

Einwilligung lässt sich nicht delegieren

Warum KI nicht entscheiden sollte, was wir mit KI teilen – und was stattdessen zu tun ist

Autor

Rafael Vrecar · CTSi · [ORCID 0000-0001-6572-5254](#)

Quellen und Ko-Autor:innen

Dieses White Paper fasst zwei eigene Publikationen des Autors zusammen und bereitet sie für ein breiteres Publikum auf:

(1) Position Paper (Hauptgrundlage). Vrecar, R. (2026). *Why AI Shouldn't Decide What We Share with AI and How We Can Do Better* [Position Paper und Präsentation], Workshop im Rahmen der CHI '26, Barcelona. Alleinautor. Open Access unter CC BY-NC-ND 4.0: hdl.handle.net/20.500.12708/228428 [1]

(2) Empirische Grundlage (Ko-Autor:innenschaft). Vrecar, R., Geld, B., Dobrosovstnova, A., Čolakovová, M. G., Weiss, A. (2026). *Do Cookies Taste Different? The Impact of Options and Website Type When Setting Cookie Preferences*. In: CHIRA 2025, CCIS 2834, S. 56–77, Springer Nature Switzerland, [doi:10.1007/978-3-032-16448-3_4](https://doi.org/10.1007/978-3-032-16448-3_4) [2]. Alle empirischen Ergebnisse in diesem White Paper stammen aus dieser gemeinsamen Arbeit mit Barbara Geld, Anna Dobrosovstnova, Michaela Gaea Čolakovová und Astrid Weiss.

ABSTRACT

Cookie-Banner und Privacy Labels sollen uns eine informierte Entscheidung über unsere Daten ermöglichen. Beides erfüllt diesen Zweck bisher nur eingeschränkt. Eine eigene Studie mit 136 auswertbaren Antworten zeigt: Wie Menschen entscheiden, hängt vor allem davon ab, welche Auswahlmöglichkeiten ein Banner anbietet. Nur dieser Faktor war statistisch signifikant; Art der Website, Vorwissen und Alter machten keinen messbaren Unterschied. Es liegt nahe, solche Entscheidungen an KI-Systeme abzugeben. Dieses White Paper zeigt, warum das rechtlich nicht funktioniert: Die DSGVO versteht unter Einwilligung eine freiwillige, informierte und unmissverständliche Erklärung der betroffenen Person selbst. Entscheidet ein KI-System an ihrer Stelle, ist diese Bedingung nicht erfüllt. Dazu kommt, dass große Sprachmodelle nachweislich Fehler produzieren. Als Alternative stellt dieses White Paper ein einheitliches Einwilligungsfenster im Browser vor, das in einer ersten kleinen und nicht repräsentativen Evaluierung besser abschnitt als übliche Banner. KI soll dabei unterstützen, nicht entscheiden.

1 Einleitung und Hintergrund

Seit die DSGVO im Mai 2018 gilt, sehen wir täglich Cookie-Banner. Sie sollen uns eine informierte Entscheidung über unsere Daten ermöglichen. In der Praxis gelingt das selten. Viele Banner machen das Ablehnen aufwendiger als das Zustimmung [3, 4]. Manche Websites setzen die getroffene Wahl technisch gar nicht um [5]. Und Dark Patterns, also Gestaltungstricks, die zu einer bestimmten Antwort drängen, sind in Bannern weit verbreitet [6, 7].

Der zweite große Versuch, mehr Transparenz zu schaffen, sind Privacy Labels: kurze Übersichten über die Daten, die eine App sammelt. Apple hat sie 2020 für den App Store eingeführt [8]. Auch hier ist das Bild gemischt. Viele Nutzer:innen verstehen die Labels nicht vollständig, weil sie komplex sind, ungewohnte Begriffe verwenden und die Informationen unübersichtlich anordnen [9, 10]. Wirkungslos sind sie aber nicht: Sie beeinflussen, ob jemand eine App installiert [11]. Bei beiden Instrumenten zeigt sich dasselbe Muster: Sie wirken, verstanden werden sie trotzdem nicht.

Daraus ergibt sich die Frage, um die es in diesem White Paper geht: Wenn Menschen mit solchen Entscheidungen überfordert sind, soll KI sie dann übernehmen?

2 Fakten und Erkenntnisse

2.1 Was die Entscheidung wirklich beeinflusst

Grundlage ist eine Online-Studie mit nachgebauten Websites (Vignettenstudie): 150 Teilnehmende, rekrutiert über die Plattform Prolific, davon 136 auswertbare Antworten [2]. Alle sahen nacheinander eine Nachrichtenseite, einen Online-Shop, ein Wetterportal und eine Informationsseite über Cookies und entschieden jedes Mal über das Cookie-Banner, zusammen also 544-mal. Welche Auswahlmöglichkeiten das Banner anbot, wechselte dabei zufällig zwischen drei Varianten:

- *Variante A*: Alle akzeptieren | Nicht notwendige ablehnen | Einstellungen anpassen
- *Variante B*: Alle akzeptieren | Einstellungen anpassen
- *Variante C*: Alle akzeptieren | Seite schließen

Von allen untersuchten Faktoren wirkte sich nur die Variante der Auswahlmöglichkeiten statistisch signifikant aus ($\chi^2 = 44,1$, $df = 2$, $p < 0,001$): Bei Variante A, der einzigen mit einem Ablehnen per Klick, akzeptierten deutlich weniger Teilnehmende alle Cookies, als bei statistischer Unabhängigkeit zu erwarten wäre; bei den Varianten B und C deutlich mehr. Weder die Art der Website noch die Vertrautheit mit dem Begriff „Cookie“ noch das Alter hatten einen messbaren Einfluss. Über alle 544 Entscheidungen hinweg entfielen 47,8 % auf „Alle akzeptieren“. In den Bannertext war zudem absichtlich ein Tippfehler eingebaut; den zugehörigen Aufmerksamkeitscheck bestanden nur 11,8 % der Teilnehmenden, wobei sich Raten nicht ausschließen lässt.

2.2 Was daraus folgt

- Wenn sich Cookies mit einem Klick ablehnen lassen, wird das auch genutzt. Fehlt dieser Button, nimmt kaum jemand den Umweg über die Einstellungen. Die meisten akzeptieren dann alles.
- Aufklärung allein ändert daran nichts. Wer erklären konnte, was Cookies sind, entschied genauso wie alle anderen.
- Entscheidend ist also die Gestaltung des Banners, nicht das Wissen der Nutzer:innen. Andere Studien kommen zum selben Schluss: Ein deutlich sichtbares „Ablehnen“ verändert die Entscheidung spürbar [12], personalisierte Banner helfen beim informierten Entscheiden [13].

2.3 Ein einheitliches Einwilligungsfenster im Browser

Hier setzt ein Prototyp an, den Andreas Schlögl in seiner Bachelorarbeit entwickelt und evaluiert hat, erstbetreut von Astrid Weiss, co-betreut vom Autor. Die Idee: Nicht jede Website baut ihr eigenes Banner, sondern der Browser stellt ein Fenster bereit, das überall gleich aussieht. Wer einmal verstanden hat, wie es funktioniert, findet sich auf jeder Seite zurecht.

Die von ihm berichteten Ergebnisse sind positiv: Die Teilnehmenden hielten das Fenster für glaubwürdiger und vertrauenswürdiger als ein klassisches Banner. Auf der System Usability Scale, einem Standardfragebogen zur Benutzerfreundlichkeit, erreichte es 72,25 von 100 Punkten [14], und 80 % zogen es der klassischen Lösung vor.

Diese Zahlen sind allerdings mit Vorsicht zu lesen. Die Evaluierung entstand im Rahmen einer Bachelorarbeit und ist nicht repräsentativ: zehn Teilnehmende, alle männlich, zwischen 18 und 30 Jahren ($M = 23,3$, $SD = 3,13$), die Hälfte davon mit Informatikhintergrund. Eine größere Folgestudie ist im Rahmen der Dissertation des Autors geplant [1].

3 Einordnung und Implikationen

3.1 Warum KI die Einwilligung nicht ersetzen kann

Die naheliegende Antwort auf überforderte Nutzer:innen wäre, die Entscheidung einem KI-System zu überlassen. Das Recht lässt das nicht zu. Art. 4 Abs. 11 DSGVO beschreibt Einwilligung als eine freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung der betroffenen Person: Sie selbst erklärt, dass sie mit der Verarbeitung einverstanden ist [15]. Entscheidet ein KI-System an ihrer Stelle, ist keine dieser Bedingungen mehr erfüllt, denn die Erklärung stammt dann nicht mehr von der Person.

Dazu kommt ein technisches Risiko: Große Sprachmodelle geben nachweislich falsche oder frei erfundene Antworten [16]. Bei rechtlichen und sicherheitsrelevanten Folgen wiegt das schwer. Man könnte ein solches System auf eine geprüfte Auswahl von Antworten festlegen; ob das für die Vielfalt echter Fälle reicht, ist offen.

3.2 Wobei KI stattdessen helfen kann

Sinnvoll ist KI hier als Assistenz, die durch die Entscheidung führt, statt sie zu treffen: Datenschutzerklärungen verständlich erklären, Begriffe aus Privacy Labels einordnen, also genau dort ansetzen, wo die Verständnisprobleme belegt sind [9, 10]. Entscheiden soll weiterhin die Person selbst.

3.3 Was zu tun ist

Ein einheitlicher Standard. Der erste sinnvolle Schritt ist ein verpflichtendes Einwilligungsfenster, das auf allen Websites gleich aussieht. Es macht die Situation wiedererkennbar und ist die Voraussetzung dafür, dass man seine Präferenzen einmal festlegt und sie danach automatisch gelten.

Gleiche Begriffe und Aufklärung. Wenn Datenschutzerklärungen dieselben Begriffe verwenden und erklärt wird, was diese bedeuten, löst das das Verständnisproblem, statt es zu umgehen.

Sicherheit mitdenken. Einwilligung betrifft nicht nur den Datenschutz. Wer Tracking zustimmt,

lädt im Schnitt 45 % mehr Skripte von Drittanbietern und 63 % mehr sicherheitsrelevante Datenflüsse mit [17]. Ein Banner, das zum Zustimmung verleitet, vergrößert damit auch die Angriffsfläche.

Grenzen. Die Studie arbeitete mit statischen, nachgebauten Websites und einer nicht repräsentativen Stichprobe; am Prototyp nahmen zehn Personen teil. Beide Ergebnisse zeigen eine Richtung an, belegen sie aber noch nicht.

4 Fazit

- **Es kommt auf die angebotenen Optionen an.** Von allen untersuchten Faktoren war nur die Auswahl im Banner statistisch signifikant ($p < 0,001$), nicht das Wissen der Nutzer:innen.
- **Einwilligung lässt sich nicht abgeben.** Entscheidet eine KI an unserer Stelle, ist das keine Einwilligung im Sinne von Art. 4 Abs. 11 DSGVO, egal wie gut das System ist.
- **Der Weg führt über einen einheitlichen Standard.** Ein überall gleiches Einwilligungsfenster, verständliche Sprache und KI in unterstützender Rolle ermöglichen informierte Entscheidungen, ohne sie den Betroffenen abzunehmen.

Literatur

- [1] Rafael Vrecar. Why AI Shouldn't Decide What We Share with AI and How We Can Do Better. Position Paper und Präsentation, Workshop im Rahmen der CHI '26, Barcelona, Spanien, May 2026. Open Access, CC BY-NC-ND 4.0, <https://hdl.handle.net/20.500.12708/228428>.
- [2] Rafael Vrecar, Barbara Geld, Anna Dobrosovstnova, Michaela Gaea Čolakovová, and Astrid Weiss. Do Cookies Taste Different? The Impact of Options and Website Type When Setting Cookie Preferences. In *Computer-Human Interaction Research and Applications (CHIRA 2025)*, volume 2834 of *Communications in Computer and Information Science*, pages 56–77, Cham, 2026. Springer Nature Switzerland.
- [3] Georgios Kampanos and Siamak F. Shahandashti. Accept All: The Landscape of Cookie Banners in Greece and the UK. In *ICT Systems Security and Privacy Protection*, pages 213–227, Cham, 2021. Springer International Publishing.
- [4] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (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)*, pages 973–990. ACM, 2019.
- [5] Célestin Matte, Nataliia Bielova, and Cristiana Santos. Do Cookie Banners Respect My Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 791–809, 2020.
- [6] Philip Hausner and Michael Gertz. Dark Patterns in the Interaction with Cookie Banners, 2021. Workshop "What Can CHI Do About Dark Patterns?" at CHI 2021.
- [7] Oksana Kulyk, Willard Rafnsson, Ida Marie Borberg, and Rene Hougard Pedersen. "So I Sold My Soul": Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions. In *Proceedings of the 2022 Symposium on Usable Security and Privacy (USEC)*. Internet Society, 2022.
- [8] Apple Inc. App Privacy Labels Now Live on the App Store. Apple Developer News, 2020. <https://developer.apple.com/news/?id=3wann9gh>.
- [9] Ishika Keswani, Kerick Walker, Adrian Clement, Eusila Kitur, Nannapas Wonghirundacha, Ryan Aubrey, Vivien Song, and Eleanor Birrell. User Understandings of Technical Terms in App Privacy Labels. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*, pages 279–298, 2025.
- [10] Shikun Zhang, Lily Klucinec, Kyerra Norton, Norman Sadeh, and Lorrie Faith Cranor. Exploring Expandable-Grid Designs to Make iOS App Privacy Labels More Usable. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 139–157. USENIX Association, 2024.
- [11] David G. Balash, Mir Masood Ali, Chris Kanich, and Adam J. Aviv. "I Would Not Install an App with This Label": Privacy Label Impact on Risk Perception and Willingness to Install iOS Apps. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 413–432. USENIX Association, 2024.

- [12] Nataliia Bielova, Laura Litvine, Anyisia Nguyen, Mariam Chammat, Vincent Toubiana, and Estelle Hary. The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2813–2830. USENIX Association, 2024.
- [13] Tom Biselli, Laura Utz, and Christian Reuter. Supporting Informed Choices about Browser Cookies: The Impact of Personalised Cookie Banners. *Proceedings on Privacy Enhancing Technologies*, 2024(1):171–191, 2024.
- [14] James R. Lewis and Jeff Sauro. The Factor Structure of the System Usability Scale. In Masaaki Kurosu, editor, *Human Centered Design*, pages 94–103. Springer Berlin Heidelberg, 2009.
- [15] Europäisches Parlament und Rat der Europäischen Union. Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung). Amtsblatt der Europäischen Union, 2016. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679>.
- [16] Gabrijela Perković, Antun Drobnjak, and Ivica Botički. Hallucinations in LLMs: Understanding and Addressing Challenges. In *2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, pages 2084–2088, 2024.
- [17] David Klein, Marius Musch, Thomas Barber, Moritz Kopmann, and Martin Johns. Accept All Exploits: Exploring the Security Impact of Cookie Banners. In *Proceedings of the 38th Annual Computer Security Applications Conference (ACSAC '22)*, pages 911–922. ACM, 2022.

Danksagung

Der in Abschnitt 2.3 beschriebene Prototyp samt Evaluierung stammt von Andreas Schlößl, der ihn im Rahmen seiner Bachelorarbeit an der TU Wien entwickelt hat, erstbetreut von Astrid Weiss, co-betreut vom Autor dieses White Papers. Auch die dort genannten Kennzahlen (System Usability Scale, Präferenz, Stichprobe) stammen aus seiner Arbeit. Die Rechte an den Screenshots liegen bei ihm (© Andreas Schlößl); sie sind hier deshalb nicht abgedruckt, im Original-Position-Paper aber zu sehen.

Die in Abschnitt 2.1 berichtete Studie entstand gemeinsam mit Barbara Geld, Anna Dobrosovestnova, Michaela Gaea Čolakovová und Astrid Weiss und ist bei Springer erschienen. Aus diesem Kapitel sind hier ausschließlich einzelne Kennzahlen und Testergebnisse referiert, keine Textpassagen, Abbildungen oder Tabellen und auch keine daraus abgeleiteten Grafiken. Wer die vollständige Studie samt Methodik, Vignetten und Kontingenztabellen lesen möchte, findet sie unter der oben angegebenen DOI.

Rafael Vrecar ist Empfänger eines DOC-Stipendiums der Österreichischen Akademie der Wissenschaften (DOC/27292).

Einsatz von KI-Werkzeugen

Für dieses White Paper wurde ein KI-Assistenzsystem (Claude, Anthropic) eingesetzt, um die beiden zugrunde liegenden eigenen Publikationen für das Format der Reihe zu kürzen, ins Deutsche zu übertragen, zu strukturieren und sprachlich zu vereinfachen. Ideen, Argumentation und Schlussfolgerungen stammen aus den referenzierten eigenen Arbeiten; sämtliche Inhalte, Zahlen und Quellenangaben wurden vom Autor gegen die Originalpublikationen geprüft. In den zugrunde liegenden Publikationen dienten DeepL, ChatGPT, Apple Intelligence Writing Tools und Overleaf Writefull ausschließlich der sprachlichen Überarbeitung.

Zitiervorschlag

Vrecar, R. (2026). *Einwilligung lässt sich nicht delegieren*. CTSi White Paper No. 01. TU Wien.

Kontakt: Rafael Vrecar · rafael.vrecar@tuwien.ac.at · CTSi · cts.wien