drittanbieter** Zugriff auf diese Daten erhält, wie lange und wo diese Daten verarbeitet werden. Auf der letzten Ebene werden weitere Informationen dargestellt, die der Gesetzgeber für eine informierte Einwilligung für relevant hält.

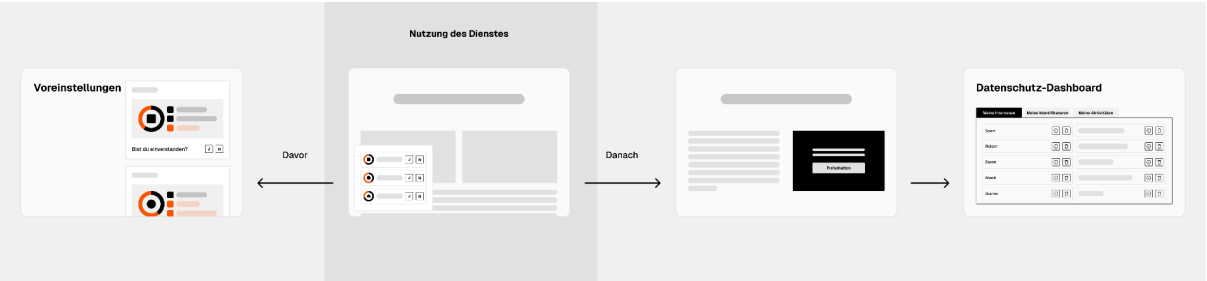
Bei der Frage, auf welcher visuellen Ebene welche Informationen wie dargestellt werden müssen, damit die Internet:nutzerinnen optimal informiert werden, gibt es selbstverständlich ebenfalls noch Potenzial, den Stand der Technik fortzuentwickeln.



3.3 Zeitpunkt und Kontext der Anfrage

Der zweite entscheidende Wendepunkt bei der evidenzbasierten Entwicklung wirksamer Entscheidungsprozesse stellt dessen Prozeduralisierung dar. Internetnutzer:innen sind am besten in der Lage, die komplexen Verarbeitungsprozesse in Hinsicht auf die potentiellen positiven wie negativen Folgen auf ihr Leben zu verstehen, wenn sie hierfür mehrere aufeinander aufbauende Möglichkeiten zu verschiedenen Zeitpunkten erhalten. Diese gestuften Informations- und Entscheidungsarchitekturen ermöglichen einen Lernprozess.[32]

[32] Vgl. Prince, C., Omrani, N., Schiavone, F. Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe. Information Information Technology & People (2024) 37 (8): 1–24; Kumar, P.C. (2022). Toward a Practice-Based Approach to Privacy Literacy. In: Smits, M. (eds) Information for a Better World: Shaping the Global Future. iConference 2022. Lecture Notes in Computer Science(), vol 13192. Springer, Cham. https://doi.org/10.1007/978-3-030-96957-8_13.



Nach aktuellem Wissensstand stehen neben dem klassischen Cookie Banner grundsätzlich zwei weitere sogenannte Touchpoints[33] zur Verfügung, die dem klassischen Cookie Banner zeitlich einerseits vorangehen und andererseits nachfolgen:

- Zum einen sogenannte Einwilligungsagenten, die Informationen und Entscheidungen vor die Klammer ziehen, also vor der Nutzung des jeweiligen Dienstes ermöglichen.
- Zum anderen kontextualisierte Informations- und Interventionsmöglichkeiten, anhand derer Internetnutzer:innen jeweils im konkreten Nutzungskontext Informationen erhalten und/oder ihre Betroffenenrechte ausüben können (zum Beispiel im Wege der sogenannten kontextuellen Einwilligung).

Einwilligungsagenten, Einwilligungsverwaltungsdienste und Personal Information Management Services (PIMS)

Einem klassischen Cookie Banner zeitlich vorgelagerte Lösungen ermöglichen es Internetnutzer:innen, sich vorab an einer zentralen Stelle über wiederkehrende Datenanfragen zu informieren und entsprechende Voreinstellungen zu treffen. Solche Lösungen haben für Internetnutzer:innen im Wesentlichen drei Vorteile:

1. Internetnutzer:innen können sich zu einem Zeitpunkt *ihrer Wahl* über die Datenanfragen informieren; damit können sie sich mit deutlich mehr Aufmerksamkeit den Informationen widmen.
2. Internetnutzer:innen brauchen sich idealerweise nur einmal mit wiederkehrenden und dadurch ermüdenden Informationen auseinandersetzen und können sich dadurch beim Besuch einer Website bzw. bei der Nutzung eines Dienstes auf Abweichungen zu den typisierten Angaben konzentrieren.
3. Internetnutzer:innen können wiederkehrende und dadurch ermüdende Anfragen, in die Verwendung ihrer Daten einzuwilligen oder ihr zu widersprechen, ebenfalls durch

[33] Zum Begriff als Komponente einer umfassenderen User Journey Lemon, Katherine N. and Verhoef, P. C. (2016). Understanding Customer Experience Throughout the Customer Journey, in: Journal of Marketing, Vol. 80 (6), 2016, S. 69–96; Hassenzahl, M., Experience Design: Technology for All the Right Reasons. San Rafael (Morgan & Claypool Publishers) 2010.

Voreinstellungen vor die Klammer ziehen. Beim Besuch einer Website bzw. bei Nutzung des jeweiligen Dienstes können sie diese Voreinstellungen dann mit Blick auf die konkrete Situation des Dienstes anpassen.

Hier wird die Reputation des Dienstes bzw. das Vertrauen, das Internetnutzer:innen gegenüber einem Dienst haben, bzw. das konkret kommunizierte Datenschutzniveau entscheidend. Genießt der Dienst eine hohe Reputation bei den Internetnutzer:innen bzw. vertrauen diese in die Verarbeitung ihrer Daten durch den konkreten Dienst, etwa weil dieser sein überdurchschnittliches Datenschutzniveau überzeugend kommuniziert, kann dies die Wahrscheinlichkeit einer Zustimmung erheblich steigern.[34]

Wichtig ist, dass Internetnutzer:innen diese Anpassungen vornehmen können, aber nicht müssen. Nehmen Internetnutzer:innen innerhalb eines bestimmten Zeitraums keine Anpassungen vor, verschwindet die Schaltfläche von selbst. So wird das Problem der sogenannten Einwilligungsmüdigkeit behoben.[35]

Kontextualisierte Informations- und Interventionsmöglichkeiten (z.B. kontextualisierte Einwilligung)

Einem klassischen Cookie Banner zeitlich nachgelagerte Lösungen ermöglichen es Internetnutzer:innen, sich mit Blick auf eine konkrete Funktion oder einen Inhalt der Website, mit der oder dem sie jeweils interagieren, über die Datenverarbeitung zu informieren und entsprechende Entscheidungen zu treffen. Solche Lösungen haben für Internetnutzer:innen die folgenden wesentlichen Vorteile:

- Internetnutzer:innen verstehen durch die Kontextualisierung in den jeweiligen Nutzungskontext den konkreten Anlass der Datenerhebung besser und damit auch, wie weit die Verarbeitung geht und welche Folgen sie hat. Wenn zum Beispiel personenbezogene Daten erforderlich sind, um ein

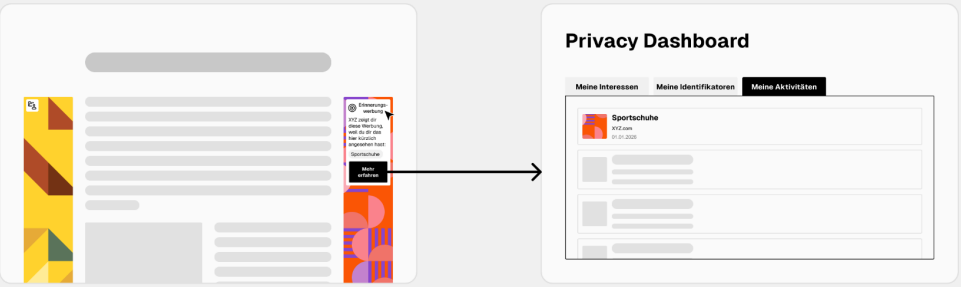
[34] Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).

[35] Zum Problem der Einwilligungsmüdigkeit mit Fokus auf Cookie Banner Nouwens, Midas et al. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence, in: CHI Conference on Human Factors in Computing Systems (CHI 2020); mit Fokus auf Datenschutzerklärungen McDonald, A. M., Cranor, L. F. (2008). The Cost of Reading Privacy Policies, in: I/S: A Journal of Law and Policy for the Information Society, Vol. 4 (3), 2008, S. 543–568.

Video abzuspielen, und Nutzer:innen das Video erst durch ihre Einwilligung freischalten, wird ihnen der Nutzen der Datenweitergabe direkt in diesem Moment verständlich – anders als beim bloßen Betreten einer Website. Wenn der Anbieter die Daten darüber hinaus auch für eigene Werbezwecke nutzen möchte, muss darauf hingewiesen werden. So können Nutzer:innen nachvollziehen, welche ihrer Daten von welchem Anbieter für Werbung verwendet werden und auf welche Weise dies geschieht (siehe dazu im Folgenden). Websitebetreiber kommen dieser Pflicht häufig nicht nach, auf die zusätzlichen Verarbeitungszwecke des Drittdienstes hinzuweisen. Stattdessen erfolgt häufig nur ein pauschaler Hinweis auf die Datenschutzerklärungen des jeweiligen Dienstes. Da diese Informationen jedoch für die Internetnutzer:in für ihre Entscheidung relevant sind, die Daten preiszugeben oder nicht, muss der Betreiber der Website bzw. des Dienstes auf diese zusätzlichen Zwecke des Drittanbieters unmittelbar hinweisen. Diese Zusammenhang werden im jeweiligen Kontext der Nutzung des jeweiligen Dienstes deutlich anschaulicher.

- Internetnutzer:innen verstehen auch ihre weiteren Betroffenenrechte besser, wenn diese im konkreten Nutzungskontext erklärt werden. Dazu gehören vor allem das Recht auf Auskunft, Berichtigung und Löschung ihrer Daten. Wenn ihnen zum Beispiel personalisierte Werbung angezeigt wird, sollte direkt dabei erklärt werden, auf welchen personenbezogenen Daten diese Werbung basiert. Konkret bedeutet das: Es sollte nachvollziehbar sein, welche Interessen die Werbeindustrie ihnen zuschreibt – und auf welchen Daten diese Annahmen beruhen. So können Nutzer:innen einschätzen, ob sie diese Datenverarbeitung für angemessen halten, ob die angenommenen Interessen ihren tatsächlichen Interessen entsprechen und ob sie die zugrunde liegenden Daten korrigieren oder löschen möchten.[36]

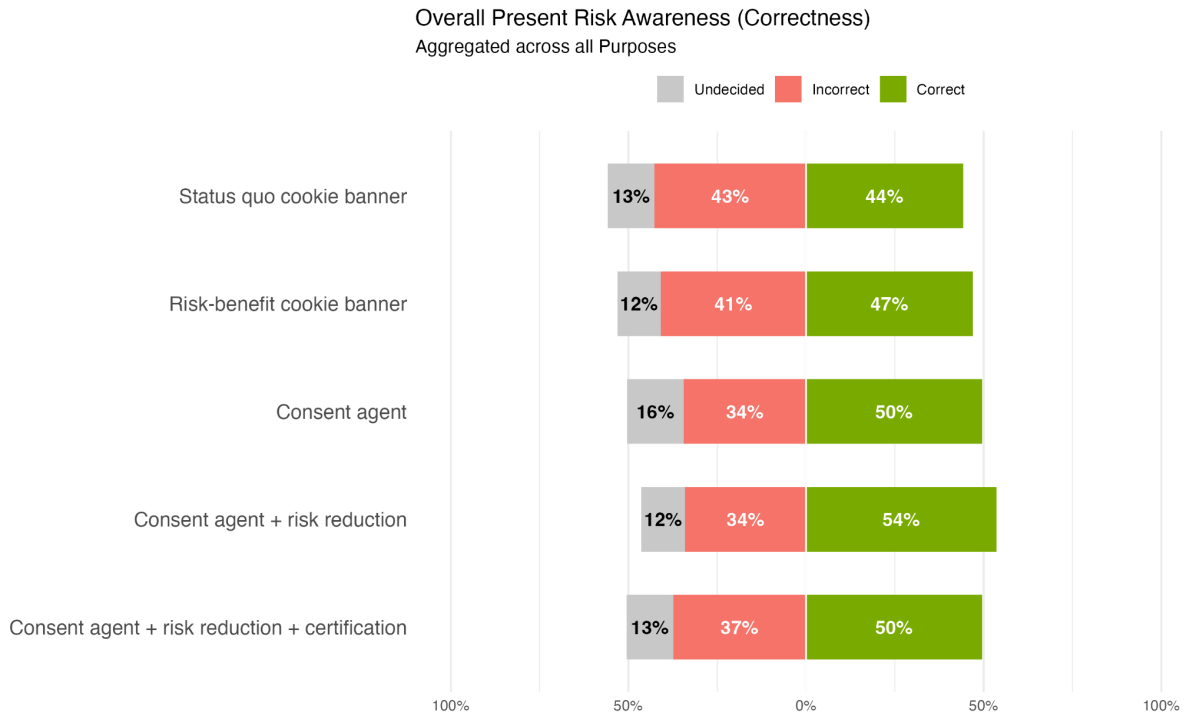
[36] Siehe grundlegend Smieskol, P., Jakobi, T., & von Grafenstein, M. (2025). From consent to control by closing the feedback loop: Enabling data subjects to directly compare personalized and non-personalized content through an On/Off toggle. Computer Law & Security Review, 59, 1-22. DOI: 10.1016/j.clsr.2025.106186.



Exkurs: Informiertheit gemäß einem quantitativen A/B/n-Test

Die Kombination der verschiedenen Touchpoints bildet zusammen einen Lernprozess, der bei Nutzer*innen zu deutlich höherer Informiertheit führt. Ein quantitativer A/B/n-Test aus dem Jahr 2024 ergab, dass vor allem die Einbindung von Einwilligungsagenten kombiniert mit Interaktionsmöglichkeiten der Internetnutzer:innen mit dem konkreten Dienst, in deren Verlauf sie weitere Informationen zum konkreten Datenschutzniveau des Dienstes erhalten und Anpassungen ihrer Voreinstellungen vornehmen können, zu einer deutlich höheren Informiertheit führt als bisherige Banner.[37]

[37] Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at https://zenodo.org/records/19332894; siehe in größerem Detail Gerber, N., Grassl, P. und v. Grafenstein, M. From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates (in review).



Dabei sei darauf hingewiesen, dass es sich bei den dieser Studie zugrunde liegenden Designs um noch nicht ausgereifte Konzept-Designs handelte (siehe Annex 1). Gleiches gilt für die kontextualisierte Einbettung der weiteren Betroffenenrechte, insbesondere in Bezug auf personalisierte Werbung oder andere personalisierte Inhalte, wo noch keine ausreichenden Studien existieren, die die Auswirkungen nutzungsfreundlicher Umsetzungen auf die Informiertheit untersuchen.[38]

Hier besteht noch erheblicher Spielraum, den Stand der Technik weiter zu entwickeln und die Informiertheit deutlicher zu steigern.

3.4 Granularität der Auswahl / Ausgestaltung der Schaltflächen

Die Kombination klassischer Cookie Banner mit Einwilligungsagenten ermöglicht auch weitere Spielräume bei der Ausgestaltung der Schaltflächen. Nach aktuellen Best Practice-Regeln sind Cookie Banner (meist) wie folgt gestaltet:[39]

- Auf der ersten visuellen Ebene werden alle Verarbeitungszwecke aufgelistet, bei denen Internetnutzer:innen eine Entscheidung treffen können.

[38] Siehe hierzu auch das laufende Forschungsprojekt "Sicher im Datenverkehr" (SiD), https://sid-projekt.de/.

[39] Vgl. abgesehen von einzelnen Abweichungen Good Practice Initiative for Cookie Banner Consent Management – Design Guidelines unter https://hdr4.bmj.de/SharedDocs/Publikationen/EN/Cookie_guidelines.pdf?__blob=publicationFile&v=3

WICHTIG: Anders als in den Design Guidelines der Good Practice Initiative for Cookie Banner Consent Management vertreten, müssen diese Zwecke bereits auf der ersten visuellen Ebene einzeln entscheidbar sein. Die Auflistung solcher Zwecke auf einer hinteren Ebene stellt ein Dark Pattern dar, weil es eine granulare Entscheidung für die Betroffenen schwieriger macht.

- Verarbeitungszwecke, die keine Entscheidung von Internetnutzer:innen erfordern, dürfen nicht auf der ersten visuellen Ebene angezeigt werden, da sie Internetnutzer:innen von den wesentlichen Entscheidungsmöglichkeiten ablenken.
- Auf der ersten visuellen Ebene sind nicht nur Verarbeitungszwecke aufzulisten, die eine Einwilligung (Opt-In) erfordern, sondern auch Zwecke, denen Internetnutzer:innen widersprechen können (Opt-Out).

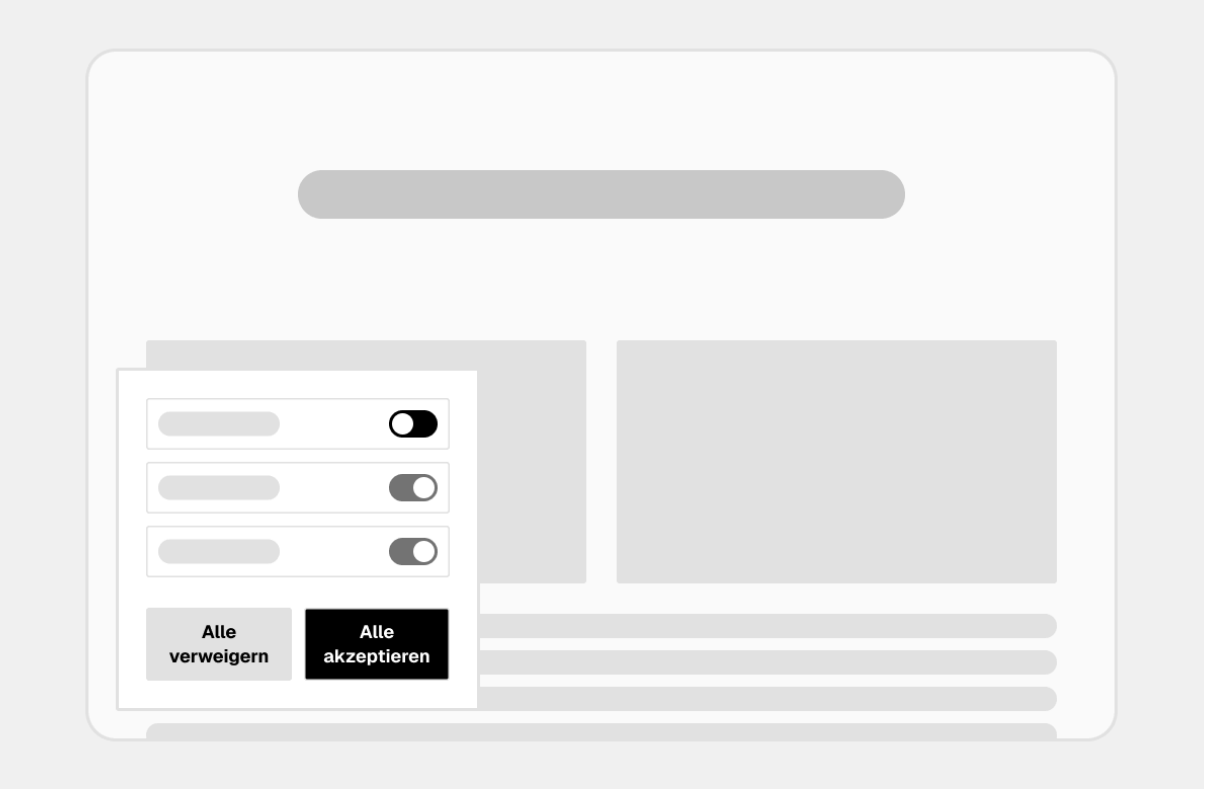
  WICHTIG: Die Darstellung solcher Opt-Out-Zwecke auf einer hinteren Ebene stellt ein Dark Pattern dar, weil es für Internetnutzer:innen eine Entscheidung schwieriger macht und daher weniger wirksam ist.

- Je nach gesetzlicher Vorgabe, muss die Schaltfläche für den jeweiligen Verarbeitungszweck per Voreinstellung ausgeschaltet (Opt-In) oder darf sie eingeschaltet (Opt-Out) sein.

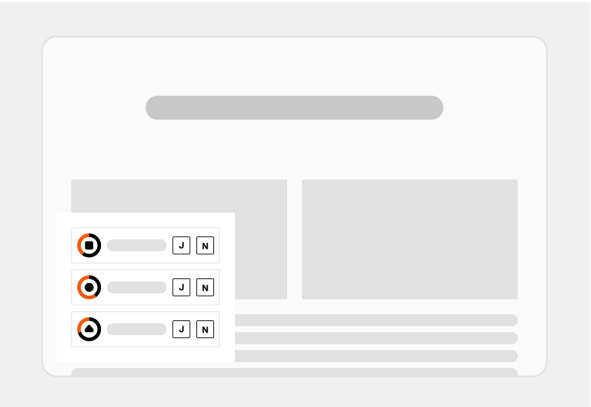
  WICHTIG: Eine neutrale Grundposition der Schaltfläche stellt solange ein Dark Pattern dar, wie Internetnutzer:innen diese Entscheidungen nicht mithilfe eines Einwilligungsagenten vor die Klammer ziehen können, weil es zusätzliche Klicks erfordert und somit das Problem der Einwilligungsmüdigkeit befördert. Auch das ist ein Punkt, der in aktuellen Best Practice Guidelines häufig übersehen wird.

- Zusätzlich zu den granularen Einstellungen müssen auf der ersten visuellen Ebene jeweils eine Schaltfläche für “Alles akzeptieren” und “Alles Ablehnen” angeboten werden. Diese Schaltflächen sind notwendig, um das Problem der Einwilligungsmüdigkeit zu reduzieren, solange Internetnutzer:innen granulare Entscheidungen nicht mithilfe eines Einwilligungsagenten vor die Klammer ziehen können.
- Alle Schaltflächen sind neutral bzw. gleichartig auszugestalten, so dass sie Internetnutzer:innen aufgrund ihres Designs nicht dazu animieren, eher auf “(Alles) Akzeptieren" oder eher auf “(Alles) Ablehnen” zu klicken.

  WICHTIG: Egal ob die Ausgestaltung von Schaltflächen das Abgeben der Einwilligung leichter als das Verweigern der Einwilligung macht oder (!) umgekehrt, beide Priorisierungen stellen ein Dark Pattern dar, weil es im Datenschutzrecht nicht darum geht, die Preisgabe von Daten schwerer als das Zurückhalten von Daten zu machen, sondern informierte Entscheidungen zu ermöglichen, egal welche Position die Betroffenen dabei einnehmen mögen.



Durch die Einbindung von Einwilligungsagenten entstehen zusätzliche Möglichkeiten beim Design der Schaltflächen: Da Internetnutzer:innen mithilfe von Einwilligungsagenten in der Lage sind, Entscheidungen vor die Klammer zu ziehen und damit das Problem der Einwilligungsmüdigkeit zu lösen, können und müssen die Schaltflächen sowohl im Einwiligungsagenten als auch in einem Cookie Banner, das Einwilligungsagenten einbindet, granular ausgestaltet werden. Diese granulare Ausgestaltung stellt sicher, dass Internetnutzer:innen zumindest einmalig Entscheidungen für die verschiedenen Datenverarbeitungszwecke treffen.



Dementsprechend zielen die folgenden Design-Vorgaben darauf ab, dass Internetnutzer:innen granulare Entscheidungen treffen:

- Die Schaltflächen sowohl im Einwilligungsagenten als auch im Cookie Banner dürfen keine Möglichkeit enthalten, alle Verarbeitungszwecke pauschal anzunehmen oder abzulehnen. Internetnutzer:innen müssen also granular, das heißt, für jeden einzelnen Zweck entscheiden.

- Die Schaltflächen sowohl im Einwilligungsagenten als auch im Cookie Banner müssen per Voreinstellung auf einer neutralen Grundposition stehen. Internetnutzer:innen müssen also aktiv entscheiden, ob sie in einen Verarbeitungszweck einwilligen oder ihm widersprechen.

WICHTIG: Diese Design-Vorgaben stehen unter der Bedingung, dass Internetnutzer:innen diese Entscheidungen mit Hilfe eines Einwilligungsagenten vor die Klammer ziehen können. Denn nur so wird das Problem vermieden, dass diese Vorgaben andernfalls mehr Klicks erfordern und damit das Problem der Einwilligungsmüdigkeit erschweren. Da Internetnutzer jedoch mithilfe eines Einwilligungsagenten eine Standardeinstellung festlegen können, die für alle Websites gilt, stellen diese Design-Vorgaben sicher, dass Internetnutzer zumindest einmal eine Entscheidung zu den verschiedenen Datenverarbeitungszwecken treffen. Vorausgesetzt, Internetnutzer:innen können mit Hilfe eines Einwilligungsagenten diese Entscheidungen vor die Klammer ziehen, stellen diese Vorgaben kein Dark Pattern dar. Im Gegenteil gewährleisten sie, dass Internetnutzer:innen informierte, bewusste und granulare Entscheidungen treffen.[40]

Auch hier dürfte es weiteres Entwicklungspotenzial hinsichtlich des aktuellen Stands der Technik geben. Sollte sich zeigen, dass eine andere Konzeption noch fundiertere und bewusstere Entscheidungen auf granularer Ebene ermöglicht, wird das den neuen Stand der Technik bei der Umsetzung der informierten Einwilligung darstellen.

Exkurs: Einwilligungsraten gemäß einem quantitativen A/B/n-Test

Auch wenn es datenschutzrechtlich irrelevant ist, soll hier kurz auf die Auswirkungen der vorgestellten Stand der Technik-Designs auf die Einwilligungsraten eingegangen werden, da dies für viele Website-Betreiber in praktischer Hinsicht sehr wichtig ist:

Bei aktuellen Best Practice-Cookie Bannern führen die granularen Einstellungsmöglichkeiten häufig zu einer Reduzierung der Einwilligungsrate. Hintergrund ist, dass die granularen Einstellungsmöglichkeiten Internetnutzer:innen vermutlich überfordern.[41] Dagegen führt die Einbindung von Einwilligungsagenten nicht automatisch zu einer Reduzierung der Einwilligungsrate. Vielmehr kann die Einwilligungsrate sogar höher ausfallen im Vergleich zu Best Practice-Cookie Bannern. Es kommt dabei entscheidend darauf an, wie die Entscheidungsmechanismen konkret gestaltet werden (siehe im Detail sogleich).

Dieser Hinweis ist wichtig, weil mit Verweis auf die Einführung von Apple's App Tracking Transparency Framework in der Wirtschaft befürchtet wird, dass die Einwilligungsraten mit der Einführung von

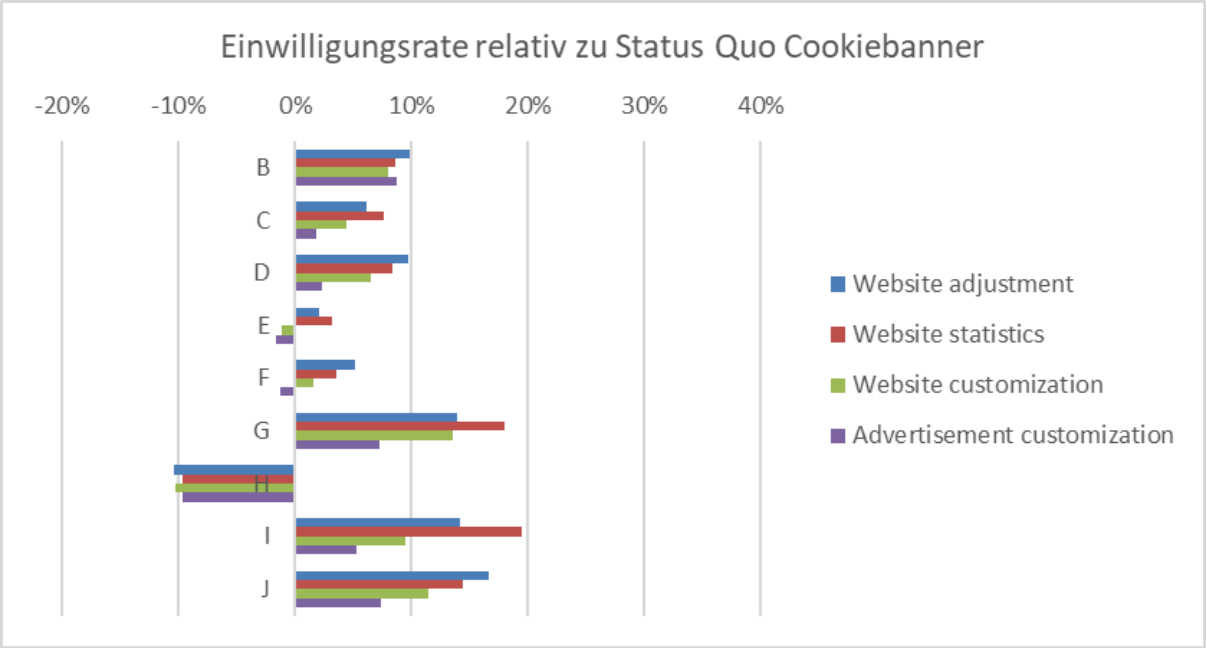
---

[40] Siehe zur Unterscheidung von Dark Patterns und neutralen bzw. unterstützenden Schaltflächen bei Grafenstein, M. v., Hölzel, J., Irgmaier, F. & Pohle, J. (2018). Nudging: Regulierung durch Big Data und Verhaltenswissenschaften, verfügbar unter https://idw-online.de/de/attachmentdata66585.pdf.

[41] Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, Proceedings of CHI '20 CHI Conference on Human Factors in Computing Systems, April 25--30, 2020.

Einwilligungsagenten fallen.[42] Werden Einwilligungsprozesse unter Bedingungen gestaltet, die hier vorgegeben werden, führt die Einbindung von Einwilligungsagenten in der Regel zu einer Erhöhung der Einwilligungsrate (siehe die Studiengruppen G und D in Annex II). Dies zeigt die nachfolgende Tabelle einer quantitativen Langzeit-Feldstudie.

Auch hier gibt es voraussichtlich noch weiteres Fortentwicklungspotential für den Stand der Technik. Sollte nachgewiesen werden, dass eine andere Ausgestaltung noch informativere und bewusstere granulare Entscheidungen ermöglicht, wird diese den neuen Stand der Technik darstellen.



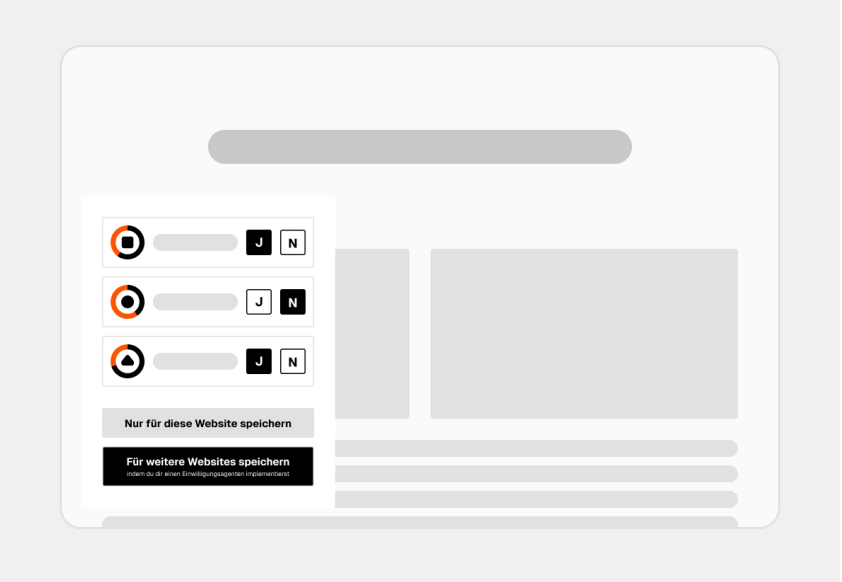
3.5 Gegenseitige Einbindung der verschiedenen Touchpoints

Damit Internetnutzer:innen wirksam informiert werden, dass sie Entscheidungen über die Verarbeitung ihrer Daten in einem Einwilligungsagenten bündeln können, sollten sie in einem passenden Nutzungskontext darauf hingewiesen werden. Der passende Nutzungskontext ist der Augenblick, in dem Internetnutzer:innen das größte Bedürfnis nach einem Einwilligungsagenten haben. Das heißt, beim An- oder Wegklicken eines Cookie Banners.

Cookie Banner müssen daher zwei Schaltflächen enthalten: über die Internetnutzer:innen ihre Entscheidungen für die einzelnen Verarbeitungszwecke nur für den jeweils genutzten Dienst speichern

[42] Siehe verschiedene Aussagen der Werbewirtschaft zu Art. 88b (und a) Digitaler Omnibus, zum Beispiel, https://www.aig-europe.eu/wp-content/uploads/2026/03/AIG-Digital-Simplification-Position-Paper.pdf https://ecommerce-europe.eu/wp-content/uploads/2026/03/Annex-2-ECOM-Final-Position-Paper-Digital-Omnibus.pdf

können; oder zusätzlich als Voreinstellung auch für alle anderen Websites bzw. digitalen Dienste, indem sie sich einen Einwilligungsagenten über den in der zweiten Schaltfläche hinterlegten Link herunterladen. Dieser Link muss zu einer Website führen, auf der alle verfügbaren Einwilligungsagenten gelistet sind.



Idealerweise klärt der Gesetzgeber, welche zuständige Behörde die Website mit den Links zu den verfügbaren Einwilligungsagenten betreibt und welche Voraussetzungen Einwilligungsagenten erfüllen müssen, um gelistet zu werden.

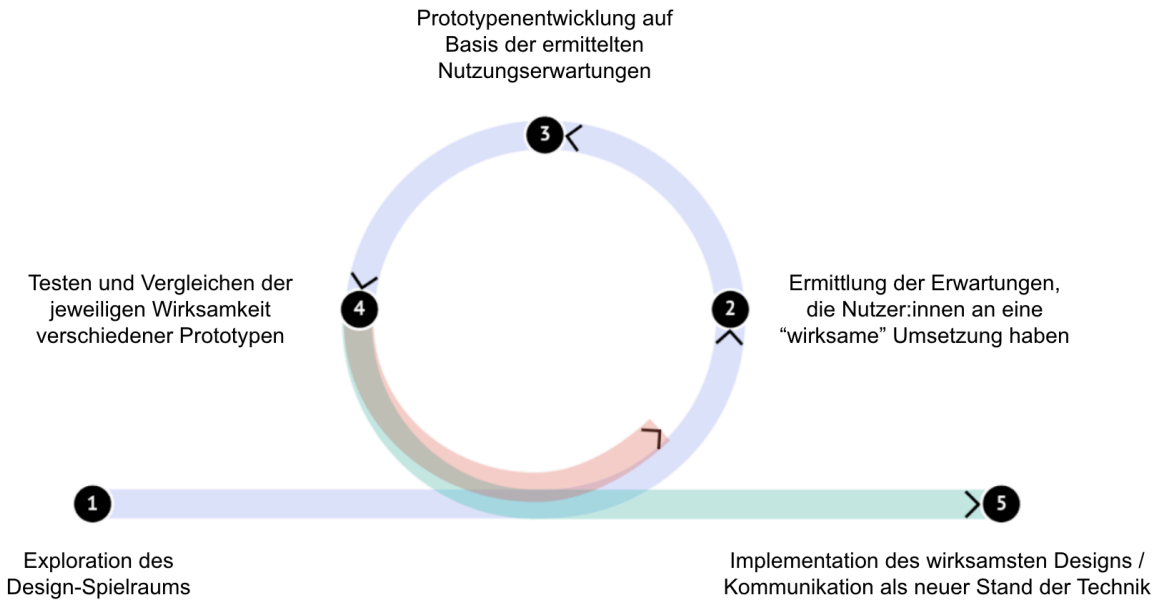
4 EMPIRISCHE METHODEN ZUM NACHWEIS WIRKSAMER ENTSCHEIDUNGSMECHANISMEN

Im vorherigen Kapitel wurden immer wieder Bereiche hervorgehoben, in denen mit einer weiteren Fortentwicklung des Stands der Technik zu rechnen ist. Die dargestellten Designvorgaben stellen nach heutigem Wissensstand zwar die aktuell wirksamste Umsetzung der informierten Einwilligung sowie anderer Entscheidungen und damit den Stand der Technik dar. Es sind aber noch wirksamere Gestaltungen erwartbar. Für die Entwicklung noch wirksamerer Entscheidungsprozesse kann folgender iterativer Designprozess beschritten werden.

4.1 Iterativer Designprozess

Der Prozess zur Gestaltung immer wirksamerer Entscheidungsprozesse lässt sich dabei in fünf grundsätzliche Schritte gliedern.[43]

[43] Im Einzelnen siehe Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924.



Im ersten Schritt sind die Rahmenbedingungen für die Designoptionen zu bestimmen. Hierzu gehören die visuellen Rahmenbedingungen, die der jeweilige Nutzungskontext setzt, in dem Internetnutzer:innen informiert werden und entscheiden sollen (also zum Beispiel im Rahmen eines Cookie Banners oder eines Einwilligungsagenten); die rechtlichen Anforderungen, die das Gesetz vorgibt; sowie der Stand der Technik, soweit es einen solchen bereits gibt.

Gibt es noch keinen Stand der Technik, muss der Verantwortliche nachweisen, dass seine spezifische Umsetzung der informierten Einwilligung im Sinne von Artikel 25 DSGVO wirksam ist (ein Nachweis, der bislang kaum erbracht wird). Gibt es eine Lösung nach dem Stand der Technik, erleichtert dies dem Verantwortlichen die Sache erheblich, da er diese einfach nachbilden (oder erwerben) kann. Alternativ kann der Verantwortliche den Stand der Technik auch selbst verbessern. Im ersten und letzten Fall benötigt er Methoden, um die (größere) Wirksamkeit nachzuweisen. Die folgende kurze Darstellung der möglichen Methoden mag ihm dabei helfen.

4.2 Maßstab: Es geht um den wirksamen Schutz vor den Risiken der Datenverarbeitung für die Grundrechte der Nutzer

Zunächst muss der Maßstab festgelegt werden, anhand dessen die Wirksamkeit gemessen werden kann. Wie bereits erläutert, verlangt Art. 25 DSGVO in Verbindung mit den jeweiligen Vorschriften zur Einwilligung, zum Widerruf und zum Widerspruch, dass diese Möglichkeiten einen wirksamen Schutz vor den Risiken der Datenverarbeitung für die *Grundrechte* der Internetnutzer:innen gewährleisten. Der Maßstab lässt sich damit in zwei grundsätzliche Komponenten aufteilen:

- Die Umsetzung muss zu einem wirksamen Schutz vor den jeweiligen Grundrechtsrisiken der

jeweiligen Datenverarbeitung führen.
- Dieser wirksame Schutz muss durch die Ermöglichung informierter und bewusster Entscheidungen für die jeweiligen Verarbeitungszwecke erreicht werden.

In einem ersten Schritt sind also für jeden Verarbeitungszweck und das hierfür eingesetzte Verfahren die Grundrechtsrisiken zu ermitteln. Hierauf kann auf die gängigen Methodologien des Datenschutzrisikoprüfung bzw. der Datenschutzfolgenabschätzung zurückgegriffen werden (vgl. bereits oben Punkt 3.1). Anhand der so zugeordneten Risiken ist sodann zu messen, ob die jeweilige Implementierung der informierten Einwilligung oder einer anderen Entscheidung zu einem wirksamen Schutz vor diesen Grundrechtsrisiken führt.

Da die richtige Zuordnung und Gewichtung entscheidend für die Wirksamkeit der Schutzmaßnahmen ist, sollte dieser Zuordnungsprozess durch entsprechende Methoden abgesichert werden. Ideal ist die Durchführung eines Multi-Stakeholder-Prozesses, der neben Laien auch Expert:innen involviert, die in verschiedenen Bereichen mit den Datenverarbeitungspraktiken befasst sind, insb. im Daten- und Verbraucherschutz sowie in den verschiedenen – gegebenenfalls untereinander konkurrierenden – Wirtschaftszweigen (siehe bereits oben Punkt 3.1).

Wie bereits erwähnt entsprechen die Grundrechtsrisiken weitgehend den Risikokategorien, die sich auch Laien in Bezug auf eine für sie ungünstige Verwendung ihrer Daten machen. Dieser Gleichlauf bildet eine wichtige Schnittstelle, um mit weitergehenden Nutzer:innenstudien zu ermitteln, wie Schutzmaßnahmen möglichst wirksam ausgestaltet werden können.[44] Die folgenden Kapitel fassen die möglichen Methoden in drei grundsätzliche Kategorien zusammen.

4.3 Qualitative Studien: Wieso, wofür – und wie?

Für die Entwicklung wirksamer Schutzmaßnahmen ist der Einsatz qualitativer Forschungsmethoden besonders geeignet, da sie ein tiefgehendes Verständnis der Wahrnehmungen, Entscheidungsprozesse und tatsächlichen Verhaltensweisen von Internetnutzer:innen ermöglichen. Dies ist insbesondere vor dem Hintergrund des vielfach belegten sogenannten Privacy Paradox relevant, wonach geäußerte Datenschutzbedenken und tatsächliches Verhalten häufig auseinanderfallen.[45] Die Disziplinen insbesondere der Mensch-Maschine-Interaktion, Psychologie und Verhaltensökonomie halten hierfür ein reiches Methodenset bereit.

[44] Grafenstein, M. v., Jakobi, T., & Stevens, G. (2021). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods. Computer Law & Security Review, 46. DOI: 10.1016/j.clsr.2022.105722.

[45] Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information, in: Science, Vol. 347, No. 6221, 2015, S. 509–514; Kokolakis, S. (2017). Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon, in: Computers & Security, Vol. 64, 2017, S. 122–134.

Eine zentrale Rolle spielen dabei leitfadengestützte Interviews, mit deren Hilfe individuelle Einstellungen, Sorgen und Abwägungsprozesse im Umgang mit personenbezogenen Daten exploriert werden können. Sie erlauben es, subjektive Bedeutungszuschreibungen und das oft komplexe Verhältnis zwischen Datenschutzbewusstsein und tatsächlichem Verhalten differenziert zu erfassen.[46] Gerade im Kontext des „Privacy Calculus" zeigen solche Studien, wie Nutzer:innen Nutzen und Risiken gegeneinander abwägen.[47] Ergänzend dazu liefern Gruppendiskussionen wertvolle Einblicke in kollektive Deutungsmuster und soziale Normen. In ihnen wird sichtbar, wie Nutzer:innen gemeinsam über Datenschutz sprechen, Argumente austauschen und Positionen entwickeln. Dies ist insbesondere relevant, da Privacy-Entscheidungen stark durch soziale Kontexte und Erwartungen geprägt sind.[48]

Um das tatsächliche Verhalten im Alltag zu verstehen, sind ethnografische Ansätze und Kontextstudien von großer Bedeutung. Durch die Beobachtung der Nutzung digitaler Dienste in realen Anwendungssituationen lassen sich Diskrepanzen zwischen geäußerten Einstellungen und tatsächlichem Handeln identifizieren. Solche Einsichten sind essentiell, um Maßnahmen zu entwickeln, die nicht nur theoretisch überzeugen, sondern auch praktisch wirksam sind.[49] Eine zeitliche Dimension bringen Tagebuchstudien ein, bei denen Teilnehmende ihre Erfahrungen und Entscheidungen im Umgang mit Datenschutz über einen längeren Zeitraum dokumentieren. Auf diese Weise können Lernprozesse, Gewöhnungseffekte und situative Einflussfaktoren nachvollzogen werden. Gerade für die Gestaltung nachhaltiger Privacy-Interventionen ist dieses Verständnis von Entwicklungsverläufen zentral.[50]

Schließlich ermöglichen Think-Aloud-Studien einen unmittelbaren Einblick in kognitive Prozesse während konkreter Interaktionen, etwa bei der Nutzung von Cookie Bannern oder Privatsphäre-Einstellungen. Indem Nutzer:innen ihre Gedanken während der Anwendung laut äußern, werden Missverständnisse, Unsicherheiten und Entscheidungslogiken sichtbar, die für die Gestaltung

---

[46] Cranor, L. F. (2012). Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, in: Journal on Telecommunications and High Technology Law, Vol. 10, 2012, S. 273–307; Nissenbaum, Helen (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford (Stanford University Press) 2010.

[47] Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, in: Information Systems Research, Vol. 17, No. 1, 2006, S. 61–80.

[48] Nissenbaum, Helen (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford (Stanford University Press) 2010; Boyd, D. and Hargittai, E. (2010). Facebook Privacy Settings: Who Cares?, in: First Monday, Vol. 15, No. 8, 2010.

[49] Shilton, K. (2009). Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection, in: Communications of the ACM, Vol. 52, No. 11, 2009, S. 48–53; Barkhuus, L. and Dey, A.K. (2003). Is Context-Aware Computing Taking Control Away from the User? Three Levels of Interactivity Examined, in: Proceedings of the Fifth International Conference on Ubiquitous Computing (UbiComp 2003), Berlin/Heidelberg (Springer) 2003, S. 149–156.

[50] Vgl. Carter, S. and Mankoff, J. (2005). When Participants Do the Capturing: The Role of Media in Diary Studies, in: CHI 2005 Proceedings; Shilton, K. (2009). Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection, in: Communications of the ACM, Vol. 52, No. 11, 2009, S. 48–53.

nutzerfreundlicher und transparenter Privacy-Interfaces berücksichtigt werden müssen.[51]

Je nach konkreter Forschungsfrage sollte das jeweilige qualitative Studiendesign gewählt werden. In der Kombination dieser Methoden entsteht ein umfassendes Bild, das sowohl individuelle als auch soziale, situative und zeitliche Aspekte des Nutzerverhaltens abdeckt. Eine solche methodische Triangulation ist zu empfehlen, wenn die Komplexität von Datenschutzentscheidungen möglichst holistisch erfasst werden soll. Es ist jedoch klarzustellen, dass bereits einzelne Methoden und Studien wertvolle Beiträge zu einer evidenzbasierten, wirksamen Maßnahmenentwicklung liefern.[52] Es ist dann eine andere Frage, wie verlässlich und umfassend der jeweilige Nachweis ist. Daher ist stets vom jeweils aktuellen Wissensstand auszugehen und auf dieser Basis kann der Nachweis für eine wirksame Schutzmaßnahme durch die Hinzuziehung weiterer Studien und Methoden verlässlicher und/oder umfassender gemacht werden. Bei der Durchführung empirischer Studien geht es also nicht um die Frage des ob, sondern des wie bzw. mit welchem Schritt man anfängt.

4.4 Prototyping: Designoptionen für das "wie?"

Auf Grundlage der ermittelten Erwartungen an einen wirksamen Schutz sollten verschiedene Prototypen entwickelt werden. Hierfür kann auf das Methodenset vor allem aus dem User Experience Design und User Interface Design zurückgegriffen werden.

Prototyping-Verfahren ermöglichen es, datenschutzbezogene Gestaltungsansätze frühzeitig zu testen, zu evaluieren und iterativ zu verbessern. Sie dienen dazu, abstrakte rechtliche Anforderungen in konkrete, nutzer:innenzentrierte Lösungen zu überführen.[53] Im Kontext von Datenschutz wird Prototyping häufig eingesetzt, um insbesondere **Privacy Interfaces** – etwa Einwilligungsdialoge, Cookie Banner oder Dashboard-Lösungen – zu entwickeln und deren Verständlichkeit sowie Entscheidungswirkungen empirisch zu überprüfen. Frühphasige Prototypen (Low-Fidelity), etwa in Form von Wireframes oder Klickdummys, erlauben es, unterschiedliche Gestaltungsvarianten mit Nutzerinnen und Nutzern zu testen, ohne bereits vollständige Systeme implementieren zu müssen. Spätere, funktionsnahe Prototypen (High-Fidelity) ermöglichen darüber hinaus die Untersuchung tatsächlicher Interaktionsprozesse unter realistischen Bedingungen.[54]

Empirische Studien zeigen, dass bereits kleine Designentscheidungen in solchen Prototypen erhebliche

---

[51] Vgl. Ericsson, K. A. and Simon, H. A. (1993). Protocol Analysis: Verbal Reports as Data, 2. Aufl., MIT Press; Nielsen, J. (1993). Usability Engineering, Academic Press.

[52] EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 7.

[53] Schaub, F., Balebako, R., Cranor, L. F. (2017). Designing Effective Privacy Notices and Controls, in: IEEE Internet Computing, Vol. 21, No. 3, 2017, S. 70–77.

[54] Snyder, C. (2003). Paper Prototyping: The Fast and Easy Way to Design and Refine User Interfaces, San Francisco (Morgan Kaufmann) 2003.

Auswirkungen auf das Nutzerverhalten haben können. Wie oben bereits geschildert, konnte gezeigt werden, dass die konkrete Gestaltung von Privacy Notices und Einwilligungsmechanismen die Bereitschaft zur Datenfreigabe signifikant beeinflusst.[55] Auch Untersuchungen zu sogenannten „Dark Patterns" verdeutlichen, dass prototypische Interface-Gestaltung nicht nur zur Verbesserung von Transparenz, sondern auch – missbräuchlich – zur gezielten Beeinflussung von Nutzerentscheidungen eingesetzt werden kann.[56] Gerade deshalb ist ein evidenzbasierter Prototyping-Ansatz entscheidend, um wirksame und zugleich faire Datenschutzmaßnahmen zu entwickeln. Durch die Entwicklung alternativer Prototypen lässt sich die jeweilige Wirksamkeit relativ rasch ermitteln und vergleichen.

Insgesamt zeigt die Forschung, dass Prototyping ein unverzichtbares Instrument für die Entwicklung wirksamer Datenschutzmaßnahmen ist. Es erlaubt nicht nur die frühzeitige Identifikation von Verständlichkeitsproblemen und Fehlanreizen, sondern auch die systematische Optimierung von Gestaltungslösungen im Sinne einer evidenzbasierten Regulierung und Umsetzung von Datenschutzrecht. Das Prototyping ist also nicht als reine Umsetzung der Erwartungen der Nutzer:innen im Rahmen des ermittelten Design-Spaces zu verstehen. Vielmehr stellt das Prototyping eine Methode zur weiteren Wissensgenerierung dar. Häufig fällt einem erst im Prototyping auf, wo das Problem konkret verwurzelt ist, wo die Herausforderungen bei der Umsetzung liegen und welche alternativen, wirksameren Lösungen es gibt, an die man zuvor nicht gedacht hatte.

Die entwickelten Gestaltungsoptionen sind stets mit qualitativen Methoden auf ihre Wirksamkeit zu testen. Hierfür sei auf den vorhergehenden Abschnitt zurückverwiesen. Diese qualitativen Test- und Entwicklungszyklen sind solange zu wiederholen, bis mindestens eine qualitativ hinreichend abgesicherte wirksame Umsetzungsoption vorliegt. Dieses Modell dient dann als Hypothese für den quantitativen Test, der die Wirksamkeit auf einer repräsentativen Basis validiert.

4.5 Quantitative A/B/n-Tests: Was ist das wirksamste Design?

Aufbauend auf den entwickelten und qualitativ getesteten Prototypen kommen in der Privacy-Forschung **quantitative Methoden** zum Einsatz, um unterschiedliche Gestaltungsvarianten systematisch zu vergleichen und das jeweils wirksamste Design empirisch zu identifizieren. Ziel ist es, die in explorativen Studien gewonnenen Hypothesen unter kontrollierten Bedingungen zu überprüfen und belastbare Aussagen über kausale Wirkzusammenhänge zwischen Designentscheidungen und Nutzerverhalten zu treffen.

---

[55] Tsai, J. Y., Egelman, S., Cranor, L. F., Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior, in: Information Systems Research, Vol. 22, No. 2, 2011, S. 254–268.

[56] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI 2018); Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L. (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 (CHI 2020).

Eine zentrale Methode sind hierbei **randomisierte kontrollierte Experimente (Randomized Controlled Trials)**, insbesondere in Form von A/B-Tests oder multivariaten Experimenten. Nutzer:innen werden zufällig verschiedenen Designvarianten – etwa unterschiedlichen Cookie Bannern – zugewiesen, sodass Unterschiede im Verhalten kausal auf die jeweilige Gestaltung zurückgeführt werden können. Solche Ansätze sind in der Privacy-Forschung weit verbreitet und haben gezeigt, dass bereits geringfügige Änderungen in der Darstellung oder Voreinstellung erhebliche Effekte auf Einwilligungsraten und Datenoffenlegung haben können.[57] Ergänzend verdeutlichen ökonomische Feldstudien die Bedeutung realer Nutzungskontexte für die Bewertung solcher Effekte.[58]

Ergänzend werden **Online-Experimente und Survey-Experimente** eingesetzt, um größere Stichproben zu erreichen sowie spezifische Einflussfaktoren isoliert zu untersuchen. In solchen Studien können etwa unterschiedliche Informationsdarstellungen, Framing-Effekte oder Default-Einstellungen variiert und deren Einfluss auf Entscheidungsprozesse gemessen werden. Die Forschung zeigt, dass Faktoren wie Framing, Timing und Kontext der Informationsbereitstellung signifikante Auswirkungen auf Privacy-Entscheidungen haben.[59] Auch sogenannte Discrete-Choice-Experimente erlauben es, die Präferenzen von Nutzerinnen und Nutzern für verschiedene Datenschutzmerkmale quantitativ zu modellieren.[60]

Darüber hinaus gewinnen großangelegte Analysen zunehmend an Bedeutung, insbesondere im Kontext von Plattformen und digitalen Diensten. Diese erlauben es, Designentscheidungen mit sehr großen Nutzergruppen zu testen und auch längerfristige Effekte zu beobachten, etwa im Hinblick auf Nutzerbindung, Vertrauen oder nachhaltige Verhaltensänderungen.[61] Gleichzeitig wird in der Forschung betont, dass solche Experimente sorgfältig gestaltet werden müssen, um ethischen Anforderungen – insbesondere im Hinblick auf informierte Einwilligung und Transparenz – gerecht zu werden.

---

[57] Adjerid, I., Acquisti, A., Brandimarte, L., Loewenstein, G. (2013). Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, in: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS), 2013; Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field, in: Proceedings on Privacy Enhancing Technologies (PoPETs), 2019(1), S. 346–367; Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L. (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 (CHI 2020).

[58] Goldfarb, A. and Tucker, C. (2012). Privacy and Innovation, in: Innovation Policy and the Economy, Vol. 12, 2012, S. 65–90.

[59] Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information, in: Science, Vol. 347, No. 6221, 2015, S. 509–514; Johnson, E. J., Bellman, S., Lohse, G. L. (2002). Defaults, Framing and Privacy: Why Opting In-Opting Out, in: Marketing Letters, Vol. 13, No. 1, 2002, S. 5–15.

[60] Beresford, A. R., Kübler, D., Preibusch, S. (2012). Unwillingness to Pay for Privacy: A Field Experiment, in: Economics Letters, Vol. 117, No. 1, 2012, S. 25–27.

[61] Goldfarb, A., Tucker, C. (2012). Privacy and Innovation, in: Innovation Policy and the Economy, Vol. 12, 2012, S. 65–90.

Insgesamt ermöglichen quantitative Methoden eine systematische, evidenzbasierte Bewertung unterschiedlicher Privacy-Designs und bilden damit eine unverzichtbare Ergänzung zu qualitativen Ansätzen.[62] Während qualitative Methoden Hypothesen generieren und Kontextverständnis schaffen, liefern quantitative Experimente die notwendige empirische Grundlage, um Designentscheidungen zu validieren und regulatorische Anforderungen in nachweislich wirksame Maßnahmen zu übersetzen. Auf ihrer Basis lassen sich verschiedene Designoptionen vergleichen und die wirksamste Schutzmaßnahme verlässlich ermitteln.

Auch hier ist klarzustellen, dass einzelne quantitative Methoden und Studien wertvolle Beiträge zu einer evidenzbasierten, wirksameren Maßnahmenentwicklung liefern.[63] Auch hier ist es eine andere Frage, wie verlässlich und umfassend der jeweilige Nachweis ist. Daher ist auch hier vom jeweils aktuellen Wissensstand auszugehen. Auf dieser Basis kann der Nachweis für eine wirksame Schutzmaßnahme durch die Hinzuziehung weiterer quantitativer Studien und Methoden noch verlässlicher oder umfassender gemacht werden.

5 AUSBLICK: DIE ENTWICKLUNG DES STANDS DER TECHNIK ZU (IMMER) WIRKSAM(ER)EN DESIGNS

Diese Ausführungen geben einen Überblick über das vielfältige Methodenset, mit dem sich eine wirksame Umsetzung der informierten Einwilligung und anderer Entscheidungsprozesse sicherstellen und nachweisen lässt. Wir an unterschiedlichen Stellen hervorgehoben, müssen die Betreiber von Websites oder anderen Diensten, wenn sie eine informierte Entscheidung ihrer Nutzer:innen herbeiführen möchten, nicht das vollständige Methodenset zur Anwendung bringen.

Am einfachsten ist es für Dienstanbieter, wenn es für den in Frage stehenden Verarbeitungszweck, die durch ihn verursachten Grundrechtsrisiken und die geeignete Schutzmaßnahme bereits einen Stand der Technik gibt. Dann müssen sie diesen Stand der Technik nur anwenden, vorausgesetzt dem stehen keine unverhältnismäßigen Kosten gegenüber. Ein eigener Wirksamkeitsnachweis ist dagegen nicht erforderlich. Ein eigener Wirksamkeitsnachweis ist jedoch erforderlich, wenn es noch keinen Stand der Technik, also noch gar keinen Nachweis der Wirksamkeit im jeweils in Frage stehenden Bereich gibt.

Für den Bereich der informierten Einwilligung und weiterer Entscheidungen liegt der Stand der Technik, wie unter Punkt 3 beschrieben, nunmehr vor. Die geschilderten Methoden sind daher vor allem für solche Akteure interessant, die den Stand der Technik weiterentwickeln oder für weitere Bereiche ergänzen

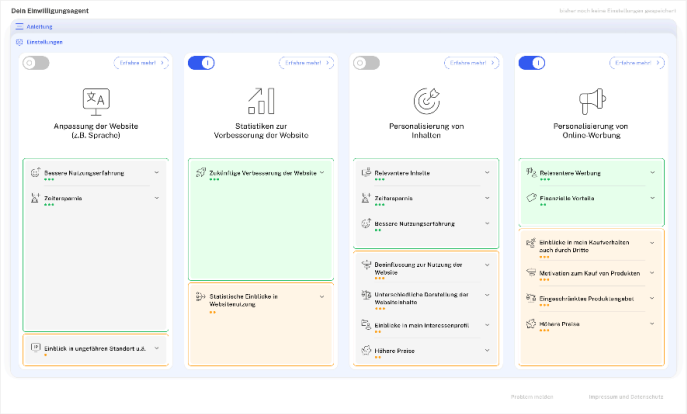
[62] Acquisti, A., Taylor, C., Wagman, L. (2016). The Economics of Privacy, in: Journal of Economic Literature, Vol. 54, No. 2, 2016, S. 442–492.

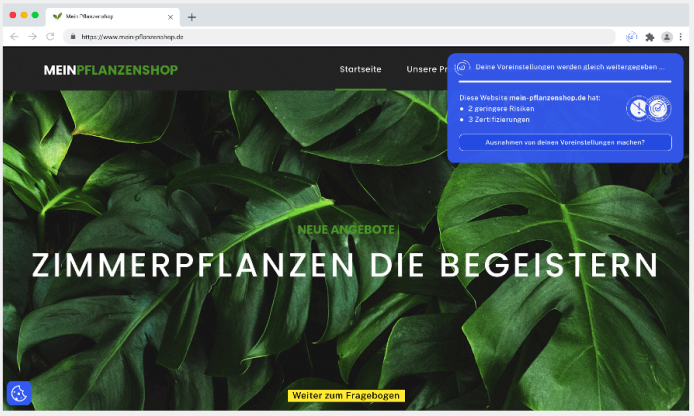
[63] EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 7.

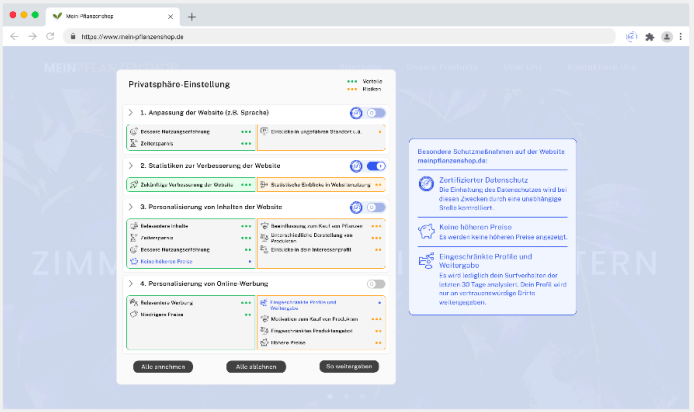
möchten.

Lasst uns zusammen – sei es aus der Forschung, Unternehmen oder Behörden heraus – die vom Gesetzgeber mit Art. 25 und 32 DSGVO vorgesehene Marktdynamik entfachen. Eine Entwicklung zu immer wirksameren Datenschutz.

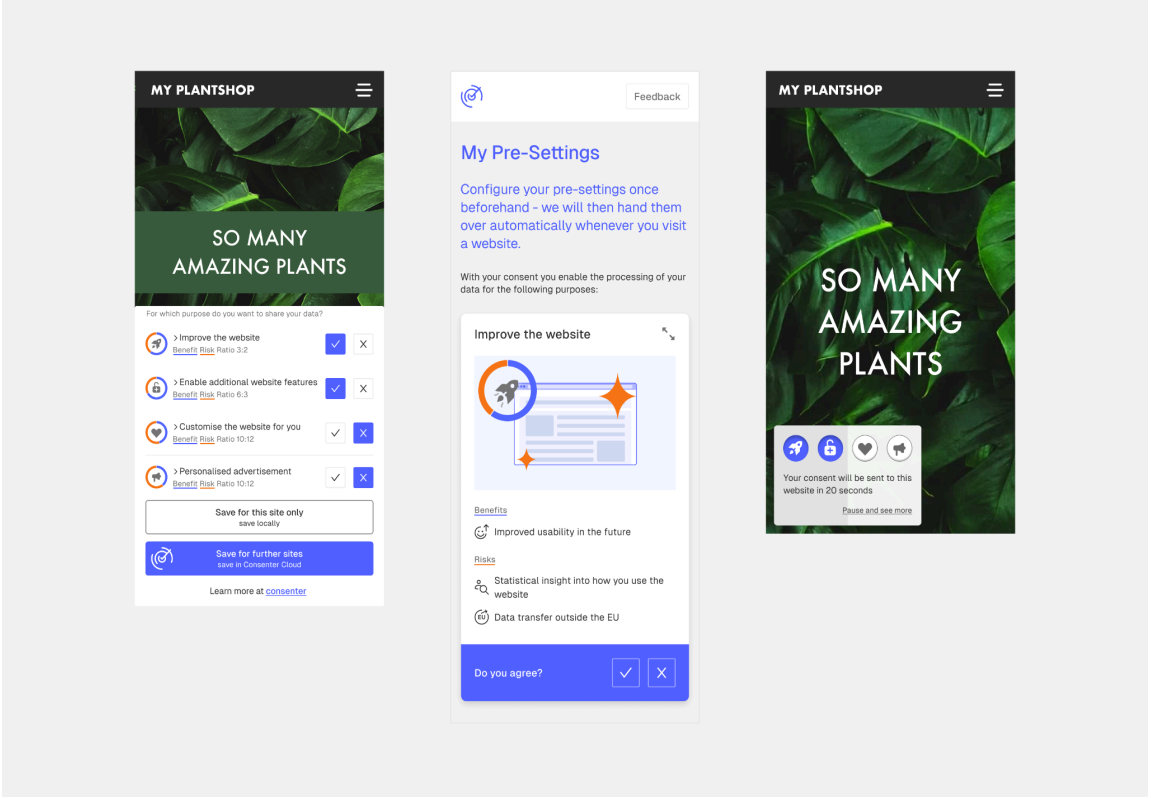
ANNEX 1: KONZEPT-DESIGNS ZUR INFORMIERTHEIT

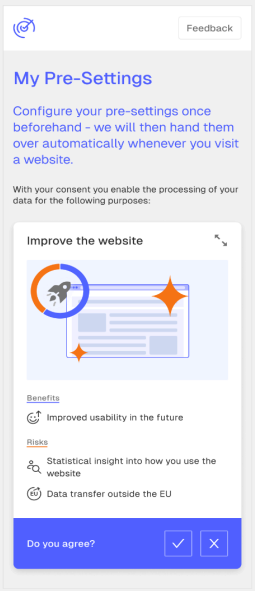


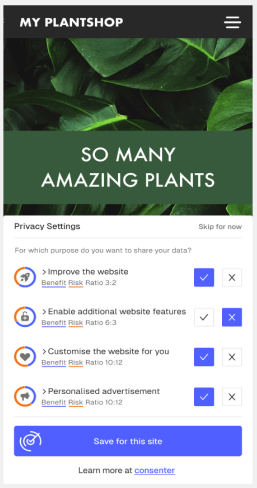


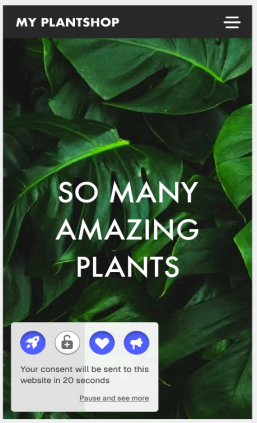


ANNEX 2: DESIGNS DER STUDIENGRUPPEN G UND D IN DER QUANTITATIVEN STUDIE ZUR EINWILLIGUNGSRATE




Feedback
My Pre-Settings
Configure your pre-settings once beforehand - we will then hand them over automatically whenever you visit a website.
With your consent you enable the processing of your data for the following purposes:
Improve the website
Benefits
Improved usability in the future
Risks
Statistical insight into how you use the website
Data transfer outside the EU
Do you agree?


MY PLANTSHOP
SO MANY AMAZING PLANTS
Privacy Settings
Skip for now
For which purpose do you want to share your data?
> Improve the website
Benefit Risk Ratio 3:2
> Enable additional website features
Benefit Risk Ratio 6:3
> Customise the website for you
Benefit Risk Ratio 10:12
> Personalised advertisement
Benefit Risk Ratio 10:12
Save for this site
Learn more at consenter


MY PLANTSHOP
SO MANY AMAZING PLANTS
Your consent will be sent to this website in 20 seconds
Pause and see more