

Studie:

# Platform Compliance

Fallstudien zu manipulativen Tricks  
in der Gestaltung von Interfaces und  
Prozessen

Wien, Juni 2024



 Bundesministerium  
Finanzen



 Bundesministerium  
Arbeit, Soziales, Gesundheit  
und Konsumentenschutz



# Inhalt

1	Einleitung	6
2	Dark Patterns	7
2.1	Entwicklungsgeschichte	8
2.2	Die Begriffsdefinition(en)	11
2.3	Rechtlicher Rahmen	14
2.4	Erhebung	20
3	Online-Shopping & Dark Patterns	23
3.1	Case Study „Temu“	24
3.2	Case Study „SHEIN“	34
4	Flugbuchungen & Dark Patterns	42
4.1	Case Study „Ryan Air“	43
4.2	Case Study „Austrian Airlines“	56
4.3	Case Study „Wizz Air“	60
4.4	Case Study „Opodo“	67
5	Registrierungsprozesse auf Social Media	74
5.1	Case Study „TikTok“	77
5.2	Case Study „Instagram“	83
5.3	Exkurs: Consent or Pay-Modell von Meta	88
6	Tools	90
6.1	Verhinderung von Tracking & Ausblendung von Cookie Bannern	90
6.2	Ausblendung von Werbung und Empfehlungen	93
6.3	Ausblendung & Highlighting von Dark Patterns	95
6.4	Erkennung und Dokumentation von Verstößen	96
6.5	Fallstricke in der automatisierten Detektion von Dark Patterns	98
7	Schlussfolgerungen	101
8	Quellen	106
8.1	Literaturverzeichnis	106
8.2	Abbildungsverzeichnis	109
9	Technischer Annex	112
9.1	Beschreibung der Tool-Entwicklung	112
9.2	Vergleich der Komplexität von Appium und Selenium für Mobile Web Monitoring	118

## Disclaimer

Die in diesem Dokument dargestellten Analysen basieren auf Recherchen zu einzelnen Wirtschaftsakteuren im Rahmen der KIRAS-Dienstleistung PCS. Sie spiegeln den Konsens wider, den die Autor:innen des vorliegenden Berichts in ihrer Interpretation der jüngst beschlossenen Bestimmungen des Digital Services Act DSA, des Digital Markets Act DMA und der DSGVO hinsichtlich der in den Untersuchungsbereich fallenden Angelegenheiten erzielt haben. Die in diesem Dokument vertretenen Standpunkte greifen der Beurteilung durch Rechtsinstitutionen nicht vor, die in jedem Einzelfall vorgenommen werden muss. Es ist besonders zu beachten, dass die dokumentierten Praktiken sich ändern können – aus diesem Grund ist jedem Screenshot ein Datum beigefügt.

# Zusammenfassung

## PCS – Platform Compliance Study

**Studien-Autor:innen:** Louise Beltzung, Julia Krickl, Irem Hölzl, Andrew Lindley

Version 1.0 – 30. September 2024

**Hintergrund** – Am 17. Februar 2024 trat die Verordnung über einen Binnenmarkt für digitale Dienste („Digital Services Act“, DSA) in der gesamten Europäischen Union in Kraft. Diese Studie untersucht insbesondere das Verbot von verhaltensbasierter Werbung für Minderjährige und das Verbot von Dark Patterns gemäß der Verordnung (EU) Nr. 2022/2065, Bezug genommen wird auch auf den Digital Markets Act (DMA), die Datenschutzgrundverordnung (DSGVO) sowie die UGP-Richtlinie.

**Ziel der Studie** – Die Studie hat folgende Hauptziele: (1) Bestandsaufnahme zu Dark Patterns im Bereich des E-Commerce und bei Flugbuchungen, (2) Dokumentation und Analyse von Registrierungsprozessen auf Social Media, (3) Untersuchung der technischen Möglichkeiten zur Erkennung, Überwachung und Dokumentation von Dark Patterns.

**Methodik** – (1) Erhebung: Toolgestützte Erhebung und Dokumentation von Dark Patterns bei ausgewählten Wirtschaftsakteuren. (2) Analyse: Rechtliche Bewertung der dokumentierten Dark Patterns. (3) Entwicklung: Erstellung eines Blueprints für ein Monitoring-Tool, das auch für Apps von Online-Marktplätzen anwendbar ist.

**Ergebnisse** – (1) Herausforderungen für den Verbraucherschutz: Schwierigkeit der Einordnung von Dark Patterns im gesetzlichen Rahmen; Abgrenzung von Marketing-Praktiken. (2) Unsicherheit über die anzuwendenden gesetzlichen Bestimmungen.

**Nutzen der Studie** – (1) Die umfassende Kritik an Dark Patterns im Online-Handel hilft, Probleme von Konsument:innen besser zu verstehen. (2) Wertvolle Einblicke zur Einordnung und möglichen Rechtsdurchsetzung im Verbraucherschutz.

**Einschränkungen der Studie** – (1) Fokus: Die Studie konzentriert sich auf einzelne Fallstudien und dient der Illustration, nicht jedoch einem umfassenden Überblick über den Online-Alltag von Konsument:innen. Es handelt sich keine quantitative Erhebung; (2) Rechtliche Unsicherheit: Bisher gibt es wenig praktische Gesetzgebung zu Dark Patterns, die gerichtlich durchgesetzt wurde; die rechtliche Einordnung erfolgte vorsichtig und muss in ihrem begrenzten Umfang gesehen werden.

**Fazit** – Die vorliegende Studie zeigt, dass die Umsetzung der neuen Regelungen des DSA im Verbraucherschutz herausfordernd ist. Die Identifizierung und rechtliche Einordnung von Dark Patterns ist komplex, dennoch bietet die Studie wertvolle Ansätze und Tools zur Unterstützung der Rechtsdurchsetzung im Verbraucherschutz.

**Schlüsselwörter:** Dark Patterns, verhaltensbasierte Werbung

## Summary

### PCS – Platform Compliance Study

**Authors:** Louise Beltzung, Julia Krickl, Irem Hölzl, Andrew Lindley

Version 1.0 – 30. September 2024

**Background** - On 17 February 2024, the Digital Services Act (DSA) entered into force across the European Union. This study examines in particular the ban on behavioural advertising to minors and the ban on dark patterns under Regulation (EU) No 2022/2065.

**Objective of the study** - The study has the following main objectives: (1) To take stock of the implementation of the ban on behavioural advertising to minors on social media. (2) To collect and analyse current examples of dark patterns in online shopping and flight bookings in Austria. (3) The investigation of the technical possibilities for recognising and monitoring dark patterns.

**Methodology** - (1) Survey: Tool-supported survey and documentation of dark patterns among selected economic actors. (2) Analysis: Legal assessment of the documented dark patterns. (3) Development: Creation of a blueprint for a monitoring tool that can also be used for online marketplace apps.

**Results** - (1) Challenges for consumer protection: Difficulty of categorising dark patterns within the legal framework; differentiation from marketing practices. (2) Uncertainty about the applicable legal provisions.

**Benefits of the study** - (1) The comprehensive criticism of dark patterns in online retail helps to better understand consumer problems. (2) Valuable insights into the categorisation and possible legal enforcement in consumer protection.

**Limitations of the study** - (1) Focus: The study focuses on individual case studies and serves as an illustration, but not as a comprehensive overview of consumers' everyday online lives. It is not a quantitative survey; the legal categorisation was carried out cautiously and must be seen in its limited scope. (2) Legal uncertainty: To date, there is little practical legislation on dark patterns that has been enforced in court.

**Conclusion** - This study shows that the implementation of the new DSA regulations in consumer protection is challenging. The identification and legal categorisation of dark patterns is complex, yet the study offers valuable approaches and tools to support enforcement in consumer protection.

**Keywords:** Dark patterns, behavioural advertising

# I Einleitung

Am 17. Februar 2024 ist die Verordnung über einen Binnenmarkt für digitale Dienste („Digital Services Act“, kurz DSA) in der gesamten Europäischen Union unmittelbar in Kraft getreten. Unter den zahlreichen durch die Verordnung (EU) Nr. 2022/2065 abgedeckten Themen widmet sich der vorliegende Studienbericht insbesondere dem **Verbot von Dark Patterns** und dem **Verbot verhaltensbasierter Werbung gegenüber Minderjährigen**. Der DSA richtet sich an Anbieter digitaler Dienste und ist neben dem Digital Markets Act (kurz DMA) ein zentraler Rechtsakt in der Europäischen Union, mit denen die Aktivitäten von Plattformen reguliert werden.

Vor dem Hintergrund dieser neuen rechtlichen Rahmenbedingungen präsentiert der vorliegende Studienbericht eine Reihe an Case Studies. Untersucht wurden Dark Patterns auf E-Commerce-Plattformen sowie in den Flugbuchungsprozessen von Airlines und Urlaubsplattformen. Als Zugang für die Untersuchung der Einhaltung des Verbots von verhaltensbasierter Werbung wurde die Gestaltung der Registrierungsprozesse für Minderjährige auf zwei Social-Media-Plattformen (TikTok, Instagram) auf Dark Patterns hin untersucht.

Der DSA richtet sich an Onlineplattformen, insbesondere auch an sogenannte „Very Large Online Platforms“ (kurz VLOPs), doch Dark Patterns sind auch nach anderen Rechtsregelungen verboten. Insofern wurde entschieden, Dark Patterns auch auf Websites von Onlineshops und anderer Unternehmen zu sammeln, um dem Ziel der Studie Rechnung zu tragen, dass die Dokumentation und Analyse von Beispielen zum besseren Verständnis des Phänomens beitragen.

Der Studienbericht beginnt mit einer Einordnung des Phänomens Dark Patterns hinsichtlich Entstehungsgeschichte, Begriffsdefinitionen und dem rechtlichen Rahmen sowie einer Darstellung der Vorgehensweise bei der Erhebung (**Kapitel 2 Dark Patterns**). Im Anschluss erfolgt die Analyse der Case Studies entlang von drei Themenbereichen (**Kapitel 3 Online-Shopping & Dark Patterns**, **Kapitel 4 Flugbuchungen & Dark Patterns** und **Kapitel 5 Registrierungsprozesse auf Social Media**). Im Anschluss an die Erhebungsergebnisse werden Tools präsentiert, die dazu beitragen können, die Exposition von Konsumentinnen und Konsumenten sowie Stakeholdern des Verbraucherschutzes gegenüber Dark Patterns zu reduzieren und diese entsprechend zu erkennen bzw. zu dokumentieren (**Kapitel 6 Tools**). In den Schlussfolgerungen werden Empfehlungen für den Verbraucherschutz formuliert und ein Ausblick auf offene Fragen gegeben (**Kapitel 7 Schlussfolgerungen**).

## 2 Dark Patterns

Teilweise liegt im Schatten unserer Aufmerksamkeit, was unsere Entscheidungen online beeinflusst: Manchmal sind es Details wie die Farbgestaltung einer Option oder der Tonfall eines Textes im Bestellprozess, manchmal auch schlicht das simple *Gefühl* es handle sich um ein besonders gutes oder auch dringliches Angebot. Was den Blick von Konsumentinnen und Konsumenten lenkt und ihre Entscheidungen beeinflusst, ist teilweise eben subtil.

Das ist nicht neu, aber: Digitalisierung hat zu einer Professionalisierung der Abstimmung von Praktiken geführt und einer größeren Wirkmächtigkeit derselben. Der UX-Designer Harry Brignull führte deshalb im Jahr 2010 den Begriff der „Dark Patterns“ neu ein und brachte damit eine Debatte ins Rollen, die bis heute anhält. Er kritisierte „Tricks“ seiner Fachkolleg:innen, mit denen User auf Websites oder in Apps über das Design von Website-Elementen zu von ihnen nicht-intendierten Aktionen zu bewegen.<sup>1</sup> In weiterer Folge wurden unter diesem Begriff eine Reihe an Praktiken beschrieben und kritisiert, die darauf abzielen **über die Gestaltung von Websites und Prozessen die Entscheidungen von Usern zu manipulieren in eine von ihnen nicht beabsichtigte oder interessenswidrige Richtung**. Bis heute wird über die Definition von Dark Patterns wissenschaftlich debattiert und es werden unter Dark Patterns sehr unterschiedliche Praktiken verstanden – von Kritik an einer irreführenden Formulierung von Texten, hin zu einer suggestiven farblichen Gestaltung von Optionen – und auch ihr Einsatz ist an sehr unterschiedlichen Stellen von Prozessen innerhalb der Wege von Verbraucher:innen online.

Im folgenden Kapitel beschreiben wir deshalb zunächst die Entwicklungsgeschichte der Praktiken, die unter dem Begriff „Dark Patterns“ neu zusammengefasst wurden. Manche der kritisierten Praktiken, wie versteckte Kosten, sind etablierte Themen im Verbraucherschutz, und auch die Mechanismen hinter Dark Patterns werden im Rahmen der Verhaltensökonomie seit den 1970er Jahren untersucht. Der historische Blick zeigt, was an Dark Patterns „neu“ ist, und wie sie sich ableiten lassen aus langjährigen Praktiken im Handel, digitalen Marketingmethoden, Entwicklungen im User Experience-Design sowie Erkenntnissen aus der Verhaltensökonomie. (**Kapitel 2.1.**)

Der Begriff „Dark Patterns“ hat Einzug in die Rechtsmaterie gefunden und gleichzeitig wird die Begriffsdefinition noch diskutiert, auch wissenschaftlich – der Begriff hat seine Stärken einerseits in seiner Breite, andererseits liegen seine Schwächen darin, dass es teilweise schwer zu fassen ist, was schon Dark Pattern ist und wo legitimes unternehmerisches Interesse im Sinne des z. B. Marketing liegt. (**Kapitel 2.2.**)

Unabhängig von diesen begrifflichen Herausforderungen sind Praktiken, die als Dark Patterns gelten indirekt bereits durch verschiedene Rechtsdokumente verboten oder eingeschränkt; mit dem Digital Services Act (DSA) und dem Digital Markets Act (DMA) wurden sie auch erstmals rechtlich als verbotene Praktiken benannt – einführend geht **Kapitel 2.3.** auf diesen rechtlichen Rahmen in der Europäischen Union bzw. in Österreich ein. In **Kapitel 2.4.** wird die methodologische Vorgehensweise der Case Studies erläutert, die ab Kapitel 3 ausführlich dargestellt werden.

---

<sup>1</sup> (Brignull, 2010)

## 2.1 Entwicklungsgeschichte

Dark Patterns beruhen teilweise auf E-Commerce Praktiken, die schon seit Jahren eingesetzt werden.<sup>2</sup> Zudem kann die Wirksamkeit von Dark Patterns auf Erkenntnisse der Psychologie zurückgeführt werden, wie die Ausnutzung der intuitiven Art Informationen wahrzunehmen und schnell zu verarbeiten. Im Folgenden soll der Einblick in einzelne Disziplinen bzw. Trends aus denen Dark Patterns entstanden sind, dazu beitragen, das Phänomen einzuordnen und zu entmystifizieren.

### System 1 und System 2

Popularisiert in den frühen 2010er Jahren durch den Nobelpreisträger und Forscher der Verhaltenspsychologie Daniel Kahnemann wird angenommen, dass dem Denken und Argumentationsprozessen zwei unterschiedliche kognitive Systeme zugrunde liegen.<sup>3</sup> Unterschieden wird zwischen dem intuitiven, automatischen und unbewussten System-1 und dem abwägenden, anstrengenderen System-2-Denkprozess.<sup>4</sup>

Erstellt ein User beispielsweise einen neuen Account auf einer Website, wird er aufgefordert den allgemeinen Geschäftsbedingungen zuzustimmen, sowie auch den Datenschutzbestimmungen. Diese Bedingungen werden von den allermeisten Usern einfach akzeptiert, aber nie gelesen – ihnen wird meist schnell, intuitiv und automatisch zugestimmt. Das ist ein Beispiel für einen System-1-Denkprozess, der automatisch und unbewusst, ohne viel aktives Nachdenken abläuft. Dem gegenüber steht das sogenannte System-2-Denken. Nimmt sich ein User Zeit und macht sich die Mühe, die gesamten Texte der AGB sowie der Datenschutzbestimmungen sorgfältig zu lesen und wägt ab, ob den Konditionen zugestimmt werden soll, bedient sie sich des System-2-Denkprozesses. Dieser Prozess findet kontrolliert und bewusst statt und ist daher auch mit einem gewissen kognitiven Aufwand verbunden. Das macht das System-2-Denken mühevoller als den intuitiven System-1-Denkprozess. System-2-Denken basiert also auf einem abwägenden, anstrengenden Entscheidungsprozess, der zu einer langsameren Ausführung des intendierten Verhaltens führt.<sup>5</sup>

### Verhaltensökonomie und „cognitive shortcuts“

Diese Erkenntnis über Denk- und Verarbeitungsprozesse in der menschlichen Wahrnehmung zählt zu den Erkenntnissen der Verhaltensökonomie. Ab den 1970er Jahren wurde vonseiten der Ökonomie, später Verhaltensökonomie, nach Erklärungen für irrationale Entscheidungen gesucht. Denn in klassischen Modellen der Ökonomie konnten bestimmte Verhaltensmuster von Menschen, die im Alltag zu beobachten waren, nicht erklärt werden.<sup>6</sup>

In der klassischen ökonomischen Theorie ist für den rationalen Agenten des Homo oeconomicus ein Mehr an Entscheidungen besser, weil dieser konsistent über die Zeit Kosten und Nutzen abwägt und entlang dessen rational handelt. Die Verhaltensökonomie veränderte hier die Annahmen über den Homo oeconomicus. In Abkehr

---

<sup>2</sup> (OECD, 2022), S. 11

<sup>3</sup> (Kahneman, 2011)

<sup>4</sup> (Bösch et al., 2016)

<sup>5</sup> (Bösch et al., 2016)

<sup>6</sup> (Holle, 2019)

von diesem Verständnis, über das Wissen um bestimmte Irrationalitäten im menschlichen Verhalten, veränderte sich das Modell des Homo oeconomicus um Referenzvariablen.

Denn viele Optionen und eine hohe Wertigkeit jener bessert nicht unbedingt die Situation einer Person. Vielmehr gibt es situationsabhängig eine optimale Anzahl an Wahlmöglichkeiten, die ökonomisch die Wohlfahrt des Individuums maximiert. Wird diese Grenze überschritten, beginnt die Wohlfahrtskurve stetig zu sinken.

Bedingt ist dies durch die beschränkte kognitive Kapazität des Menschen, einer gewissen Lähmung in der Entscheidungsfindung, sowie auch einer Reduktion der Zufriedenheit bei Entscheidungen mit übermäßig vielen Optionen. Denn je mehr Optionen, desto höher ist die Wahrscheinlichkeit, dass eine bessere hätte dabei sein können, was das Phänomen des „Paradox of Choice“ darstellt. Mit jeder zusätzlichen Option steigen auch die Opportunitätskosten, sprich die Kosten von nicht wahrgenommenen Möglichkeiten.

Zudem gehen zu viele Optionen mit einer übertriebenen Erwartungshaltung einher.<sup>7</sup> Nimmt man all diese Überlegungen zusammen, wird klar, die Verhaltensökonomie geht von einem anderen Menschenbild aus, das einem „realen“ Menschen eher entspricht als das der klassischen ökonomischen Theorie. Die so entdeckten kognitiven Abkürzungen (cognitive shortcuts), machten die beobachteten, irrationalen Verhaltensweisen vieler Menschen nicht nur erklärbar, sondern auch vorhersehbar.

## Nudges

Auf dieser Basis wurde das Konzept der Nudges entwickelt, psychologische Tricks, die Individuen ursprünglich zu einem gesellschaftlich wünschenswerten Verhalten anleiten sollten. Nudges basieren auf den Prinzipien der Verhaltensökonomie und nutzen kognitive Verzerrungen, um Entscheidungen in eine bestimmte Richtung zu lenken, ohne die Wahlmöglichkeit einzuschränken.<sup>8</sup> Als Standardwerk zum Thema gilt „Nudge“ von Richard Thaler (Wirtschaftsnobelpreisträger 2017) und Cass Sunstein (2009).<sup>9,10</sup> In „Nudge“ wird entgegen der These der klassischen ökonomischen Theorie, dass menschliches Verhalten nur über Preismechanismen oder Gebote und Verbote gesteuert werden kann betont, dass es vielfältige Werkzeuge gibt, um menschliches Verhalten zu steuern und zu beeinflussen.

„[Mit] ‘Nudges‘ (Anstupser) [können], bestimmte Verhaltensweisen ohne Zwang positiv beeinflusst [werden].“<sup>11</sup>

Die Forschung zu psychologischen Abkürzungen oder Biases war nicht geleitet von Marketing, sondern hatte das Ziel, das Verhalten von Bürger:innen hin zur Minimierung negativer Externalitäten zu steuern – zum Beispiel hinsichtlich Fragen wie Organspenden. Erst später wurden Nudges für ihren Einsatz im Marketing

---

<sup>7</sup> (Holle, 2019)

<sup>8</sup> (Thaler, 2018; Thaler & Sunstein, 2009)

<sup>9</sup> (Thaler & Sunstein, 2009)

<sup>10</sup> (Thaler, 2017) Online: <https://www.nobelprize.org/prizes/economic-sciences/2017/thaler/facts/>

<sup>11</sup> (Holle, 2019)

entdeckt – als Instrumente, die kostengünstig verfügbar und einfach implementierbar sind.<sup>12</sup>

Seither kam es auch schon zu einer Distanzierung von Thaler et al. von dem für sie negativen Einsatz der Techniken und der Popularisierung des Terminus „Sludge“.<sup>13</sup> Sludges beschreiben manipulative Nudges, die entgegen dem besten Interesse von Konsument:innen eingesetzt werden – gemeint sind damit auch Dark Patterns.

### Traditionelle Verkaufstricks im E-Commerce

Die Entwicklung und die Verbreitung von Dark Patterns sind auf die zunehmende Digitalisierung von Marketing und von Entwicklungen im E-Commerce zurückzuführen.

Betrachtet man beispielsweise Preisstrategien, die schon seit geraumer Zeit im Verkauf im stationären Einzelhandel eingesetzt werden, wird klar, dass auch diese sich subtiler Tricks bedienen, um Produkte besser zu verkaufen. Ein Beispiel dafür ist die Preisgestaltung nach einem gewissen Muster, damit etwas günstiger wirkt (z.B.: 1,99 €, 599 €, 2.999,99 €, Vergleich zur UVP), aber auch die Anordnung und Präsentation von gewissen Produkten für Marketingzwecke (billigere Produkte nicht in Augenhöhe). Es handelt sich um Praktiken, die von Verbraucher:innen akzeptiert werden.

### Spam – die ersten Dark Patterns

In Kombination mit der zunehmenden Bedeutsamkeit von digitalen Marketingmethoden, die vor allem in den frühen 2000er Jahren Spam-artig eingesetzt wurden, hat dies maßgeblich zur Verbreitung von Dark Patterns beigetragen.<sup>14</sup> Ein prominentes Beispiel hierfür ist der Free-Mail Anbieter Hotmail. Das Unternehmen hat schon 1996 jedem E-Mail automatisch die Fußzeile: „*Get your free E-Mail with Hotmail*“ hinzugefügt, eine Marketingstrategie, die dem Unternehmen zu viralem Wachstum verholfen hat.<sup>15</sup> Bei diesen und ähnlichen Methoden wurden teils die Grenzen der Legalität ausgereizt: Bspw. griffen Services wie LinkedIn auf die Kontaktbücher ihrer Nutzer:innen zurück und luden diese automatisiert ein, das Service auch zu nutzen. In dem Fall von LinkedIn führte das zu einem „Class Action Lawsuit“, den das Unternehmen verlor.<sup>16</sup>

### A/B Tests und Dark Patterns

Ein Wachstumsbeschleuniger für die Verbreitung von Dark Patterns war die zunehmende Bedeutung der digitalen Welt. Im E-Commerce, wie auch in der Bewerbung von Produkten, konnte auf Strategien zurückgegriffen werden, die dem Offline-Handel traditionell nicht zur Verfügung standen: 1. Das Prinzip der Verhaltensänderung durch Nudges und psychologische Tricks, wie schon oben beschrieben, und 2. A/B Testing.

---

<sup>12</sup> (Holle, 2019)

<sup>13</sup> (Thaler, 2018)

<sup>14</sup> (Narayanan et al., 2020)

<sup>15</sup> (Murray, 2023)

<sup>16</sup> (Narayanan et al., 2020) und (Strange, 2015)

Mithilfe von A/B-Testing, konnten unterschiedliche Darstellungsformen von Websites auf einen Schlag tausenden Personen ausgespielt werden. So entdeckten UX-Designer:innen, dass selbst triviale Veränderungen im Website-Design, wie z. B. die Änderung einer Buttonfarbe oder deren Platzierung substantielle Veränderungen im Verhalten von Usern bewirken können. Mittlerweile ist die Idee der datengesteuerten Optimierung von Benutzeroberflächen fest im Designprozessen vieler Unternehmen verankert. Aus diesem Grund gilt der weitverbreitete Einsatz von A/B-Tests als ein Schlüsselement des Phänomens Dark Patterns.

Die Reifung bzw. wachsende Bedeutung der Online-Wirtschaft bzw. des E-Commerce verlagerte den Fokus von Onlinediensten von reinem Wachstum auf tatsächliche Einnahmen. Um diese Konversion von Aufmerksamkeit zu Umsatz zu schaffen, setzten Unternehmen zunehmend auf Verhaltensbeeinflussung – teils auf eine Art, die die Autonomie von Verbraucher:innen bzw. ihre informierte Entscheidungsfähigkeit beeinflusste. Hierfür wurde vor allem A/B-Testing und die zielgerichtete Gestaltung von Benutzeroberflächen gesetzt. In einigen Fällen waren dies optimierte Versionen von Tricks, die schon lange im Einzelhandel verwendet werden, aber in anderen Fällen waren sie völlig neu.

## 2.2 Die Begriffsdefinition(en)

Im Jahr 2010 umfasste die Kategorisierung von Harry Brignull zunächst folgende Kategorien:<sup>17</sup>

- **Comparison Prevention:** Die Verhinderung von Vergleichen
- **Confirm shaming:** Das Drängen zur Annahme
- **Disguised Ads:** Versteckte oder getarnte Werbung
- **Fake scarcity:** Vorgetäuschte Knappheit
- **Fake social proof:** Vorgetäuschter sozialer Druck
- **Fake urgency:** Vorgetäuschte Zeitnot oder Dringlichkeit
- **Forced action:** Erzwungene Handlungen
- **Hard to cancel:** Schwer rückgängig zu machen oder zu stornieren
- **Hidden costs:** Versteckte Kosten
- **Hidden subscription:** Verstecktes Abonnement
- **Nagging:** Wiederholte Aufforderungen
- **Obstruction:** Behinderung
- **Preselection:** Vorauswahl
- **Sneaking:** In den Warenkorb schleichen
- **Trick wording:** Fangfragen oder Trickfragen
- **Visual interference:** Visuelle Störung

Aufbauend auf diesen ersten Überlegungen von Kategorien wurden Dark Patterns laufend gesammelt und im Sinne einer Taxonomie unerwünschter Praktiken erweitert. Ein Großteil der ersten akademischen Arbeiten zum Thema konzentrierte sich darauf, an der Definition von Dark Patterns anhand von Beispielen zu arbeiten

---

<sup>17</sup> (Brignull, 2022) Types of deceptive pattern, online: <https://www.deceptive.design/types> (aufgerufen 12.03.2024)

bzw. auch unterschiedliche Kategorie-Systeme miteinander zu vergleichen. Bekannte Arbeiten dazu verfassten u.a. Mathur et al., Bösch et al., Gray et al. sowie Luguri und Strahilevitz.<sup>18</sup> Unterschiede in Ansätzen sind z. B. wenn anhand der Wirkungsweise von Designentscheidungen unterschieden wird, wie bei Gray et al.:<sup>19</sup>

- **Exploiting perceptual vulnerabilities:** Ausnutzung von Wahrnehmungsschwächen
- **Exploiting vulnerabilities in comprehension:** Ausnutzung von Schwachstellen beim Verstehen
- **Exploiting vulnerabilities in decision making:** Ausnutzung von Schwachstellen bei der Entscheidungsfindung
- **Exploiting expectations:** Ausnutzung von Erwartungen
- **Resource depletion and pressure:** Erschöpfung der Ressourcen und Druck
- **Forcing and blocking:** Erzwingen und Blockieren
- **Exploiting emotional vulnerabilities:** Ausnutzung von emotionalen Schwachstellen
- **Exploiting addiction:** Ausnutzen von Abhängigkeiten

Wissenschaftliche Erhebungen zu Dark Patterns gab es teilweise bezogen auf spezielle Themenfelder, wie Gaming oder Privatsphäre. Immer wieder wird in der Literatur darauf hingewiesen, dass nicht hinlänglich definiert sei, was die Begrifflichkeit „Dark Patterns“ umfasst – die Frage „wann genau ein User Interface Design zu einem Dark Pattern wird“ ist für manche der kritisierten Praktiken jedenfalls eine schwierige. Caragay et al. (2024) sprechen von einem rezenten Wandel in der wissenschaftlichen Auseinandersetzung mit der Thematik weg von deskriptiven Taxonomien hin zu Überlegungen zu hinter Dark Patterns liegenden Mechanismen.<sup>20</sup>

Im Jahr 2022 veröffentlichte die OECD einen umfassenden Bericht zu „Dark Commercial Patterns“. Folgende Schwierigkeiten bei Definitionen von Dark Patterns werden darin genannt: (1) zu eng gefasste Definitionen eignen sich nicht für ein sich rapide veränderndes Feld, (2) Definitionen entlang des Schadens für den User stehen vor der Schwierigkeit, dass dieser eben definiert werden müsste, (3) die Nutzung des Begriffs „deceptive“ (täuschend) wird als reduktiv kritisiert, weil manche, aber nicht alle Dark Patterns tatsächlich Konsumentinnen und Konsumenten täuschen (z. B. Nagging), (4) der Fokus auf User Interface vergesse auf Dark Patterns, die sich mehr auf die Gestaltung von Prozessen (z. B. Hürden bei Kündigung von Verträgen) beziehen.

In diesem Sinne stellte das OECD Committee on Consumer Policy eine Arbeitsdefinition von Dark Patterns auf, unter die die gesammelten Praktiken gefasst sind, die zum Zeitpunkt der Veröffentlichung bekannt waren:

*“Dark commercial Patterns are business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce or manipulate consumers and are likely to cause direct or indirect consumer detriment*

---

<sup>18</sup> (Bösch et al., 2016; Gray et al., 2018; Luguri & Strahilevitz, 2021; Mathur et al., 2019)

<sup>19</sup> (Gray et al., 2018)

<sup>20</sup> (Caragay et al., 2024)

*in various ways, though it may be difficult or impossible to measure such detriment in many instances.”<sup>21</sup>*

Der Begriff Dark Patterns wurde inzwischen durch den DSA in die EU-Gesetzgebung übernommen, doch viele Forscher:innen entfernen sich inzwischen von dem Begriff, auch der „Erfinder“ des Begriffs, Harry Brignull selbst. In seinem 2023 erschienenen Buch „Deceptive Patterns: Exposing the Tricks Tech Companies use to Control You“, führt er als Ersatz den Begriff des „Deceptive Design“ ein. Deceptive Design, wörtlich übersetzt mit „Täuschendes Design“ beschreibe eingesetzte Techniken umfassender. In „Deceptive Patterns“ arbeitet Brignull wiederum mit Taxonomien von Dark Patterns, die manipulative User Interface und User Experience Design-Entscheidungen in andere und teils weitere Kategorien fassen. Dieser Begriff wird auch von anderen, wie der World Wide Web Foundation favorisiert.<sup>22</sup>

Es lassen sich jedoch auch Zugänge finden, die nicht so sehr anhand der Beschreibung von unerwünschten Praktiken Dark Patterns definieren wollen, sondern als Abweichungen von normalen Praktiken. In diesem Sinne argumentieren Caragay et al. (2024) – sie kritisieren, dass es für UX-Designer:innen schwierig sei anhand von Dark Patterns-Taxonomien zu arbeiten, vor allem angesichts teilweise schwieriger Abgrenzungen – zum Beispiel: Ab wann ist etwas Nagging? Mit Verweis auf Mathur et al. betonen sie, dass Dark Patterns durch Änderungen in der Standard-Entscheidungsarchitektur entstehen. Doch was gilt als eine Standard-Entscheidungsstruktur für das Design einer Website oder die Gestaltung eines Prozesses?

Statt nach einer einheitlichen Repräsentation aller Standard-Entscheidungsstrukturen zu suchen, schlagen die Autor:innen vor, die gängigen Praktiken zu erfassen und diese mit den zu durchschnittlichen, üblichen Erwartungen von Usern abzugleichen. Ihr vorgeschlagener Ansatz umgeht die Schwierigkeit die psychologischen Wirkmechanismen von Praktiken zu erforschen, indem eine Designentscheidung als Dark Pattern gilt, wenn sie von den Standarderwartungen abweicht und gegen die Interessen von Usern steht. Standards sollen entlang von Konzepten entwickelt werden, z. B. könnte über das Konzept einer User-Registrierung gesprochen werden – wie wird hier von Akteuren vorgegangen und inwiefern deckt sich dies mit den Erwartungen von Usern. Vorteil dieser Methode wäre, dass bei Feststellung einer Abweichung von Erwartungen, Konzepte direkter kritisiert werden könnten und Überarbeitungsvorschläge klar würden. Interessant, aber noch nicht vorliegend, sind Überlegungen hinsichtlich der Kopplung solcher Überlegungen an die Verbraucherleitbilder.

---

<sup>21</sup> (OECD, 2022), S. 5, Eigene Übersetzung ohne Anspruch auf Vollständigkeit:

*„Dark Commercial Patterns sind Geschäftspraktiken, die Elemente der digitalen Entscheidungsarchitektur, insbesondere in Online-Benutzeroberflächen, nutzen, die die Autonomie, Entscheidungsfindung oder Wahlmöglichkeiten von Verbraucher:innen untergraben oder beeinträchtigen. Oft täuschen, zwingen oder manipulieren sie Verbraucher:innen und verursachen direkte oder indirekte Nachteile für diese, auch wenn es in vielen Fällen schwierig oder unmöglich ist, solche Nachteile zu messen.“*

<sup>22</sup> (Tech Policy Design Lab - Deceptive Design, o. J.)

## 2.3 Rechtlicher Rahmen

Seit 2010 entwickelt sich eine Taxonomie von Dark Patterns, die verschiedene Praktiken definiert. Diese sind unterschiedlich präzise beschrieben und oft schwer voneinander abzugrenzen. Bisher wurden über 1000 Dark Patterns dokumentiert, teils von Nutzer:innen, teils wissenschaftlich. Die rechtliche Bewertung von Dark Patterns stellt sich jedoch anders dar: Obwohl der Begriff inzwischen im Digital Services Act (DSA) verwendet wird, bleibt unklar, welche spezifischen Praktiken darunterfallen. Zudem können einige Praktiken, die als Dark Patterns bezeichnet werden, bereits nach bestehenden Gesetzen wie der DSGVO als rechtswidrig gelten.

Im Folgenden wird ein Abriss über die derzeitige rechtliche Behandlung des Themas gegeben, wobei wir uns auf die für die Studie relevanten Rechtsakte konzentrieren, insbesondere die Richtlinie über unlautere Geschäftspraktiken (UGP-RL) und den DSA, weniger auf die DSGVO. Angesichts der noch frühen Phase der Verwendung des Begriffs im rechtlichen Bereich gibt es nicht ausreichend Durchsetzungsmaterial, um einen rechtlichen Begriff von Dark Patterns zu definieren, mit dem bereits gearbeitet werden könnte. Es ist zu erwarten, dass es zu Abwägungen kommen und sich so zeigen wird, wo die Rechtsprechung an die wissenschaftliche und aktivistische Begriffsdebatte andockt.

### Dark Patterns und DSGVO

Dark Patterns beeinflussen die Entscheidungsfähigkeit von Verbraucher:innen, um sie zu einer geschäftlichen Entscheidung zu bewegen, die sie sonst nicht getroffen hätten. Bei der Gestaltung von Dark Patterns werden oft personenbezogene Daten der Nutzer:innen verwendet, um das Nutzerverhalten besser zu verstehen und ihren Entscheidungsfindungsprozess effektiv zu beeinflussen. Obwohl die Richtlinie über unlautere Geschäftspraktiken (UGP-RL)<sup>23</sup> und die Datenschutz-Grundverordnung (DSGVO)<sup>24</sup> noch keine konkrete Definition von Dark Patterns enthalten, erfordern die Ausgestaltung und die Folgen der Verwendung von Dark Patterns durch Online-Plattformen aus diesem Grund eine lauterkeits- und datenschutzrechtliche Prüfung.

In der vorliegenden Erhebung anhand von Case Studies betreffen keine Dark Patterns mögliche Verstöße im Sinne des DSGVO und entsprechend werden vorliegende rechtliche Einschätzungen in diesem Bereich nicht behandelt – darunter relevant sind vor allem die Guidelines des European Data Protection Board (EDPB) aus dem Jahr 2022. Der EDPB hat in seinen Leitlinien 03/2022<sup>25</sup> bereits eine Liste von Praktiken

---

<sup>23</sup> Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken)

<sup>24</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

<sup>25</sup> (European Data Protection Board, 2022) Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them.

zusammengestellt, die häufig als manipulative Gestaltungsmuster auf Social Media Plattformen zu beobachten sind und auch einen Verstoß gegen die DSGVO darstellen können. Ein ähnlicher Ansatz ist für weitere Gestaltungsmuster erforderlich, die als Dark Patterns und damit als irreführende bzw. aggressive Geschäftspraktiken im Sinne der UGP-RL angesehen werden können.

### Dark Patterns und die UGP-RL

Der Begriff „Dark Patterns“ wurde auch nach der Überarbeitung der UGP-RL durch die Modernisierungsrichtlinie (EU) 2019/2161 nicht aufgeführt. Dies hat auch die Europäische Kommission in ihren Leitlinien zur Auslegung der UGP-RL bestätigt, aber zugleich darauf hingewiesen, dass die UGP-RL unabhängig von ihrer Einordnung auf alle „unlauteren Geschäftspraktiken“ anwendbar ist, die die Voraussetzungen des sachlichen Anwendungsbereichs der Richtlinie erfüllen. Werden Dark Patterns im Rahmen von Geschäftsbeziehungen zwischen Unternehmen und Verbraucher:innen verwendet, kann die Richtlinie zusätzlich zu anderen Instrumenten des EU-Rechtsrahmens (z.B. DSGVO) herangezogen werden, um die Lauterkeit solcher Praktiken in Frage zu stellen.<sup>26</sup>

### Dark Patterns und der DSA

Die Verwendung von Dark Patterns ist in Online-Umgebungen bereits seit Jahren weit verbreitet. Dennoch ist der Digital Services Act (DSA) die erste europäische Rechtsvorschrift, die dieses Phänomen rechtlich definiert und ein ausdrückliches Verbot seiner Nutzung vorsieht. Nach Art. 25 Abs. 1 DSA dürfen *Anbieter von Online-Plattformen ihre Online-Schnittstellen nicht so konzipieren, organisieren oder betreiben, dass Nutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden.* In Erwägungsgrund 67 werden Dark Patterns definiert und anhand von Beispielen erläutert. Demnach sind Dark Patterns *Praktiken, mit denen darauf abgezielt oder tatsächlich erreicht wird, dass die Fähigkeit der Nutzer, eine autonome und informierte Auswahl oder Entscheidung zu treffen, maßgeblich verzerrt oder beeinträchtigt wird. Solche Praktiken können eingesetzt werden, um die Nutzer zu unerwünschten Verhaltensweisen oder ungewollten Entscheidungen zu bewegen, die negative Folgen für sie haben.* Nach dieser Definition ist zu verstehen, dass die Grenze zwischen einem erlaubten Gestaltungsmuster und einem Dark Pattern dann überschritten ist, wenn die angewandte Praktik die Entscheidungsfähigkeit der Nutzer:innen maßgeblich beeinflusst, um ihr Verhalten zu kontrollieren und sie zu einer unbeabsichtigten Entscheidung zu bewegen, die für sie negative Folgen hat. Zu diesem Zweck werden im Erwägungsgrund die folgenden Praktiken als Beispiele aufgeführt:

- Die wiederholte Aufforderung der Nutzer:innen, eine Auswahl zu treffen, obwohl diese bereits getroffen wurde.
- Erheblich aufwendigeres Verfahren für die Stornierung eines Dienstes als für dessen Anmeldung.

---

<sup>26</sup> Die Leitlinien der Kommission zur Auslegung und Anwendung der Richtlinie 2005/29/ EG über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt, ABl 2021 C 526/1, unter 4.2.7

- Die Gestaltung bestimmter Wahlmöglichkeiten schwieriger oder zeitaufwändiger als andere.
- Unverhältnismäßige Erschwerung des Abbruchs eines Kaufs oder der Abmeldung einer bestimmten Online-Plattform.
- Verbraucher:innen in die Lage versetzen, Fernabsatzverträge mit Unternehmern abzuschließen, und die Nutzer:innen in die Irre führen, indem sie zu Entscheidungen über Transaktionen veranlasst werden.
- Unverhältnismäßige Beeinflussung der Entscheidungsfindung der Nutzer:innen durch Standardeinstellungen, die nur sehr schwer zu ändern sind, und dadurch Verzerrung und Beeinträchtigung der Autonomie, der Entscheidungsfreiheit oder der Wahlmöglichkeiten der Nutzer:innen.

Der DSA bestimmt auch, dass dieses Verbot der Verwendung von Dark Patterns nicht für Praktiken gilt, die unter die UGP-Richtlinie oder die DSGVO fallen (Artikel 25 Absatz 2 DSA). Mit anderen Worten: Die Bestimmung des DSA gilt nur, wenn die betreffende Geschäftspraktik nicht bereits durch die UGP-RL oder die DSGVO abgedeckt ist. Dies führt zu einer rechtlichen Unklarheit, da die in dem Erwägungsgrund aufgeführten Praktiken auch als irreführende oder aggressive Geschäftspraktiken im Sinne der UGP-RL angesehen werden können. Nach Art. 6 UGP-RL sind Geschäftspraktiken irreführend, wenn sie falsche oder unwahre Angaben enthalten oder sonst geeignet sind, den Durchschnittsverbraucher zu täuschen und ihn dadurch zu einer Kaufentscheidung zu veranlassen, die er ansonsten nicht getroffen hätte.

Ebenfalls nach Art. 7 UGP-RL gilt eine Geschäftspraxis als irreführend, wenn sie im konkreten Fall unter Berücksichtigung aller tatsächlichen Umstände und der Beschränkungen des Kommunikationsmediums wesentliche Informationen vorenthält, die der Durchschnittsverbraucher je nach den Umständen benötigt, um eine informierte geschäftliche Entscheidung zu treffen, und die somit einen Durchschnittsverbraucher zu einer geschäftlichen Entscheidung veranlasst oder zu veranlassen geeignet ist, die er sonst nicht getroffen hätte.

Dies wirft die Frage auf, wenn eine Online-Plattform, die in den Anwendungsbereich des DSA fällt, Dark Patterns verwendet, um die Entscheidungsfreiheit ihrer Nutzer:innen zu beeinflussen und sie zu einer Transaktionsentscheidung zu bewegen, welche Sanktions- und Durchsetzungsregelung für diese Praktik gelten würde. Nach der Regelung unter dem DSA ist zunächst zu prüfen, ob die UGP-RL auf die Praktik anwendbar ist. Es besteht daher die Gefahr, dass Art. 25 Abs. 2 DSA vielmehr die Rechtsdurchsetzung erschwert. Zudem könnte dies dazu führen, dass die DSA-Behörden auch eine lauterkeits- und datenschutzrechtliche Prüfung durchführen müssen, ohne für diese Bereiche zuständig zu sein.

#### DSA und DMA für „Torwächter“

Am 6. September 2023 ernannte die Europäische Kommission sechs Torwächter im Rahmen des Digital Markets Act (DMA): Alphabet, Amazon, Apple, ByteDance, Meta und Microsoft. Insgesamt wurden 22 zentrale Plattformdienste benannt, die von diesen Torwächtern angeboten werden. Soziale Netzwerke wie TikTok, Facebook,

Instagram, YouTube und LinkedIn zählen dazu.<sup>27</sup> Als Torwächter nach dem DMA wird ein Unternehmen, wenn es einen erheblichen Einfluss auf den Binnenmarkt hat, einen zentralen Plattformdienst bereitstellt, der gewerblichen Nutzer:innen als wichtiger Zugangstor zu Endnutzer:innen dient, und hinsichtlich seiner Tätigkeiten eine gefestigte und dauerhafte Position innehat oder absehbar ist, dass es eine solche Position in naher Zukunft erlangen wird.<sup>28</sup>

Torwächter verarbeiten personenbezogene Daten von Endnutzer:innen zum Zweck der Bereitstellung von Online-Werbung. Darüber hinaus stellen Dritte, die die Torwächter-Plattform nutzen, den Torwächtern auch personenbezogene Daten ihrer eigenen Endnutzer:innen zur Verfügung, um die Plattformdienste nutzen zu können. Dies verschafft den Torwächtern einen potenziellen Marktvorteil, da ihr Geschäftsmodell datenbasiert ist. Daher verlangt der DMA von den Torwächtern, dass sie die Einwilligung der Endnutzer:innen gemäß der DSGVO einholen, um personenbezogene Daten für ihre datengestützten Geschäftspraktiken zu verarbeiten, und schränkt die Rechtsgrundlagen ein, auf die sie sich dabei stützen können. Folglich sollten Torwächter den Endnutzer:innen die Möglichkeit geben, frei zu entscheiden, ob sie solchen Datenverarbeitungen und Opt-in-Praktiken zustimmen, indem sie eine weniger personalisierte, aber gleichwertige Alternative anbieten, ohne die Nutzung des Kerndienstes der Plattform oder bestimmter Funktionen von der Einwilligung des:der Endnutzer:in abhängig zu machen. Hierzu könnte neben der Einwilligung nach dem DSA auch Artikel 6 Absatz 1 Buchstaben c, d und e der DSGVO und nicht Artikel 6 Absatz 1 Buchstaben b und f der DSGVO als Rechtsgrundlage für die Verarbeitung verwendet werden.

Wenn die Einwilligung des Users für die Datenverarbeitung erforderlich ist, muss die Einwilligung die Bedingungen der DSGVO erfüllen.<sup>29</sup> Torwächter müssen die Endnutzer:innen über die Folgen einer Nichteinwilligung informieren. Damit die Einwilligung freiwillig bleibt, müssen sie eine weniger personalisierte, aber gleichwertige Alternative anbieten, ohne die Nutzung des Kerndienstes der Plattform oder bestimmter Funktionen von der Einwilligung des:der Endnutzer:in abhängig zu machen.<sup>30</sup>

Der Digital Services Act (DSA) konzentriert sich stärker auf die Regulierung von Online-Inhalten und betrifft mehr Social Media Plattformen. Die Regulierung gilt bereits für die „sehr großen Online-Plattformen“ (VLOPs). LinkedIn, Facebook, Instagram, TikTok, YouTube, Snapchat und X werden im Rahmen des DSA als VLOPs bezeichnet.<sup>31</sup> Es gibt einige Überschneidungen zwischen Unternehmen, die unter dem DMA als Torwächter und unter dem DSA als VLOPs bezeichnet werden. Unternehmen, die beiden Gesetzen unterliegen, müssen beide Vorschriften einhalten. Nach Art. 28 DSA dürfen Anbieter von Online-Plattformen auf ihrer Schnittstelle keine Werbung anzeigen, die auf Profiling im Sinne der DSGVO unter

---

<sup>27</sup> (Europäische Kommission, 2024a) [https://digital-markets-act.ec.europa.eu/gatekeepers\\_en](https://digital-markets-act.ec.europa.eu/gatekeepers_en)

<sup>28</sup> Artikel 3 Absatz 1 Digital Markets Act

<sup>29</sup> Erwägungsgrund 36 Digital Markets Act

<sup>30</sup> Erwägungsgrund 37 Digital Markets Act

<sup>31</sup> (Europäische Kommission, 2024a, 2024c) <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

Verwendung personenbezogener Daten des Users beruht, wenn sie hinreichende Gewissheit haben, dass der betreffende User minderjährig ist. Darüber hinaus ist Werbung auf der Grundlage von „Profiling“ von Daten der „besonderen Kategorie“ im Sinne der DSGVO nach dem DSA unzulässig.<sup>32</sup> Mit dem DSA werden Transparenzanforderungen für auf allen Online-Plattformen angezeigte Werbung sowie zusätzliche Transparenzanforderungen und Anforderungen zur Durchführung einer Risikobewertung für potenzielle systemische Risiken für VLOPs eingeführt. Die VLOPs sind nach dem DSA auch verpflichtet, ein Archiv für den gesamten Zeitraum, in dem sie Werbung anzeigen, und für ein Jahr nach der letzten Anzeige der Werbung auf ihren Online-Schnittstellen zu erstellen und öffentlich zugänglich zu machen. Dieses Archiv enthält Informationen wie den Inhalt der Werbung, die natürliche oder juristische Person, in deren Namen die Werbung geschaltet wurde, den Zeitraum, in dem die Werbung geschaltet wurde, ob die Werbung für eine oder mehrere bestimmte Nutzergruppen bestimmt war und die Gesamtzahl der erreichten Nutzer:innen.<sup>33</sup>

### Verbraucherleitbilder

Als Maßstab für die Beurteilung der Auswirkungen von Geschäftspraktiken in UGP-RL werden unterschiedliche Verbraucherleitbilder genutzt: (1) der sogenannte Durchschnittsverbraucher, (2) der schutzbedürftige Verbraucher.<sup>34</sup>

### Der Durchschnittsverbraucher

Die UGP-RL sieht den „Durchschnittsverbraucher“ als Maßstab für die Beurteilung der Auswirkungen einer Geschäftspraktik. Dieses Konzept wurde bereits vor der Verabschiedung der UGP-RL vom EuGH entwickelt (in C-210/96 - Gut Springenheide und Tusky / Oberkreisdirektor des Kreises Steinfurt) und später durch die UGP-RL kodifiziert. Danach ist unter einem Durchschnittsverbraucher eine situationsadäquat aufmerksame Person zu verstehen. Der Durchschnittsverbraucher im Sinne der UGP-RL ist stets in der Lage, sich die verfügbaren Informationen zu beschaffen und auf dieser Grundlage vernünftig zu handeln.<sup>35</sup> Aufgrund spezifischer Interessen können bestimmte Verbraucher:innen über spezifische Kenntnisse und Eigenschaften verfügen, die ein Durchschnittsverbraucher nicht unbedingt hat. Nach den Leitlinien der Kommission zur Auslegung und Anwendung der Richtlinie 2005/29/EG wirken sich daher die spezifischen Interessen bestimmter Verbrauchergruppen unmittelbar auf die Beurteilung der Auswirkungen einer Geschäftspraktik aus. Wenn keine spezifische Gruppe von Verbraucher:innen identifiziert werden kann, sollte der fiktive allgemeine Durchschnittsverbraucher die Grundlage für die Beurteilung sein. Beispielsweise hat ein nationales Gericht im Zusammenhang mit irreführender Werbung für Babywindeln, in der ein Zusammenhang zwischen Allergien und den Windeln des betreffenden Gewerbetreibenden hergestellt wurde, als

---

<sup>32</sup> Artikel 26 Absatz 3 Digital Services Act

<sup>33</sup> Artikel 39 Digital Services Act

<sup>34</sup> Urteil des Gerichtshofs vom 16. Juli 1998, Gut Springenheide und Tusky/Oberkreisdirektor des Kreises Steinfurt - Amt für Lebensmittelüberwachung, C-210/96, ECLI:EU:C:1998:369, Rn. 31

<sup>35</sup> Die Leitlinien der Kommission zur Auslegung und Anwendung der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt, ABl 2021 C 526/1, unter 2.5 Durchschnittsverbraucher

Durchschnittsverbraucher Eltern von Kleinkindern angesehen, die keine besonderen Kenntnisse über Allergien haben.<sup>36</sup>

Es ist auch möglich, dass verschiedene Gruppen von Verbrauchern von ein und derselben Geschäftspraktik betroffen sind. So kann es beispielsweise einen Durchschnittsverbraucher geben, an den sich die Praxis richtet, und gleichzeitig kann die Praxis auf eine Gruppe von schutzbedürftigen Verbrauchern ausgerichtet sein. Grundsätzlich sollten bei der Beurteilung die Verbraucher:innen berücksichtigt werden, die durch die Praxis tatsächlich erreicht wurden, unabhängig davon, ob es sich um die Verbraucher:innen handelt, die der Gewerbetreibende zu erreichen beabsichtigte.

### Leitbild des schutzbedürftigen Verbrauchers

Die UGP-RL beruht auf dem Gedanken, dass für Verbraucher:innen, die einer der in Artikel 5 Absatz 3 genannten Gruppen zuzurechnen sind, ein höheres Schutzniveau gewährleistet werden sollte als für den in Artikel 5 Absatz 2 genannten „Durchschnittsverbraucher“. In diesem Artikel werden Verbraucher:innen ausschließlich wegen ihrer „geistigen oder körperlichen Gebrechen, Alter oder Leichtgläubigkeit“ als schutzbedürftig eingestuft. Der Begriff der "Leichtgläubigkeit" wird im Zusammenhang mit Verbrauchergruppen verwendet, die dazu neigen, gewissen Behauptungen leichter zu glauben. Ziel des Begriffs ist der Schutz der Mitglieder einer Gruppe, die aus einem beliebigen Grund besonders anfällig für die Beeinflussung durch bestimmte Geschäftspraktiken sind. Theoretisch kann jeder Verbraucher zu dieser Gruppe gehören.<sup>37</sup>

Im Einklang mit der Position der Europäischen Kommission in den Leitlinien zur Auslegung und Anwendung der Richtlinie 2005/29/EG ist der Begriff der Schutzbedürftigkeit in der UGP-RL dynamisch und situationsabhängig, was bedeutet, dass ein Verbraucher in einer bestimmten Situation schutzbedürftig sein kann, in einer anderen Situation jedoch nicht. Beispielsweise können bestimmte Verbraucher:innen in einem digitalen Umfeld besonders anfällig für personalisierte Überzeugungspraktiken sein, während dies in einem Ladengeschäft oder einem anderen Offline-Umfeld nicht der Fall ist.<sup>38</sup> Im Sinne eines verbraucherfreundlichen und modernen Ansatzes sollte das Konzept der Schutzbedürftigkeit überdacht werden, da die zunehmende Erhebung personenbezogener Daten von Verbraucher:innen bei der Nutzung von Online-Diensten und die Entwicklungen im Bereich der Dark Patterns zu einer erhöhten Schutzbedürftigkeit der Verbraucher:innen führen.

---

<sup>36</sup> Entscheidung des Marknadsdomstolen vom 4. Juli 2012

<sup>37</sup> Die Leitlinien der Kommission zur Auslegung und Anwendung der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt, ABl 2021 C 526/1, unter 2.6 Schutzbedürftige Verbraucher

<sup>38</sup> Die Leitlinien der Kommission zur Auslegung und Anwendung der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt, ABl 2021 C 526/1, unter 4.2.7 zu Dark Patterns

## 2.4 Erhebung

Die Erhebung fokussiert sich bei Dark Patterns auf drei sehr unterschiedliche Bereiche. (1) Die zwei Case Studies im Online-Shopping betreffen die zwei Plattformen Temu und SHEIN. Beide Anbieter wurden 2024 von der Europäischen Kommission als Very Large Online Platform (VLOP) im Sinne des DSA deklariert; Temu im Mai 2024, SHEIN Ende April 2024. (2) Zum Themenbereich „Flugbuchungen“ wurden vier Case Studies durchgeführt – dieser Bereich ist von Relevanz, weil er die Schwierigkeit der Bewertung von Dark Patterns in Prozessen gut illustriert und zahlreiche Beschwerden von Konsumentinnen und Konsumenten wie zu gebuchten Zusatzservices eine Folge von Dark Patterns sein könnten. Es werden deshalb die Flugbuchungsprozesse bei Ryan Air, Austrian Airlines, Wizz Air und Opodo exemplarisch dokumentiert und hinsichtlich ihrer Gestaltung vergleichend analysiert. (3) Letztlich wurde das Thema der verhaltensbasierten Werbung auf Social Media durch Analyse der Registrierungsprozesse auf TikTok und Instagram behandelt – auch hier werden für den Zweck Dark Patterns eingesetzt.

Die Frage, ob Flugbuchungsplattformen als Online-Plattformen im Sinne des DSA anzusehen sind, ist nicht einfach zu beantworten. Denn nach Art. 3 lit. i DSA ist eine „Online-Plattform“ ein Hosting-Dienst, der im Auftrag eines Users Informationen speichert und öffentlich verbreitet, sofern es sich bei dieser Tätigkeit nicht nur um eine unbedeutende und reine Nebenfunktion eines anderen Dienstes oder um eine unbedeutende Funktion des Hauptdienstes handelt, die aus objektiven und technischen Gründen nicht ohne diesen anderen Dienst genutzt werden kann, und sofern die Integration der Funktion der Nebenfunktion oder der unbedeutenden Funktion in den anderen Dienst nicht dazu dient, die Anwendbarkeit dieser Verordnung zu umgehen. Unklar ist, inwieweit diese Buchungsplattformen die von ihren Usern erstellten Daten und Informationen speichern und veröffentlichen. Aus diesem Grund kann die Verwendung von Dark Patterns durch diese Unternehmen nur im Rahmen der UGP-RL und der DSGVO bewertet werden.

Als Online-Plattformen können beispielsweise digitale Marktplätze wie Amazon oder Social-Media-Netzwerke wie Instagram eingeordnet werden. Diese werden in **Kapitel 5 Registrierungsprozesse auf Social Media** näher betrachtet. Für die Überprüfung und Dokumentation der Standard-Privatsphäre Einstellungen von verschiedenen VLOPs (Very Large Online Platforms) wie Google, Meta und TikTok wurde im Rahmen der Studie ein Test-Smartphone erstanden. Dieses Testgerät wurde für eine 16-jährige Persona („Anna“) eingerichtet mit dem Geburtsdatum 01.03.2008. Die Person ist demnach noch nicht volljährig. Mit diesem Profil, das in den Systemeinstellungen des Smartphones (Apple ID) hinterlegt war, wurden in Folge diverse Onlinekonten eröffnet und deren Standardeinstellungen dokumentiert. Das verwendete Smartphone ist ein Apple SE mit einer österreichischen Prepaid SIM-Karte.

Die Erhebung ist nicht vollständig im Sinne eines Anspruchs auf Aussagen zu Online-Shopping in Österreich oder auch Flugbuchungen insgesamt – es wurden exemplarisch Case Study-Fälle gesucht, um Gemeinsamkeiten und Unterschiede bei der Gestaltung von Website-Design und Prozessen hervorheben zu können.

Dazu kommt, dass die Analyse sich durch zwei Zugänge unterscheidet. Entschieden wurde mit der aktualisierten Taxonomie von Dark Patterns von Harry Brignull<sup>39</sup> zu arbeiten, um mögliche Verstöße zu identifizieren. Gleichzeitig ist es aus einer juristischen Perspektive noch nicht möglich all jene Dark Patterns, die laut Taxonomie als solche gelten, auch als rechtlich laut DSA verbotene Praktiken zu bezeichnen. Dafür fehlt es aktuell noch an Rechtsprechung – und insofern werden die rechtlichen Einschätzungen im Folgenden getrennt aufgeführt und bedienen sich nur ausgewählter Terminologien von Dark Patterns. Trotzdem wurde die Entscheidung getroffen Dark Patterns in einem breiten Sinne zu identifizieren, dies kann als möglicher Startpunkt für rechtliche Überlegungen und Maßnahmen dienen.

### Liste erhobener Dark Patterns

Im Folgenden werden eine Reihe an Design Entscheidungen (Dark Patterns) erwähnt, in Anlehnung an die erweiterte Taxonomie von Brignull.<sup>40</sup> All diese Dark Patterns wurden im Laufe der Erhebung gefunden und in den folgenden Kapiteln dokumentiert:

- **Bait-and-Switch:** Auch Lockvogeltrick genannt, z. B. die Bewerbung eines „Gratis“-Angebots, das sich als kostenpflichtig herausstellt.
- **Comparison Prevention und Exploiting Vulnerabilities in Budgeting:** Die Verhinderung von Vergleichen oder das Verhindern von „Mental Budgeting“, z. B. über die Verhinderung von Preisvergleichen oder den Einsatz von unvergleichbaren Tarifpaketen.
- **Confirm Shaming und Emotional Stirring:** Das Drängen zur Annahme über emotionale Botschaften oder Manipulation, z. B. über den Einsatz tendenziöser Formulierungen und das Hervorrufen von Scham- oder Schuldgefühlen.
- **Deliberate Misdirection und Tagging:** Absichtliche Fehlleitung, z. B. die tendenziöse Gestaltung von Buttons, Ablehnung nicht in Form eines Buttons, sondern nur als Link.
- **Disguised Ads:** Versteckte oder getarnte Werbung, z. B. über Angebote, die sich als Produktwerbung herausstellen.
- **Fake Scarcity:** Vorgetäuschte Knappheit, z. B. über Anzeigen, die suggerieren, dass sich viele Menschen ein Angebot gerade ansehen.
- **Fake Social Proof:** Vorgetäuschter sozialer Druck, z. B. über die Behauptung, dass tausende Andere, dieses Produkt gekauft haben.
- **Fake Urgency:** Vorgetäuschte Zeitnot oder Dringlichkeit, z. B. über Countdown Timer oder zeitlich begrenzte Angebote.
- **Forced Action:** Erzwungene Handlungen, z. B. wenn ein Prozess nur über eine Anmeldung weitergeführt werden kann.
- **Hard to Cancel:** Etwas schwer rückgängig zu machen oder zu stornieren, z. B. die erschwerte Löschung eines Benutzerkontos.
- **Hidden Costs:** Versteckte Kosten, z. B. über die Bewerbung „kostenloser“ Produkte, die aber nicht verfügbar sind.

---

<sup>39</sup> (Brignull, 2022), online: <https://www.deceptive.design/types> (18.06.2024).

<sup>40</sup> (Brignull, 2022)

- **Hidden Subscription:** Verstecktes Abonnement, z. B. über Club-Mitgliedschaften, bei denen unklar ist, dass es sich um Abos handelt.
- **Nagging:** Wiederholte Aufforderungen, z. B. über das wiederholte Nachfragen, ob eine Zusatzleistung gebucht werden soll.
- **Obstruction und Visual Interference:** Behinderung bzw. visuelle Störung, z. B. über die wiederholte Unterbrechung eines Buchungsprozesses, oder das wiederholte Erscheinen eines Pop-Up-Fensters.
- **Preselection:** Vorauswahl, z. B. zum Erhalt eines Newsletters.
- **Privacy Zuckering:** Mechanismen, die User zur Preisgabe privater Daten anstiften, z. B. über das wiederholte Anfordern privater Informationen oder das wiederholte Fragen zum Teilen der persönlichen Kontakte.
- **Sneaking:** In den Warenkorb schleichen, z. B. über die automatische Auswahl einer Premium-Mitgliedschaft, beim Buchen eines Fluges.
- **Trick Wording:** Fangfragen oder Trickfragen, z. B. über die verwirrende Formulierung von Vertragsbedingungen.

### 3 Online-Shopping & Dark Patterns

Der Onlinehandel hat in den letzten Jahren einen beispiellosen Aufschwung erlebt und ist heute aus dem täglichen Leben nicht mehr wegzudenken. Konsument:innen können mittlerweile eine Vielzahl von Produkten bequem von zu Hause aus bestellen, sei es Kleidung, Elektronik, Haushaltswaren oder Lebensmittel. Online-Shopping-Plattformen wie Temu und SHEIN bieten eine beeindruckende Vielfalt an Produkten und nutzen moderne Technologien, um das Einkaufserlebnis kontinuierlich zu verbessern. Gleichzeitig haben sich die Wettbewerbsbedingungen im Onlinehandel verschärft, was nicht zuletzt auf das Aufkommen zahlreicher neuer Marktteilnehmer und die fortschreitende Digitalisierung zurückzuführen ist.

Mit diesen Entwicklungen geht jedoch auch eine besorgniserregende Tendenz einher: die Anwendung manipulativer Designstrategien: Dark Patterns. Zu den häufigsten Dark Patterns, die im Bereich Online-Shopping eingesetzt werden, gehören gefälschte Countdown-Timer, aufdringliche Pop-Up-Fenster und irreführende Anzeigen sozialer Bestätigung (Fake Social Proof). Trotz der zahlreichen Regulierungsmaßnahmen, die die Europäische Union in den letzten Jahren ergriffen hat, um den Schutz der Konsument:innen im digitalen Raum zu verbessern wie Informationspflichten und Transparenzanforderungen, zeigt auch die vorliegende Analyse den weitreichenden Einsatz von Dark Patterns, die zu unerwarteten Kosten, enttäuschten Erwartungen und Verwirrung von Konsument:innen führen.

Im Zuge der Studie wurden die Websites folgender Anbieter genauer untersucht: Fabletics, helloFresh, Mr. Gugu, Donner.de, Barfußschuhe Roeck, Zalando, Recentia.at, eis.at, Temu und SHEIN. Bei all diesen Websites wurden Dark Patterns gefunden und mithilfe des Open Source Tools „Eagle“ dokumentiert. Im Detail werden hier jene zwei dieser Anbieter als Case Studies analysiert, SHEIN und Temu, die seit Kurzem (April bzw. Mai 2024) auch offiziell von der Europäischen Kommission als VLOP (Verly Large Online Platform) klassifiziert wurden.<sup>41</sup>

Die beiden chinesischen Unternehmen SHEIN und Temu zeichnen sich durch teils ähnliche Taktiken in der Gestaltung ihrer Websites sowie der Werbung aus. Bei beiden Anbietern wurden zahlreiche Dark Patterns gefunden, darunter Zeitdruckelemente wie Countdowns und Timer, zahlreiche Pop-Ups (Nagging, Obstruction) und die weitreichende Bewerbung von Rabatten. Teils besteht Verdacht auf Bait-and-Switch-Angebote, auch Lockvogelangebote genannt, bei denen ein beworbener Rabatt nicht wirklich eingelöst werden kann, bzw. zu unintendierten Folgen für Konsument:innen führt.

Im Folgenden werden die Anbieter Temu und SHEIN genauer beleuchtet und die dokumentierten User-Interface und User-Experience-Entscheidungen der Anbieter in einem zweiten Schritt analysiert. Die Analyse zeigt, dass eine gewisse Überladung mit Angeboten, Farben, Pop-Ups und anderen Elementen zur Normalität auf diesen Plattformen geworden ist.

---

<sup>41</sup> (Europäische Kommission, 2024b)

### 3.1 Case Study „Temu“

Temu, ein aufstrebender chinesischer E-Commerce-Riese, ist seit einiger Zeit auch in Österreich aktiv und erregt zunehmend Aufmerksamkeit durch die aggressiven Werbestrategien, die vor allem auf Social Media sehr präsent sind. Als Tochterunternehmen der PDD Holdings Inc., die auch die bekannte Plattform Pinduoduo (PDD Holdings) betreibt, hat sich Temu schnell auch am europäischen Markt etabliert, auch über seine breite Produktpalette, die von Elektronik über Mode bis hin zu Haushaltswaren reicht.

Kritik erntet der Konzern wegen der aggressiven Preisstrategien, die aus Rabatten, Sonderangeboten und Promotionen besteht. Der Konzern setzt auf stark lokalisierte Werbung, und Social Media und Influencer Marketing und verfolgt über diese Strategien ambitionierte Wachstumspläne im europäischen E-Commerce-Markt.

#### 3.1.1 Dokumentation

**Dokumentationsgrundlage:** Screenshots der Website <https://www temu.com/> von 07.05.2024 und Oktober und Juli 2023. Bitte zu beachten, dass die Website sowie die App regelmäßig verändert werden und die Heranziehung der Beispiele insofern nur mit Hinweis auf Datum erfolgen sollte.

Öffnet man die Website von Temu, zeichnet sich diese durch viele unterschiedliche visuelle Reize aus. Teils arbeitet Temu mit Countdowns (kostenloser Versand, der zeitlich begrenzt ist) und Spezialangeboten, wie z.B. zu Black Friday (siehe Abb.1.). Geworben wird mit hohen Rabatten, bis zu minus 90 %.

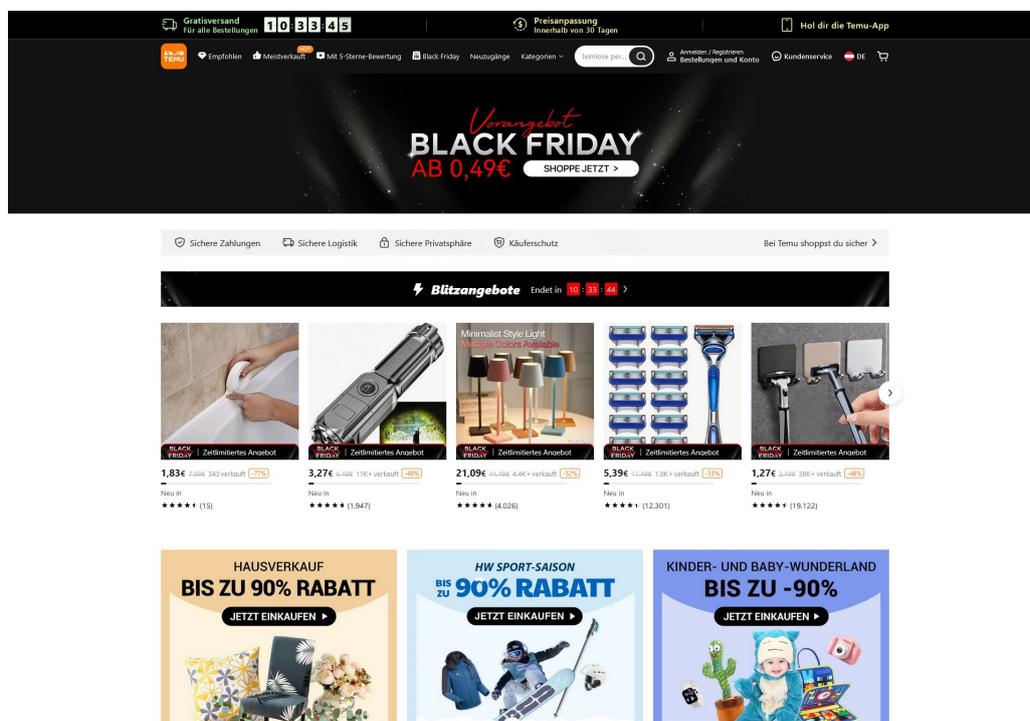


Abbildung 1: Die Startseite von Temu.com (Screenshot, 30.10.2023).

Im Oktober 2023 wurden im Rahmen der Studie einige Werben von Temu Austria dokumentiert, die mit kostenlosen Produkten warben. Es wurden zahlreiche angeblich kostenlose Produkte auf diversen Social Media Plattformen (dokumentiert wurden im Rahmen dieser Studie nur Werbeanzeigen auf Facebook und Instagram) beworben, Stand Juni 2024 sind in der Meta Werbebibliothek über 42.000 Anzeigen von Temu Austria dokumentiert.

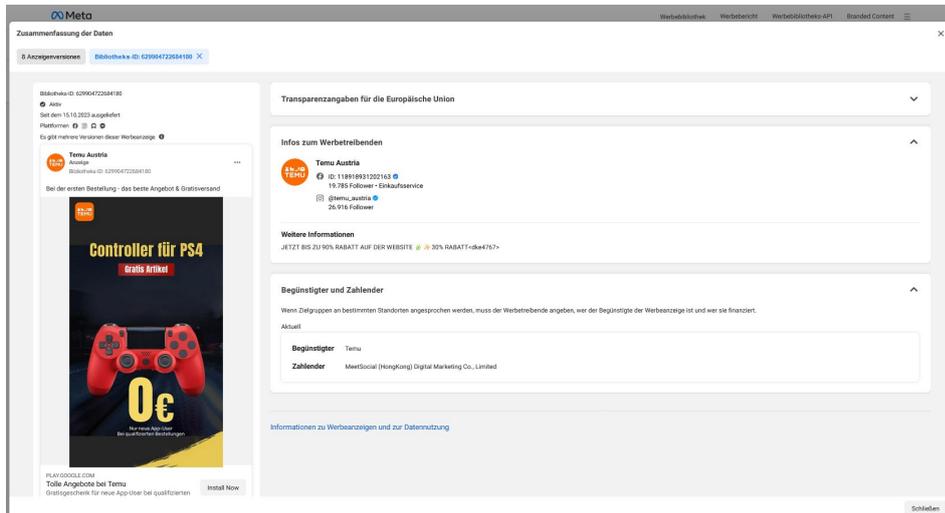


Abbildung 2: Werbeanzeige für PS4-Controller, Temu Austria (Screenshot, 16.10.2023).

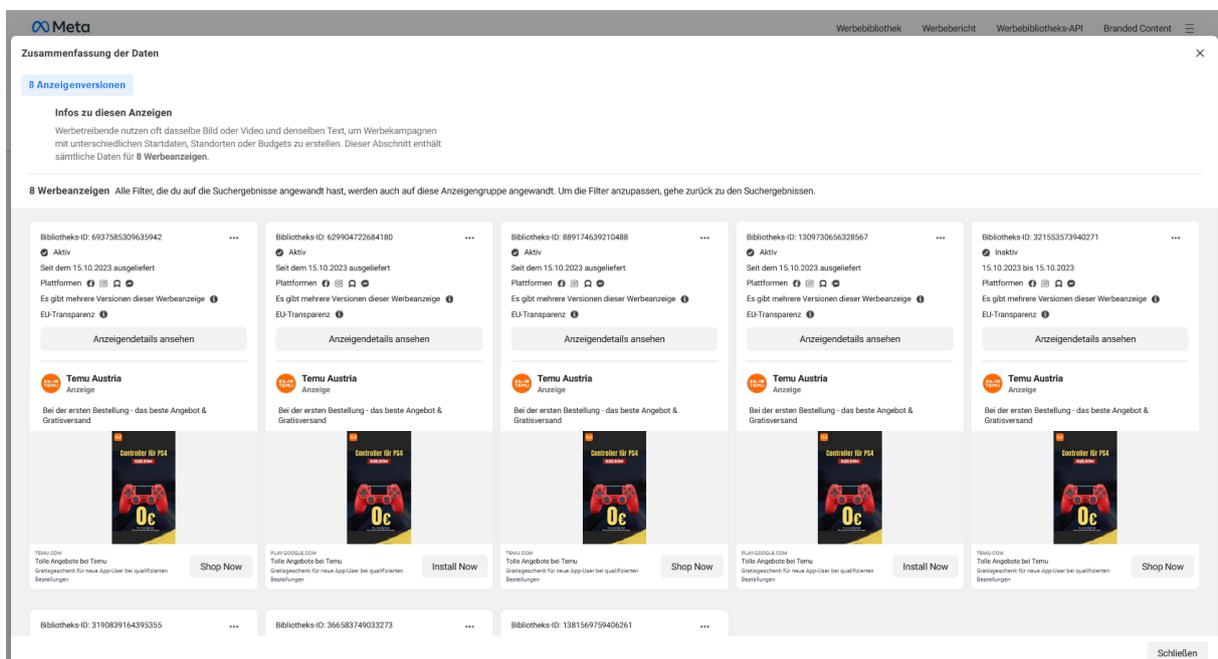


Abbildung 3: Gleiches Werbesujet mit leicht veränderten Texten (Screenshot, 16.10.2023).

Was in der Werbeanzeige als kostenloses Produkt beworben wurde, stellte sich nach dem Klick auf das Angebot als Werbung für ein Gewinnspiel heraus: Auf der Zielseite zu lesen war „Toller Rabatt zu gewinnen, Temu bietet dir einen Sonderrabatt“. Um auf den Sonderrabatt zuzugreifen sollte man einen QR-Code scannen, der zum Download der Temu-App führt. Somit wurde man beim Klick auf die Werbeanzeigen, nicht zum Produkt weitergeleitet, und auch nach einem Download der App landeten User auf einer allgemein Startseite und das Produkt der Werbung war nicht auffindbar.

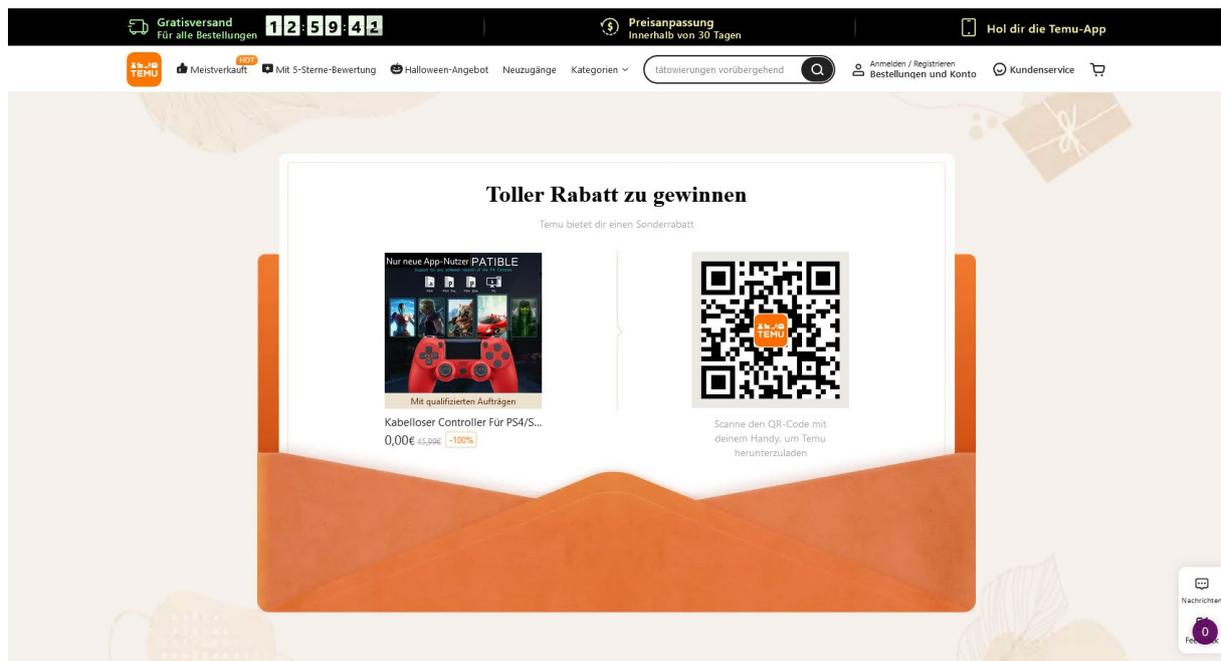


Abbildung 4: Rabatt zu gewinnen, Temu-App (Screenshot, 16.10.2023).

Temu setzt auch zahlreiche Countdowns ein, um Konsument:innen zu raschen Kaufabschlüssen zu bringen. In dem hier dokumentierten Fall sind auf einer Seite drei Countdowns angeführt, zwei beziehen sich auf ein zeitlich begrenztes Angebot für Gratisversand, ein weiterer auf Wertgutscheine, sollte man innerhalb der nächsten 23 Stunden bestellen.

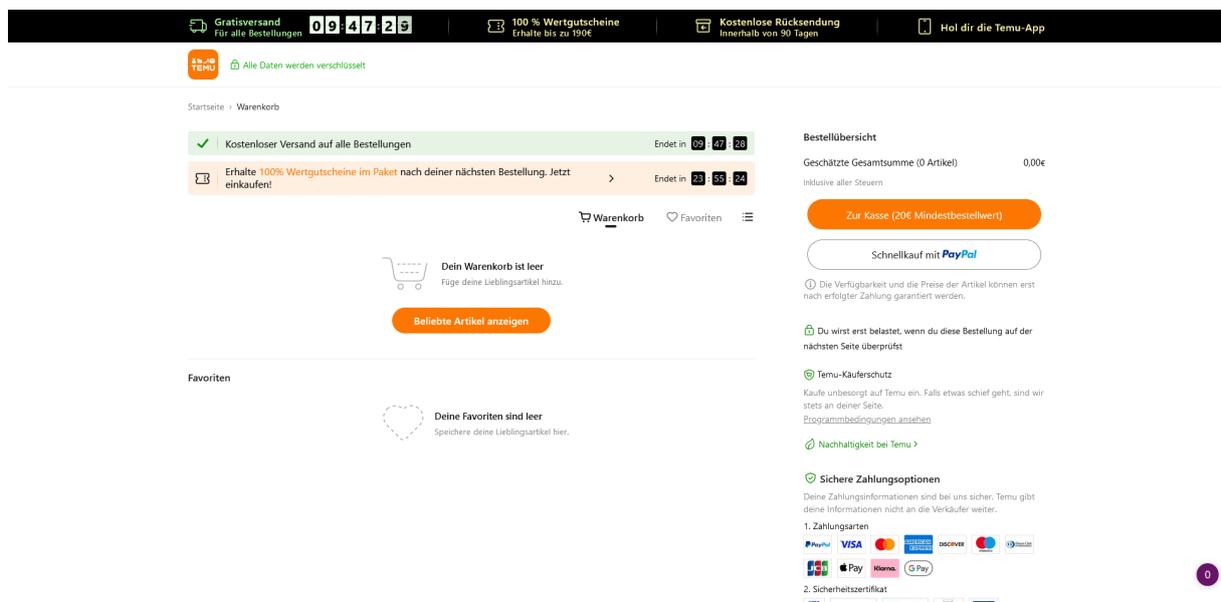


Abbildung 5: Countdowns auf Temu (Screenshot, 09.11.2023).

Auch an anderen Orten auf der Website von Temu kommt es zu Knappheitsanzeigen, darunter Verfügbarkeitsanzeigen, die auch in Kombination mit Countdown-Timern eingesetzt werden. In dem unten angeführten Beispiel ist ersichtlich, dass die als

„Blitzangebot“ gekennzeichneten Waren mit einem Timer versehen sind. Zudem wird angegeben, wie viele tausend Stück des Produktes bereits verkauft wurden.

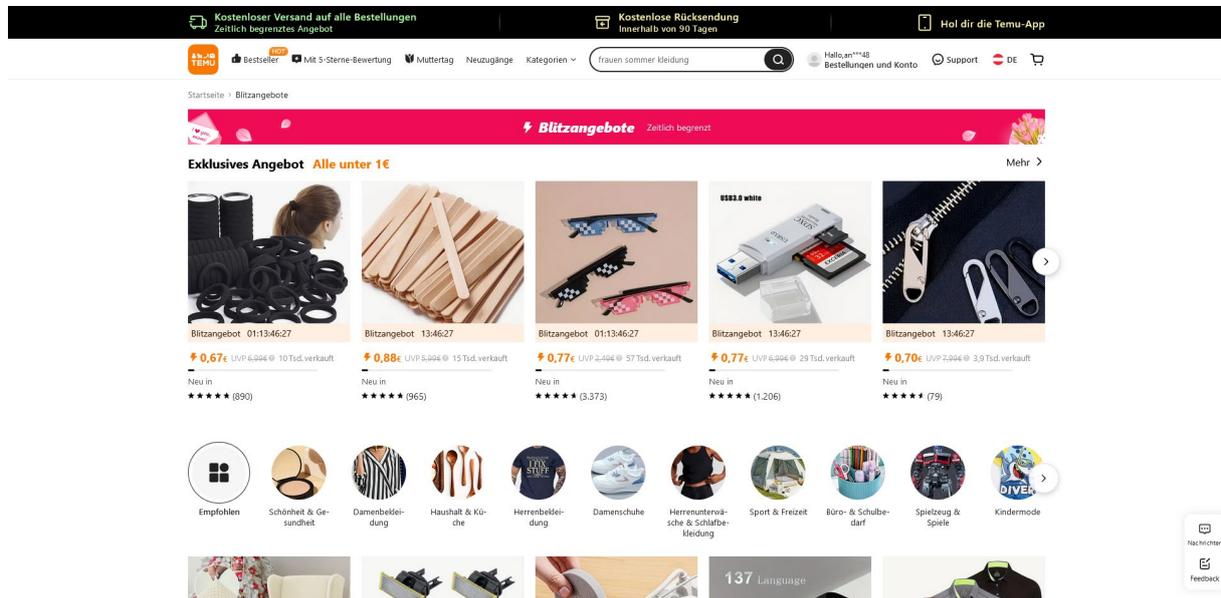


Abbildung 6: Countdowns und Knappheitsanzeigen auf Temu (Screenshot, 07.05.2024).

## Werbung

Stand 07.05.2024 findet man 36.000 Resultate in der Meta Werbebibliothek zu Temu Austria – also dem offiziellen Kanal von Temu für Österreich. Im Juni 2024 sind es schon über 42.000. Diese Zahl macht die extensive Onlinewerbestrategie des Unternehmens sichtbar.

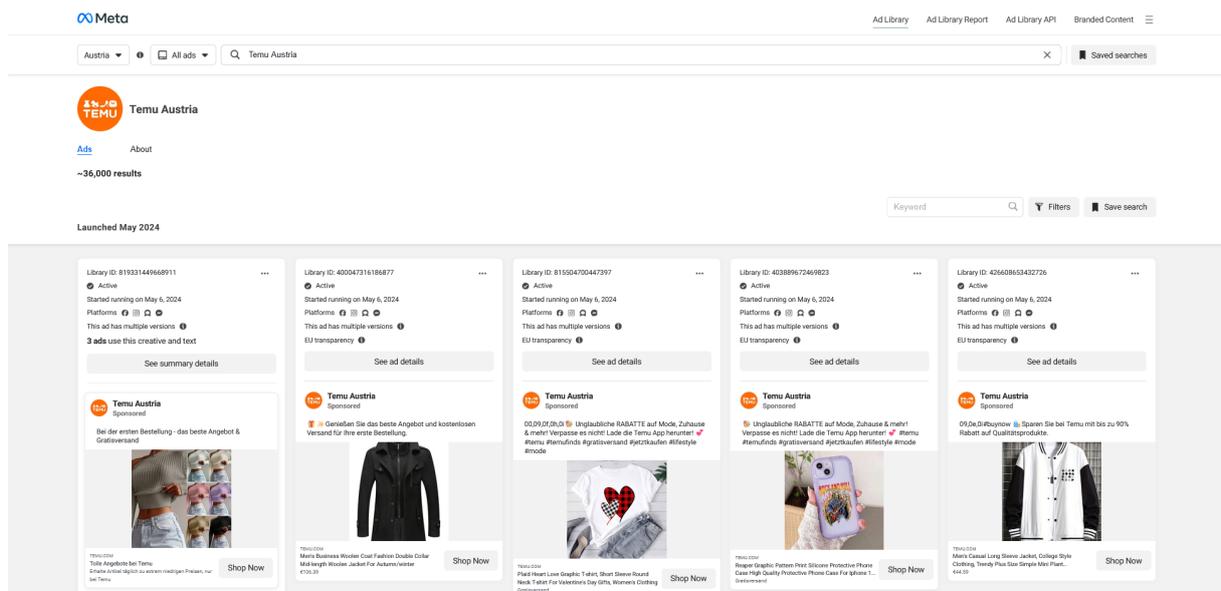


Abbildung 7: Meta-Werbekbibliothek, Temu Austria (Screenshot, 07.05.2024).

Teilweise werden „gratis“ Produkte beworben, wie in dieser Anzeige von April 2024. Bei der Neuregistrierung als Temu-Kunde, bzw. bei Download der Temu-App, werden Neukund:innen zahlreiche Vergünstigungen wie kostenlose Produkte versprochen.

Die Werbemaßnahmen erstrecken sich über den gesamten europäischen Raum, jedoch wurde im Rahmen dieser Studie nur die für Österreich relevante Werbung dokumentiert.

**Summary Data**

Library ID: 1076929456731805

2 ad versions

**Temu Austria**  
Sponsored  
Library ID: 1076929456731805

Im Frühling, bei ersten Bestellung bestes Angebot & Gratisversand

**Schuhkarton**  
Nur neue App-Nutzer  
bei qualifizierten Bestellungen

**0€**

FRÜHLING  
Frühlingsangebote bei Temu  
Einmalig Artikel täglich zu extrem niedrigen Preisen, nur bei Temu.

Shop Now

This ad has multiple versions

1 of 2

**European Union transparency**

We provide additional information for ads that were shown on Meta technologies anywhere in the EU.

**EU ad audience**

Advertisers can target their ads to certain audiences based on their country, region, postal code or city.

**Location**

All location types: Included Excluded

Location: Austria Location type: 11 Included or excluded: 11

Country/Region: Austria

**Age**

18-65+ years old

Advertisers can choose a minimum and maximum age of who will be shown an ad.

**Gender**

All

Advertisers can choose to target their ad based on gender.

**EU ad delivery**

**Reach**

5,349

The number of Accounts Center accounts in the EU that saw this ad at least once. Reach is different from impressions, which may include multiple views of your ads by the same Accounts Center accounts. This metric is estimated.

Reach by location, age and gender

Abbildung 8: Werbeanzeige Temu, „kostenloses Produkt“ (Screenshot, 07.05.2024).

Beim Klick auf die Werbeanzeigen, die kostenlose Produkte bewerben, bzw. die Werbung auf Facebook, wird man zu einer Seite weitergeleitet, die einen auffordert, einen QR-Code einzuscannen und die TEMU-App herunterzuladen. Hat man die App heruntergeladen, ist das angeblich kostenlose Angebot allerdings nicht mehr verfügbar bzw. nicht mehr auffindbar.

Kostenloser Versand auf alle Bestellungen  
Zeitlich begrenztes Angebot

Preisanpassung  
Innerhalb von 30 Tagen

Hol dir die Temu-App

Bestseller Mit 5-Sterne-Bewertung Muttertag Neuzugänge Kategorien

kommerkleidung damen

Anmelden / Registrieren  
Bestellungen und Konto Support

**1 Stück stapelbarer, faltbarer Schuhkarton – frei installierbarer Schuhkarton für Damen und He...**

6,1 Tsd. verkauft ★★★★★ (540)

**KOSTENLOS** UVP 52,79€

Nur neue App-Nutzer | Mit qualifizierten Bestellungen

Scanne diesen QR-Code, um die Temu-App zu erhalten

Hol es dir bei  
Google Play

Laden im  
App Store

Entdecke deine Interessen

Before messy shoes

Adjustable Flow

Nachrichten  
Feedback

Abbildung 9: Temu Website (Screenshot, 07.05.2024).

Diese Werbemaßnahme ist schon im Juli 2023 aufgefallen, auch im Juni 2024 waren noch zahlreiche Werbeanzeigen aktiv, die mit kostenlosen (0 EUR) Produkten warben.

Temu warb auf Instagram und Facebook für den Download der TEMU-App. Die hier dokumentierte Werbung war in Form eines Glücksrades gestaltet, bei dem man um einen Rabatt spielen konnte. Zudem wurden Timer eingesetzt, um auf die begrenzte Verfügbarkeit des Angebotes hinzuweisen. Beim Ausprobieren des Glücksrades musste man einige Male drehen um dann zu dem maximalen Rabatt von -94% zu kommen (siehe Abb. 10-12).



Abbildung 10: Temu Gewinnspiel, Werbeanzeige auf Instagram, (Screenshot, 18.07.2023).

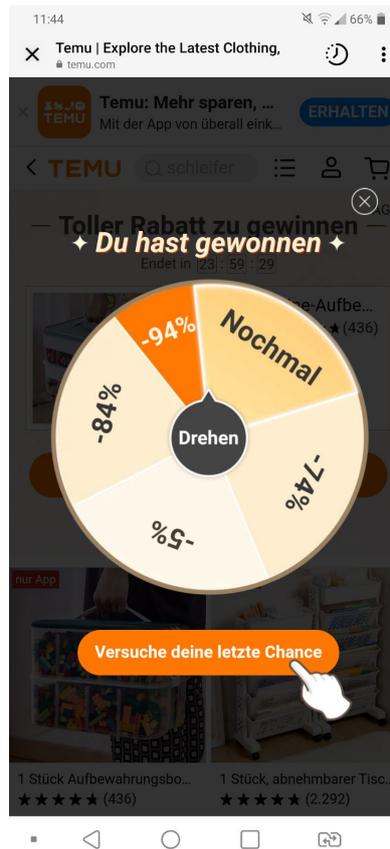


Abbildung 11: Temu Gewinnspiel auf Instagram (Screenshot, 18.07.2023).



Abbildung 12: Temu Instagram Werbung (Screenshot, 18.07.2023).

Hat man den Rabatt erhalten erschien ein Pop-Up mit dem Text „Exklusiver Rabatt – 94 %“ zudem wurde ein Timer in dem Pop-Up angezeigt. Als User hatte man nur die Option auf „In der App erhalten“ den einzigen Button der verfügbar und in orange hervorgehoben war, zu klicken. Wollte man dies nicht, hätte man die gesamte Seite schließen müssen (X rechts über dem weißen Pop-Up im Bild). Diese Schritte sind in Abb. 10-12 dokumentiert.

Diese Art der Werbung erinnert stark an Glücksspiel. Beworben wird eine „100 % GEWINNCHANCE“ unter dem Glücksrad. In jedem Fall kann man gewinnen, die Frage ist nur wie hoch der Rabatt sein wird, den man sich erspielt. Auch Knappheit wird als Taktik angewandt, mit „Versuche deine letzte Chance“ in Abb. 11. drängt die Werbeanzeige den User zu einer Handlung. Wie in Abbildung 12 klar wird, kann der

Gewinn aber nur über eine weitere Aktion des Users, in dem Fall über den Download der App eingelöst werden.



Abbildung 13: Temu mobile Website, (Screenshot, 18.07.2023).

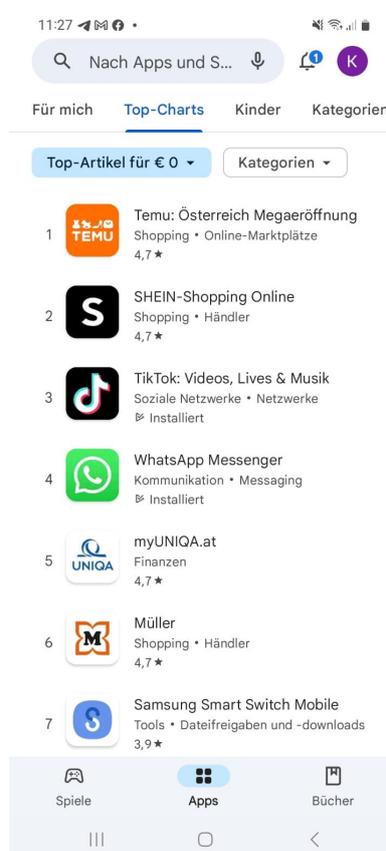


Abbildung 14: App Store Temu-App (Screenshot, 18.07.2023).

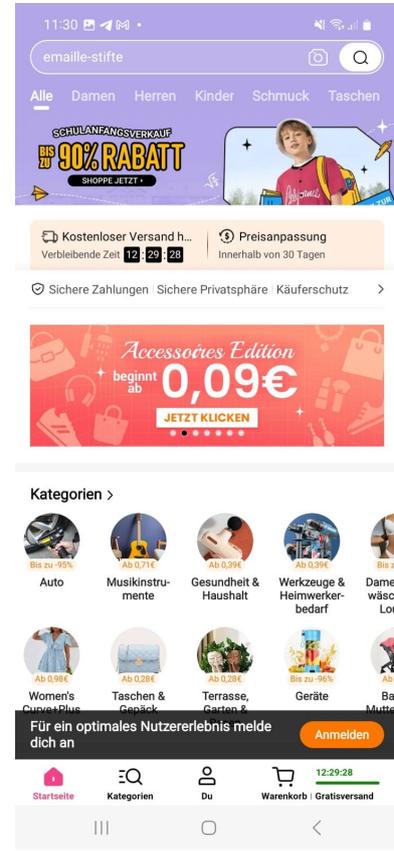


Abbildung 15: Startseite der Temu App nach Download (Screenshot, 18.07.2023).

Beim Klick auf „In der App erhalten“ wurde man auf die mobile Version der Temu Website weitergeleitet (siehe Abb. 13). Danach musste man als User nochmals auf „in der App erhalten“ klicken, um den Rabatt von -94 % auf das Produkt (in diesem Fall Bausteine-Aufbewahrungsboxen) zu erhalten (Abb. 13.). In einem weiteren Schritt wurde man zum App-Store weitergeleitet und musste die TEMU-App herunterladen, um den Rabatt zu erhalten (Abb. 14.). Ist das geschehen, war das Angebot sowie das Angebot mit -94% Rabatt nicht mehr auffindbar (Abb.15.).

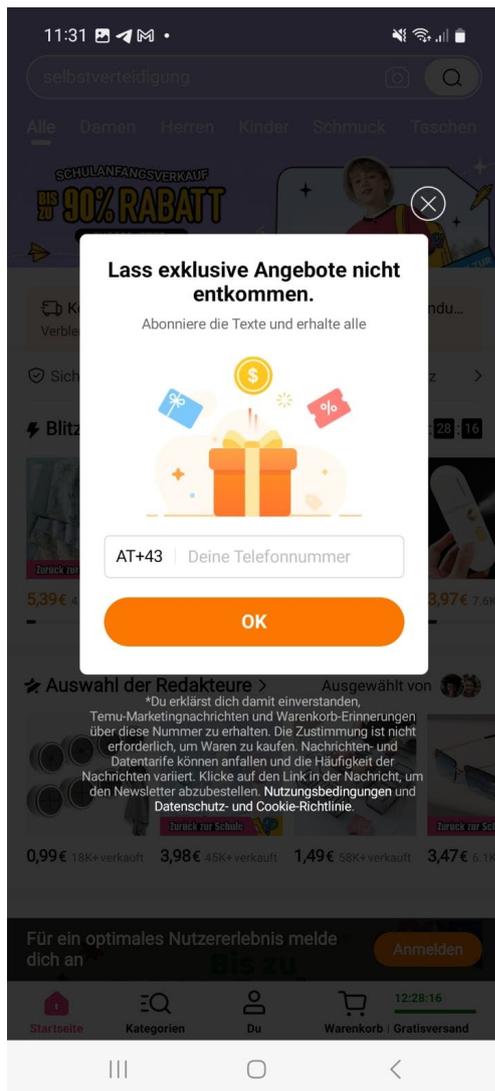


Abbildung 16: Pop-Ups in Temu-App (Screenshot, 18.07.2023).

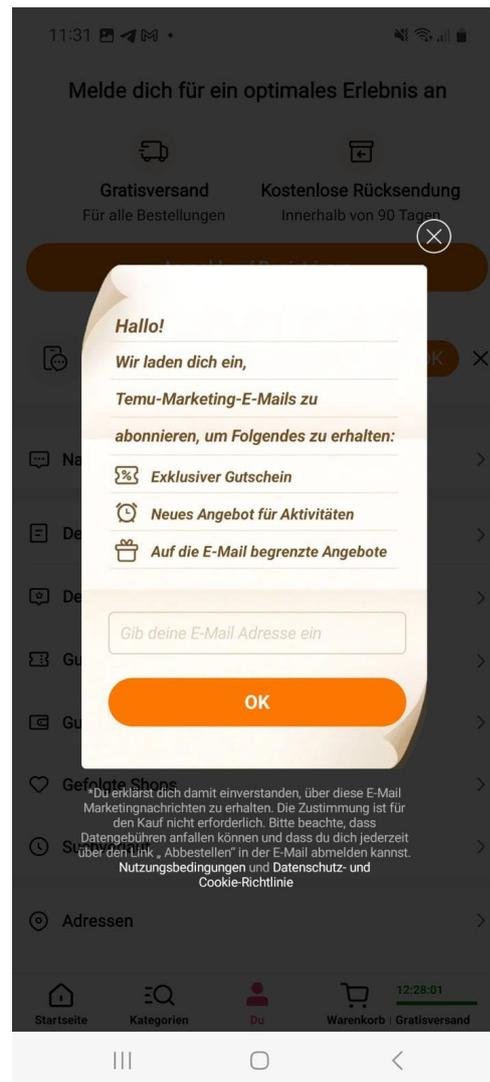


Abbildung 17: Pop-Ups in Temu-App (Screenshot, 18.07.2023).

Nach dem Download und der Installation der Temu-App wurden zahlreiche Pop-Ups angezeigt, die weitere „exklusive Angebote“ bewarben, wenn User ihre Daten preisgeben, wie z. B. die Telefonnummer. Zudem wurden die Temu-Marketing-E-Mails in einem eigenen Pop-Up beworben: Wenn User dem Newsletter von Temu zustimmen, würden sie exklusive Gutscheine, neue und begrenzte Angebote, die nur Newsletter-Abonent:innen vorbehalten sind, erhalten.

### 3.1.2 Analyse

Zusammenfassend zeigt die Analyse, dass die Website von Temu, aber auch die Werbestrategie des Konzerns auf aggressives Marketing sowie auf eine Vielzahl von Dark Patterns setzt, um Kund:innen zum Kauf anzuregen.

Temu wirbt auf Social Media mit angeblich kostenlosen Produkten. Nach dem Klick auf die Anzeige stellt sich heraus, dass es sich um Werbung für ein Gewinnspiel handelt; für die Teilnahme müssen Konsument:innen allerdings die Temu-App herunterladen. Diese Praxis kann als „**Bait-and-Switch**“ bezeichnet werden, bei der

ein attraktives Angebot beworben wird, das in Wirklichkeit nicht existiert. Dies führt zu enttäuschten Erwartungen, da die als kostenlos angepriesenen Produkte nicht wirklich verfügbar bzw. nicht leicht auffindbar sind.

Die Aufforderung zum Kauf eines Produkts zu einem bestimmten Preis und die anschließende Weigerung, dem Verbraucher das beworbene Produkt zu zeigen oder Bestellungen dafür anzunehmen, in der Absicht, stattdessen ein anderes Produkt abzusetzen („**Bait-and-Switch**“-Technik), gilt als irreführende Geschäftspraxis gemäß Anhang I Ziffer 6 der UGP-RL. Obwohl keine direkte Absicht besteht, ein anderes Produkt zu verkaufen, werden die Verbraucher:innen zur Teilnahme an einem Gewinnspiel veranlasst, welches sie zum Kauf anderer Produkte auf der Plattform verleiten soll. Es bleibt daher die Frage offen, ob eine solche Praxis von der dieser Regelung erfasst wird. Wenn das verwendete Dark Pattern nicht in den Anwendungsbereich der UGP-RL fällt, könnte es nach Artikel 25 DSA als unzulässig eingestuft werden.

Nach dem Klick auf eine Werbeanzeige werden Konsument:innen aufgefordert, die Temu-App herunterzuladen, um vermeintliche Rabatte oder kostenlose Produkte zu erhalten. Diese Angebote sind jedoch nach der Installation oft nicht auffindbar. Diese Strategie fällt unter „**Forced Action**“, da Konsument:innen gezwungen werden, eine unerwünschte Handlung (Herunterladen der App) durchzuführen, um das beworbene Angebot wahrnehmen zu können. Zudem handelt es sich bei der Werbung für kostenlose Produkte um ein „**Disguised Ad**“, also eine versteckte Werbung für den Download der Temu-App. Temu setzt zudem zahlreiche Countdown-Timer und Knappheitsanzeigen ein, um den Eindruck von **Dringlichkeit** und begrenzter Verfügbarkeit zu erzeugen (**Fake Urgency, Fake Scarcity**). Diese Elemente sind auf verschiedenen Seiten der Website präsent und suggerieren, dass Angebote nur für kurze Zeit verfügbar sind. Diese Dark Patterns nutzen das psychologische Phänomen der Verlustaversion aus, bei dem Konsument:innen aus Angst, ein Angebot zu verpassen, schnell eine Kaufentscheidung treffen. Problematisch ist hierbei, wenn die tatsächliche Verfügbarkeit der Angebote nicht gegeben ist, was ohne Blick hinter die Kulissen kaum zu beurteilen ist.

Die unrichtige Behauptung, dass das Produkt nur für eine sehr begrenzte Zeit oder nur für eine sehr begrenzte Zeit zu bestimmten Bedingungen verfügbar sein wird, um Verbraucher:innen zu einer sofortigen Entscheidung zu verleiten, so dass sie weder die Zeit noch die Möglichkeit haben, eine informierte Entscheidung zu treffen, gilt als irreführende Geschäftspraktik gemäß Anhang I Ziffer 7 der UGP-RL. Die Verwendung von Gestaltungsmerkmalen, wie z. B. eines falschen Countdowns oder falscher Angaben über die begrenzte Verfügbarkeit des Produkts, könnte also eine irreführende Geschäftspraktik im Sinne von Anhang I Ziffer 7 UGP-RL darstellen. Auch hier könnte das verwendete Dark Pattern, wenn es nicht in den Anwendungsbereich der UGP-RL fällt, nach Artikel 25 DSA unzulässig sein.

Auch wird mit versteckten Kosten und verwirrenden Preisangaben gearbeitet: In den Werbeanzeigen werden Produkte beworben, die nach der Installation der App nicht mehr auffindbar sind. So werden Konsument:innen auch nach dem Klick auf „kostenlose“ Angebote dazu animiert, die vielen kostengünstigen Angebote auf Temu wahrzunehmen und einzukaufen. Das Versprechen von kostenlosen Produkten wird allerdings nicht erfüllt. Diese Art der Werbung kann als „**Hidden Costs**“ und „**Sneak**

into Basket“ klassifiziert werden, bei denen zusätzliche Kosten oder Bedingungen erst im Verlauf des Kaufprozesses offengelegt werden. Nach Anhang I Z 20 UGP-RL gilt eine Geschäftspraxis als irreführend, wenn ein Produkt als „gratis“, „umsonst“, „kostenfrei“ oder in ähnlicher Weise beschrieben wird, obwohl der Verbraucher weitere Kosten als die Kosten zu tragen hat, die im Rahmen des Eingehens auf die Geschäftspraxis und für die Abholung oder Lieferung der Ware unvermeidbar sind.

Nach dem Download der Temu-App werden Konsument:innen mit zahlreichen Pop-Ups konfrontiert, die sie auffordern, ihre persönlichen Daten preiszugeben und sich für den Newsletter anzumelden, um weitere exklusive Angebote zu erhalten (**Obstruction, Visual Interference, Nagging, Forced Action**). So werden Konsument:innen wiederholt zu Handlungen gedrängt, die sie möglicherweise nicht beabsichtigt haben. Für diese Geschäftspraxis stellt sich die Frage, welche Verordnung anzuwenden ist. Die Einwilligung, Newsletter zu erhalten, um exklusive Angebote zu erhalten, könnte die Frage aufwerfen, ob dies unter das Kopplungsverbot der DSGVO fällt. Bei dieser Frage geht es jedoch in erster Linie um die Rechtmäßigkeit der Verarbeitung in Bezug auf einzelne natürliche Personen. Fraglich ist daher, ob auch die bloße Umsetzung dieses Gestaltungsmusters im Sinne der DSGVO für unzulässig erklärt werden kann. Sollte die DSGVO insoweit nicht anwendbar sein, kann dieses Dark Pattern nach Art. 25 DSA unzulässig sein.

In unterschiedlichen Werbungen (Abb.10-12.) setzt Temu auch auf Elemente, die aus dem Online-Glücksspiel bekannt sind. Hier wird auf Mechanismen der **Gamification** gesetzt, um User in der Interaktion mit dem Werbeelement zu halten. Die Tendenz, Casino- oder glückspielartige Elemente einzusetzen werden auch in anderen Bereichen der digitalen Welt zunehmend sichtbar, wie beispielsweise bei Online-Gaming, das primär Kinder und Jugendliche zur Zielgruppe hat. Elemente wie diese erhaschen die Aufmerksamkeit von insbesondere vulnerablen Zielgruppen und haben auf diese auch eine verstärkte Wirkung. Wenn diese Angebote dann mit „**Bait-and-Switch**“ bzw. „**Lockvogeltaktiken**“ kombiniert werden, werden potenziell vulnerable Zielgruppen dazu gebracht, Apps zu downloaden und Geld auszugeben, das sonst nicht ausgegeben worden wäre.

Fraglich ist, ob die Verwendung von Glücksspielelementen als aggressive Geschäftspraxis eingestuft werden kann. Eine Geschäftspraxis gilt als aggressiv, wenn sie im konkreten Fall unter Berücksichtigung aller tatsächlichen Umstände die Entscheidungs- oder Verhaltensfreiheit des Durchschnittsverbrauchers in Bezug auf das Produkt durch Belästigung, Nötigung, einschließlich der Anwendung körperlicher Gewalt, oder durch unzulässige Beeinflussung tatsächlich oder voraussichtlich erheblich beeinträchtigt und dieser dadurch tatsächlich oder voraussichtlich dazu veranlasst wird, eine geschäftliche Entscheidung zu treffen, die er andernfalls nicht getroffen hätte (Art. 8 UGP-RL). Fraglich ist, ob die Verwendung von Glücksspielelementen als aggressive Geschäftspraxis eingestuft werden kann. In diesem Zusammenhang kommt wohl nur die Fallvariante der „**unzulässigen Beeinflussung**“ in Betracht: In diesem Fall könnte das verwendete Dark Pattern, wenn die UGP-RL keine Anwendung findet, nach Art. 25 DSA als unzulässig eingestuft werden.

## 3.2 Case Study „SHEIN“

SHEIN fällt durch den extensiven und additiven Einsatz von Dark Patterns auf. Diese verändern sich laufend – der Konzern passt seine online Angebote nicht nur an Saisonen, sondern auch an neue Bestimmungen an. Im Laufe der Dokumentation haben sich einige Darstellungen grundlegend verändert, diese Veränderungen werden in Folge aufgeführt und diskutiert. Auf SHEIN sind weiterhin zahlreiche Dark Patterns zu finden, insbesondere betrifft dies den exzessiven Einsatz von Pop-Ups, Rabattaktionen und Gamification-Elementen, die besonders das Treue- bzw. VIP-Programm von SHEIN betreffen.

### 3.2.1 Dokumentation

**Dokumentationsgrundlage:** Screenshots der Website <https://de.SHEIN.com/> von 18. und 11.06.2024 und Oktober, bzw. November 2022 sowie 2023. Bitte zu beachten, dass die Website sowie die App regelmäßig verändert werden und die Heranziehung der Beispiele insofern nur mit Hinweis auf Datum erfolgen sollte.

Bei Abruf der deutschsprachigen Website von SHEIN ([de.SHEIN.com](https://de.SHEIN.com/)), erscheint zunächst ein Pop-Up, das auf Rabattaktionen aufmerksam macht, ebenso bei Registrierung bzw. Download der App.

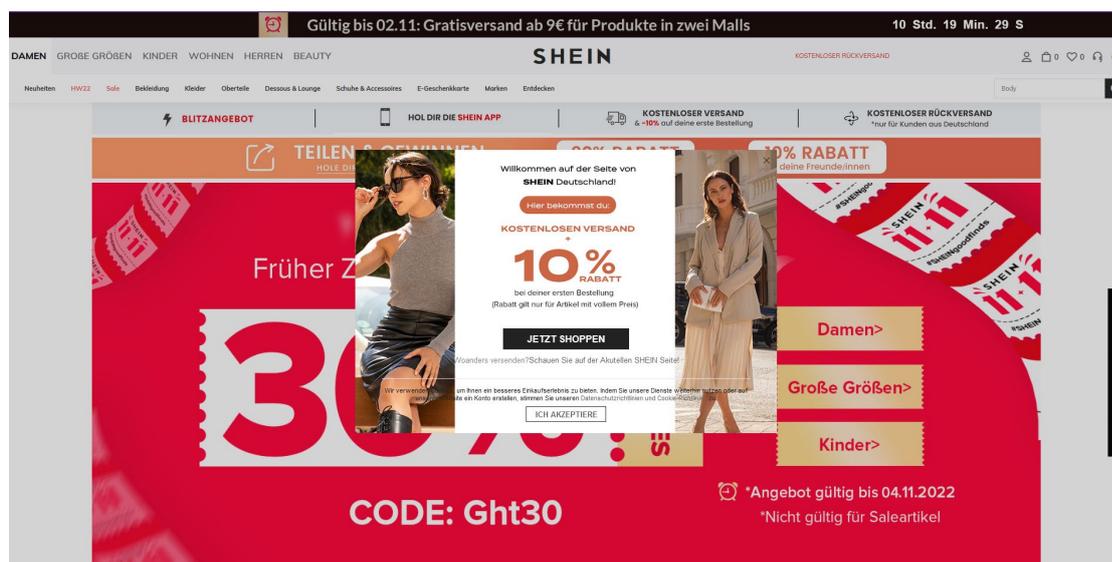


Abbildung 18: Website von SHEIN.com (Screenshot, 18.10.2022).

Der Vergleich von einem Screenshot der SHEIN.com/de Website im Oktober 2022 und im Juni 2024 zeigt: Beide Seiten sind überladen mit Informationen, Bildern und diversen Pop-Ups. Während im Oktober 2022 noch die Registrierung auf der Seite beworben wurde, ist es im Juni 2024 der Download der SHEIN-App, der mit diversen Vergünstigungen wie z. B. gratis Versand und gratis Rückversand beworben wird.

In beiden Fällen (Abb. 18 und Abb. 19) ist es nicht einfach ersichtlich, wie das Pop-Up Fenster entfernt werden kann. Es gibt nur einen Button mit der Aufschrift „JETZT EINKAUFEN“ darunter ein kleines Kästchen mit „ICH AKZEPTIERE“, das sich auch die verwendeten Cookies bezieht – es fehlt eine gleichermaßen ersichtliche Opt-Out-Option für Konsument:innen.

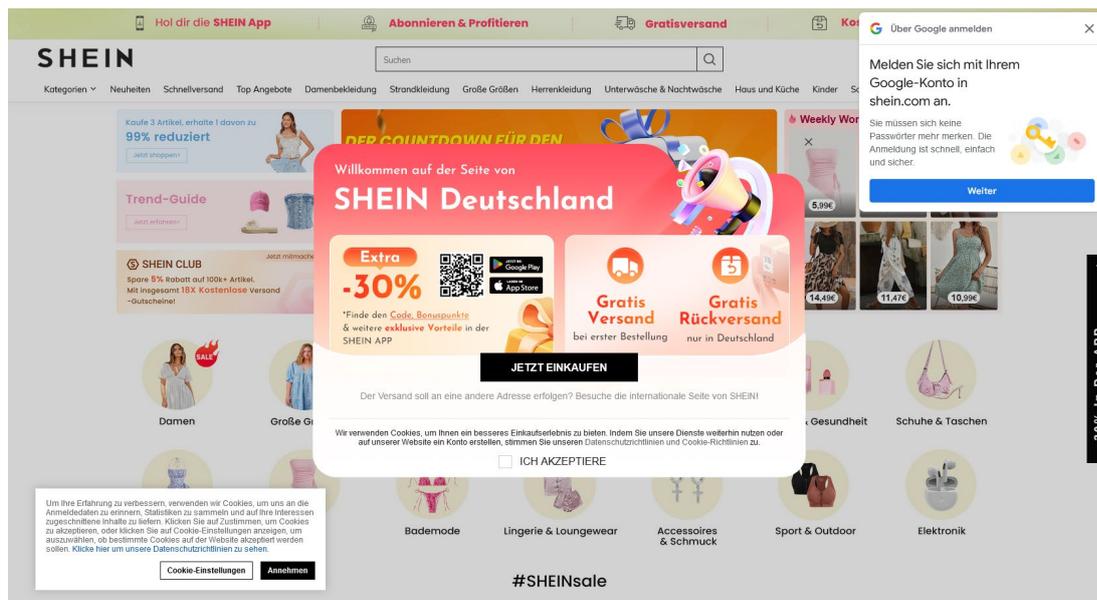


Abbildung 19: Website SHEIN.com mit Pop-Up zu App (Screenshot, 11.06.2024).

Nach dem Klick auf „JETZT EINKAUFEN“ folgt ein weiteres Pop-Up Fenster, mit dem Titel „Sonderangebote nur für dich“. In diesem wird mit einem 30-prozentigen Rabatt geworben, dieser ist mit einem Countdown von 15 Stunden verfügbar. Außerdem wird angeführt wieviel Rabatt neue Nutzer:innen erhalten, sollten sie über 19 Euro (20 % Rabatt), über 59 Euro (25 % Rabatt) oder über 119 Euro (30 % Rabatt) einkaufen – auch diese Aktion ist mit einer Zeitbegrenzung versehen, „Läuft in 1 Tag(en) ab“. Am unteren Rand des Pop-Up gibt es nur einen schwarzen Button, mit der Aufschrift „Sammeln Alle“ – eine animierte, weiße Hand zeigt auf diesen Button, um die gewünschte Aktion des Klicks zu unterstreichen. Man könnte dieses Pop-Up wegklicken, über ein kleines X-Symbol rechts über dem Pop-Up, dieses ist visuell sehr unauffällig und fällt daher kaum auf.

Bei Klick auf den Button „Sammeln Alle“, erscheint ein weiteres Pop-Up zur Registrierung beim SHEIN CLUB. Es gibt die Möglichkeit sich mit der E-Mail-Adresse bzw. via Google-Account oder Facebook-Account zu registrieren bzw. anzumelden. Die zuvor angezeigten Rabatte und Coupons können nur bei einer Anmeldung bzw. Registrierung in Anspruch genommen werden.

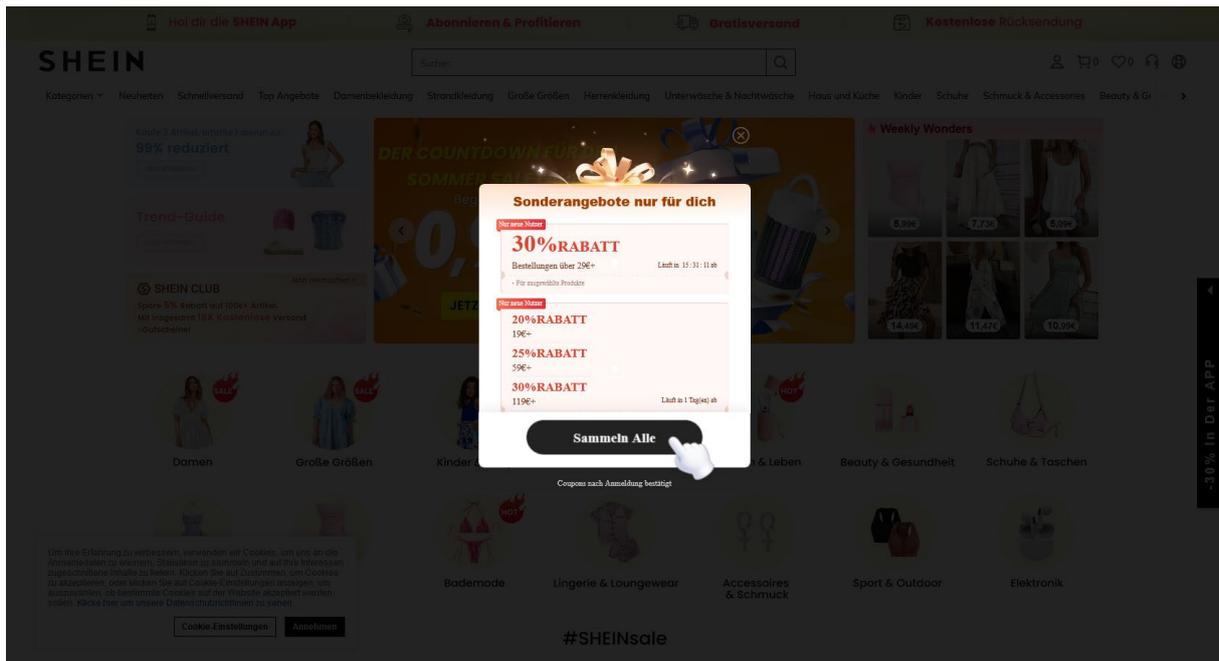


Abbildung 20: Pop-Up „Sonderangebote nur für dich“ (Screenshot, 11.06.2024).

Bei Dokumentation zu Shein im Jahr 2022 ist der Empfang des Newsletters bei der Registrierung bei SHEIN vorausgewählt, 2024 ist das nicht mehr der Fall (siehe Abb.18 vs. Abb. 19). Die Registrierung erfolgte 2022 noch in einem Schritt, 2024 wurde die Registrierung in zwei Schritte (Pop-Up) aufgeteilt.

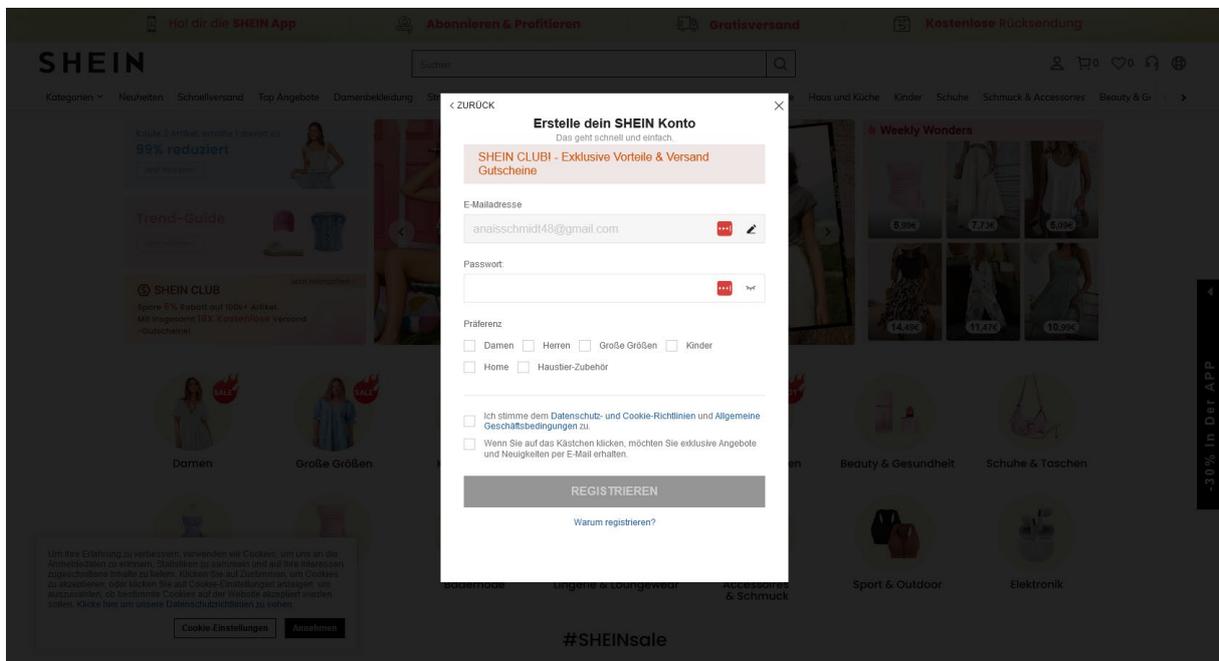


Abbildung 21: Pop-Up zur Registrierung bei SHEIN (Screenshot, 11.06.2024).

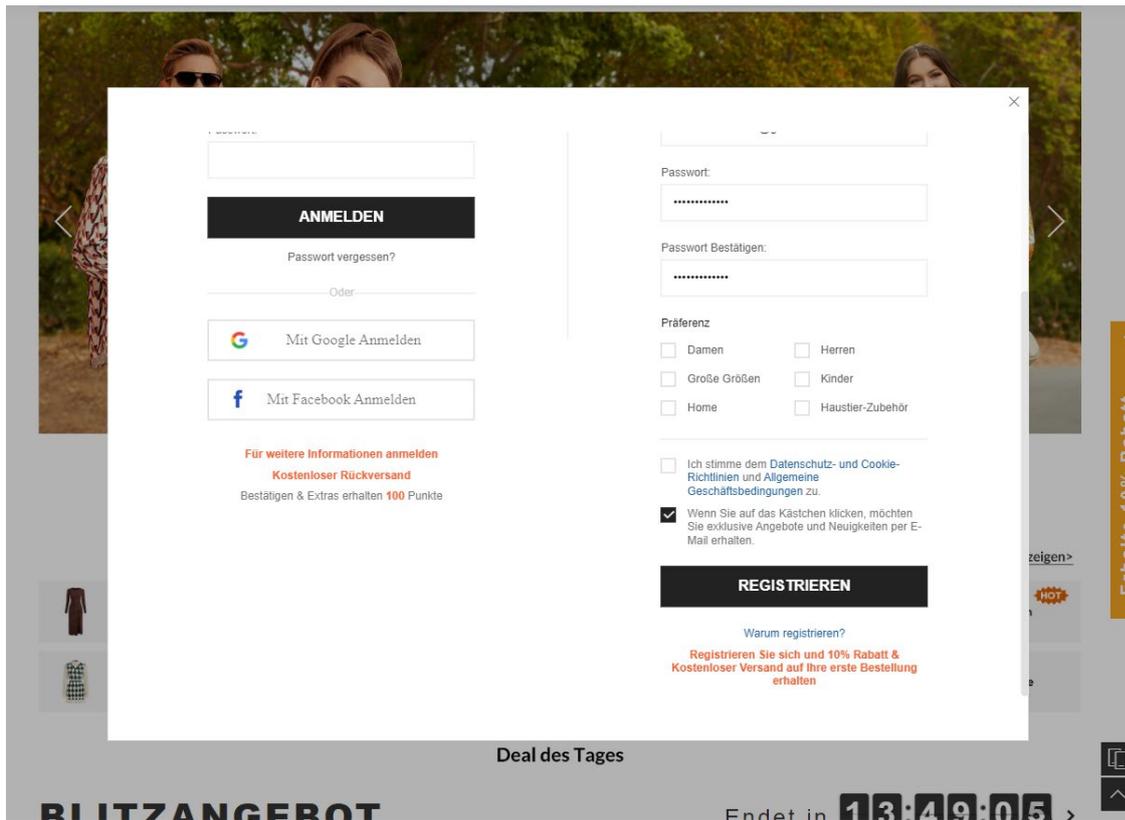


Abbildung 22: Pop-Up zur Registrierung bei SHEIN (Screenshot, 18.10.2022).

Es wird mit Rabatten und Vorteilen für die Registrierung bei SHEIN geworben. Auf der SHEIN-Website wird auch mit zahlreichen Pop-Ups für Vergünstigungen und Sonderangebote geworben. Die visuelle Gestaltung der Seite passt sich an Jahreszeiten, Saisonen, kulturelle Ereignisse, aber auch unabhängig davon immer weiter in ihrer Grafik an. Zu jedem Zeitpunkt ist #SHEINsale, also bestimmte Produkte sind immer vergünstigt.

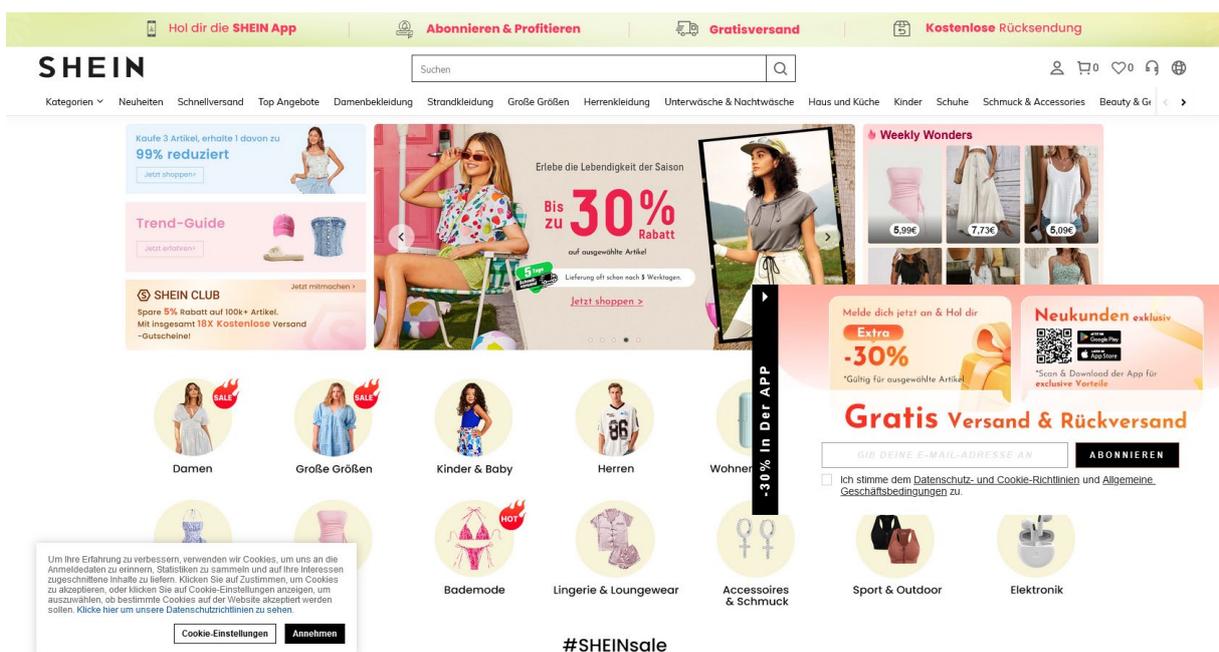


Abbildung 23: Startseite von de.SHEIN.com (Screenshot, 11.06.2024).

Mitte Juni 2024 warb SHEIN mit „Erlebe die Lebendigkeit der Saison. Bis zu 30 % Rabatt“. Diverse Produkte waren mit einem flammenden „SALE“-Icon versehen. Unter dem Begriff „Weekly Wonders“ werden manche Produkte besonders vergünstigt angeboten. SHEIN setzt auch zahlreiche Countdowns ein, z.B. bei den sogenannten Blitzangeboten.

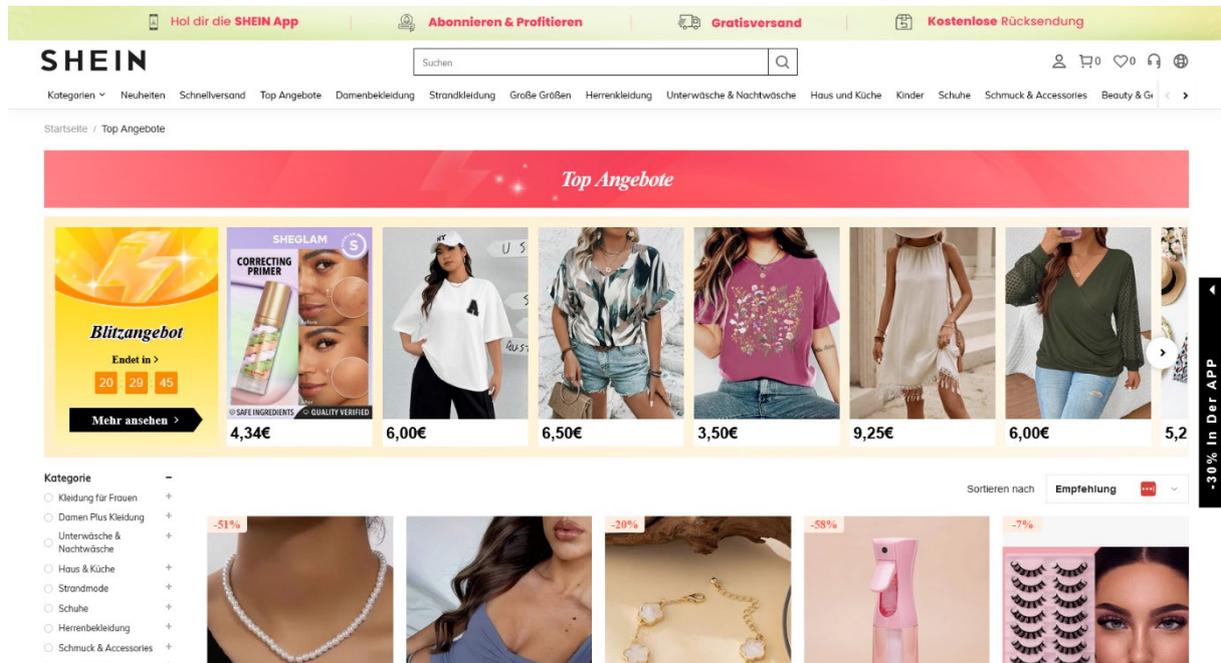


Abbildung 24: Übersicht der Blitzangebote SHEIN (Screenshot, 11.06.2024).

Die Blitzangebote werden intensiver beworben, sie sind mit einem Zeitlimit versehen. Bei Klick auf „Mehr ansehen“, werden Elemente hinzugefügt, um die Dringlichkeit des Angebots zu unterstreichen: Der Countdown wird weiter angezeigt, zusätzlich wird der Rabatt für jedes Produkt angezeigt (gelbes Icon mit Blitz und Prozentanzahl des Rabatts) und wieviel von dem jeweiligen Produkt schon verkauft wurde.

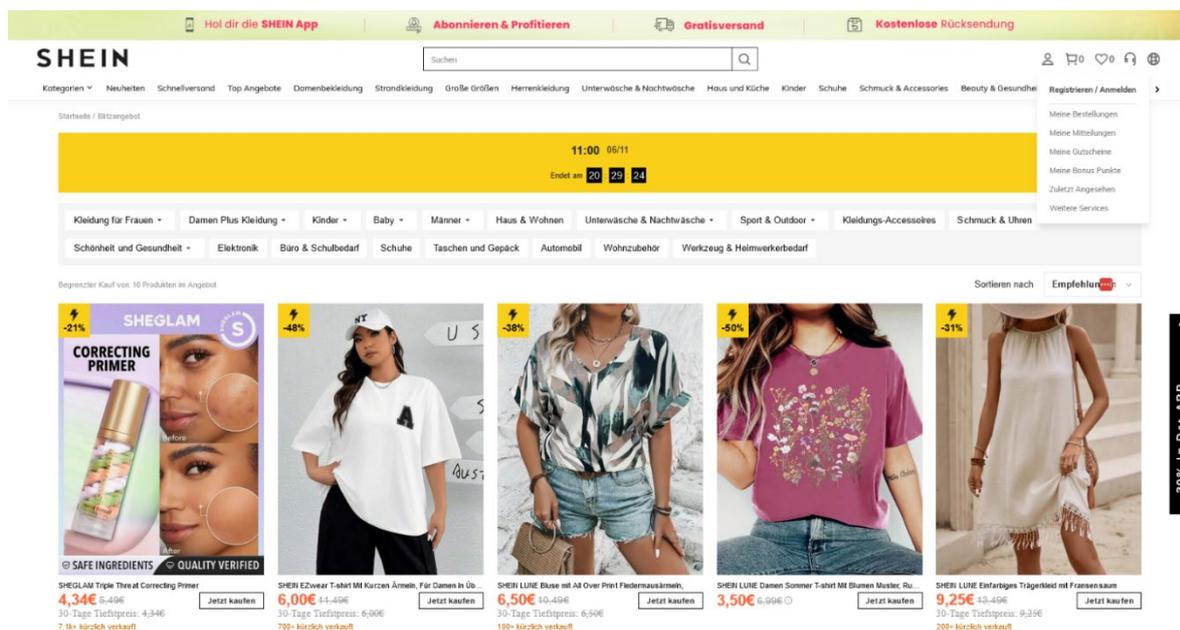


Abbildung 25: Blitzangebote von SHEIN (Screenshot, 11.06.2024).

SHEIN wirbt auch mit speziellen Vorteilen für die SHEIN-Club Mitglieder: Hier gibt es Untergruppen. Die SHEIN-Community wird unterteilt in den SHEIN Club, SHEIN Saver, und SHEIN VIP. Bei diesen Clubs handelt es sich mit Ausnahme von SHEIN VIP um Abo-Modelle, bei denen Rabatte und Vorteile an Mitgliedsbeiträge geknüpft sind.

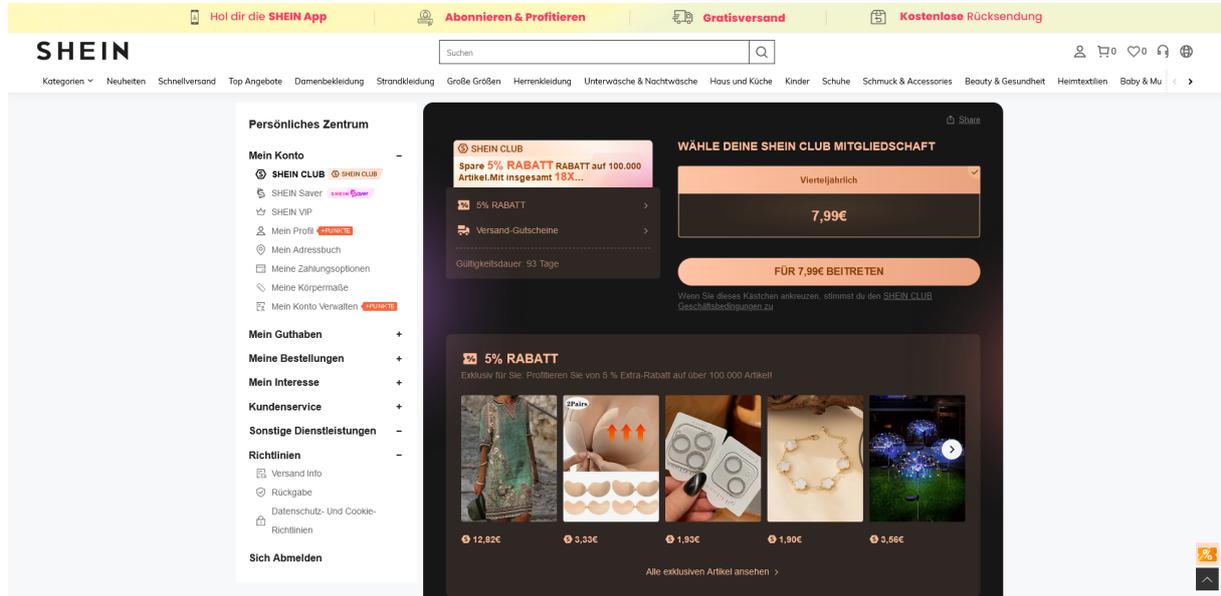


Abbildung 26: Seite des SHEIN CLUB (Screenshot, 18.06.2024).

Die Mitgliedschaft im SHEIN CLUB kostet 7,99 Euro vierteljährlich, also 31,96 Euro jährlich. Dem SHEIN Saver Club kann man für 7,90 Euro beitreten. Lediglich der SHEIN VIP Club ist kostenfrei, hierbei handelt es sich um ein Belohnungssystem, je mehr bei SHEIN eingekauft wird, desto mehr Vergünstigungen bekommen die SHEIN VIP Mitglieder.

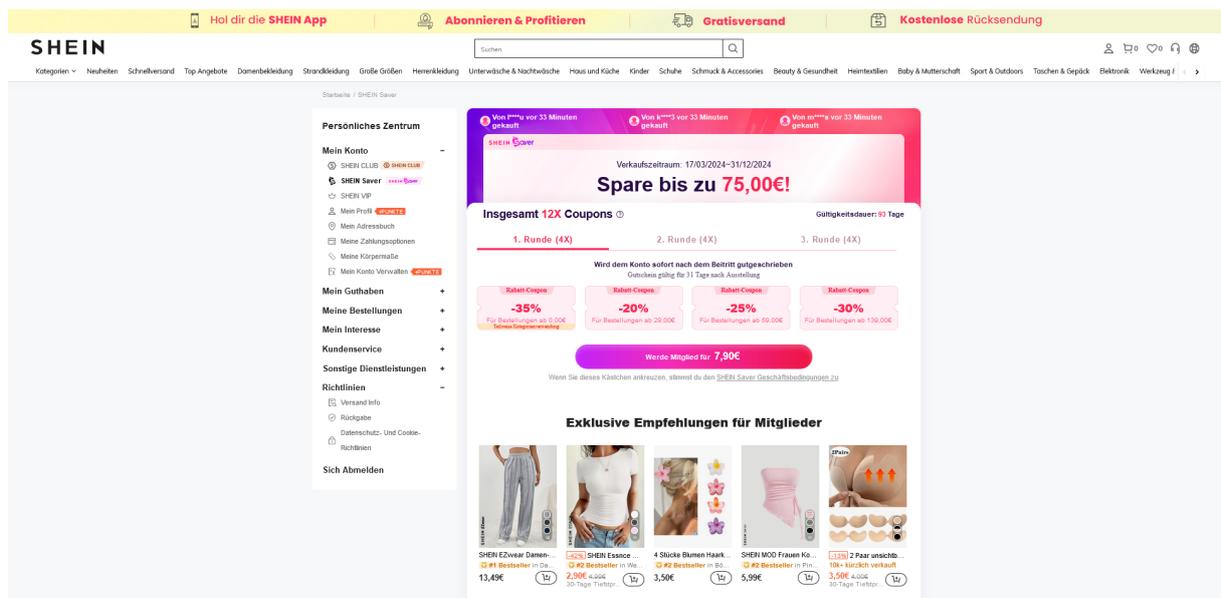


Abbildung 27: Seite des SHEIN Saver Clubs (Screenshot, 18.06.2024).

### 3.2.2 Analyse

Die Website von SHEIN eignet sich als Beispiel für den Einsatz von Dark Patterns, gleichzeitig aber auch für manche Schwierigkeiten bei der definitorischen Abgrenzung. Dokumentiert wurden zahlreiche bzw. schwer zu entfernende Pop-Up-Fenster, viele Countdown-Timer und Zeitbegrenzungen, die Konsument:innen zu raschen Entscheidungen drängen sollen, Social-Proof-Anzeigen, erschwerte Opt-Out-Möglichkeiten sowie Abo-Modelle, die teils mithilfe von Gamification beworben werden.

Bei jedem Aufruf der Website macht ein Pop-Up-Fenster auf Rabattaktionen aufmerksam, die an die Registrierung oder den Download der App gekoppelt sind. Es gibt nur einen klar erkennbaren Button mit der Aufschrift "JETZT EINKAUFEN", während die Option, das Pop-Up zu schließen, kaum sichtbar ist. Diese Strategie nutzt das als „**Forced Action**“ bezeichnete Dark Pattern: User werden dazu gedrängt, eine Aktion durchzuführen (in diesem Fall, auf den Button zu klicken), ohne eine leicht erkennbare Option die Aktion abzulehnen (**Forced Action, Deliberate Misdirection**). Bestimmte Wahlmöglichkeiten schwieriger oder zeitaufwändiger zu gestalten als andere, stellt ein Dark Pattern im Sinne von Erwägungsgrund 67 DSA dar. Aus diesem Grund könnte die Verwendung dieses Dark Pattern nach Artikel 25 DSA unzulässig sein.

Die zahlreichen Rabattaktionen und Sonderangebote auf SHEIN sind oft mit Countdown-Timer versehen, die eine zeitliche **Dringlichkeit** suggerieren (**Fake Urgency**). Beispielsweise wird ein 30-prozentiger Rabatt nur für 15 Stunden angeboten. Die suggerierte Dringlichkeit ist ein Grundprinzip von SHEIN – beispielhaft zum Pop-Up mit Rabattangeboten bei erstem Aufruf der Seite wurde von uns festgestellt, dass jeweils Countdowns bis Mitternacht getimed waren – allerdings nicht mit der Angabe Tagesrabatt, sondern eine Stundenangabe (15 Stunden, 17 Stunden, 6 Stunden). Keine Unterschiede wurden bei Countdowns gefunden, wenn Cookies gelöscht wurden oder andere User die Website aufrufen (**Visual Interference, Urgency**).

Anders gesagt: Sobald ein Countdown abgelaufen ist, wird ein neuer Countdown gestartet, Konsument:innen befinden sich somit unter ständigem Abverkaufs-Stress, sobald sie auf der SHEIN-Website einkaufen. Diese Form des Einsatzes von Countdown-Timern nutzt die psychologische Tendenz der Verlustaversion aus – Konsument:innen ist die tatsächliche Verfügbarkeit dieser Angebote nicht klar, bzw. wissen diese unter Umständen nicht, dass jeden Tag die gleiche Dringlichkeit über scheinbar limitierte Angebote suggeriert wird. Die Verwendung eines falschen Countdowns könnte eine irreführende Geschäftspraxis im Sinne von Anhang I Ziffer 7 UGP-RL darstellen. Dieses Dark Pattern kann auch nach Art. 25 DSA unzulässig sein, wenn die UGP-RL insoweit nicht anwendbar ist.

Ähnlich verhält es sich bei den Social Proof Anzeigen. SHEIN gibt an, wieviel von einem Produkt bereits verkauft wurde – statt wie 2022 hier mit Prozentangaben zu arbeiten, werden 2024 absolute Produktverkaufszahlen angeführt. Um Angebote besonders hervorzuheben, wird angezeigt, wie viele Produkte bereits verkauft wurden (**Fake Social Proof, Fake Scarcity**). Diese Zahl ist jedoch ohne jeglichen Kontext nicht von den Konsument:innen einzuordnen. Auch in der Annahme, dass diese Zahlen

stimmen, bleibt unklar auf welchen Zeitraum und welche Lagerbestände sich diese beziehen (Österreich, deutschsprachiger Raum, Europa, weltweit?).

Die Verwendung visueller Anreize wie flammende „SALE“-Icons und Blitzangebot-Icons, unterstreicht, dass Produkte äußerst beliebt und knapp verfügbar sind – auch hier ist unklar, ob dies der Fall ist oder bloß als Dark Pattern eingesetzt wird, um einen schnellen Kaufabschluss zu erwirken.

Die Pop-Up-Fenster, die beim Aufrufen der Seite angezeigt werden, bieten keine leicht erkennbare Opt-Out-Option für Konsument:innen, und das Schließen der Fenster wird absichtlich erschwert (**Forced Action, Deliberate Misdirection, Nagging, Obstruction**). Dies kann zu einer unfreiwilligen Zustimmung der Nutzer:innen führen und verstößt möglicherweise gegen die DSGVO, die klare und leicht zugängliche Opt-Out-Optionen vorschreibt. Ein solcher Mangel an Transparenz und Wahlfreiheit könnte rechtlich problematisch sein.

Die Belohnungsprogramme der SHEIN-Community nutzen **Gamification-Elemente**, um Nutzer:innen zu binden. Verschiedene Club-Modelle bieten Vergünstigungen gegen Mitgliedsbeiträge an, während der SHEIN VIP Club ein Belohnungssystem basierend auf dem Einkaufsvolumen darstellt. Gamification kann die Nutzer:innen zu wiederholten Käufen motivieren, um Belohnungen zu erhalten. Die damit verbundenen Abo-Modelle (SHEIN CLUB) könnten als verschleierte Kostenfallen wirken, insbesondere wenn die Informationen über die Kosten und Bedingungen der Mitgliedschaft nicht klar und transparent dargestellt werden (**Hidden Costs, Hidden Subscription**).

## 4 Flugbuchungen & Dark Patterns

Wer eine Reise nicht selbst zusammenstellen will, kann auf das Angebot von Buchungsportalen zurückgreifen – vom Flug, über die Unterkunft, den Mietwagen, die Reiseversicherung bis hin zu Aktivitäten kann auch alles in einem Zug gebucht werden. Nicht nur Buchungsportale, sondern auch viele Fluggesellschaften selbst verkaufen längst nicht mehr nur Flugtickets, sondern bieten Kombi-Angebote an, für die sie auf unterschiedliche weitere Anbieter zurückgreifen. Mit diesen digitalen Veränderungen einher geht eine verschärfte Wettbewerbssituation zwischen Anbietern – u. a. geprägt vom Aufkommen der Billigfluglinien, von Buchungsportalen hin zu Vergleichsplattformen zur Preisbeobachtung.

Als Antwort auf diese veränderten Marktbedingungen können die zahlreichen Regulierungsbemühen der Europäischen Union verstanden werden, in deren Rahmen zum Beispiel zahlreiche Informationspflichten zum besseren Schutz von Konsumentinnen und Konsumenten beschlossen wurden. (z.B. Pauschalreise-regulierung) Auch einige wettbewerbsrechtliche Entscheidungen (siehe Fälle Booking.com) haben das Feld (inkl. Preis- und Angebotsgestaltung) positiv geprägt. Hinzu kommt nun über den DSA die Möglichkeit Dark Patterns in diesem Feld zu melden.

Die Auswertung von Beschwerden im Bereich Reisebuchungen bei der Internet Ombudsstelle, zeigt, dass diese nicht unter dem Begriff „Dark Patterns“ einlangen. Die Probleme, die Konsumentinnen und Konsumenten mit digital gebuchten Reisen (oder Reisebestandteilen) haben, sind unter anderem unerwartete Kosten, enttäuschte Erwartungen an gebuchte Leistungen, Probleme mit Flugverschiebungen oder Stornierungen. Teilweise handelt es sich jedoch, wie im Folgenden näher erläutert wird, um Folgen von Praktiken, die als Dark Patterns klassifiziert werden können.

Die dabei dokumentierten Dark Patterns reichen von der visuellen Hervorhebung einer Option im Sinne einer Vorauswahl „Visual interference“, über ein Ausnutzen von kognitiven Schwächen bei Budgeting („Exploiting vulnerabilities in Budgeting“ und „Comparison Prevention“), hin zu dem Drängen von Konsument:innen zu einer bestimmten Auswahl über wiederholtes Nachfragen („Nagging“), der visuellen Verhinderung der Fortführung des Buchungsprozesses über Pop-Ups und andere störende Elemente („Obstruction“), der nicht-Vergleichbarkeit, und erzwungener Fortsetzung von nicht intendierten Prozessen („Forced Action“).

Bei der Reservierung von Sitzplätzen wird vor allem bei Billigfluggesellschaften versucht, Aufpreise zu verrechnen. In der Analyse wurden zahlreiche Dark Patterns dokumentiert, die darauf abzielen die Kundenentscheidung dahin zu lenken – dazu zählen das wiederholte Nachfragen im Rahmen des Buchungsprozesses, ob die Entscheidung nicht geändert werden wolle („Nagging“), die Vorauswahl einer Entscheidung („Preselection“), die emotional-suggestive Formulierung von Texten („Confirmshaming“), das absichtliche Behindern des Prozesses („Obstruction“), missverständliche Formulierungen oder Fangfragen („Trickwording“), die Verhinderung von Vergleichen („Comparison Prevention“) und das Verhindern der Änderung der eigenen Meinung oder der schon getroffenen Entscheidung („Hard to Cancel“).

In allen untersuchten Fällen gibt es die Möglichkeit für eine Reservierung eines Sitzplatzes nach Wahl zusätzlich zu zahlen – allerdings zeigen sich große Unterschiede in den Formulierungen und der Darlegung des Angebots. Grundsätzlich kann angenommen werden, dass Konsument:innen davon ausgehen, dass die Buchung eines Fluges einen Sitzplatz umfasst – gegenläufig zu z. B. der Buchung eines Zugtickets. Diese Sicherheit wird jedoch durch Arten der Formulierung („Trickwording“ & „Confirmshaming“) in unterschiedlichem Ausmaß in Frage gestellt. Verwendete Formulierungen für das Zusatzservice einer kostenpflichtigen Auswahl des Sitzplatzes: „Reservierter Sitzplatz“ (Ryan Air), „Sitzplatzreservierung“ (Austrian Airlines), „Sitzplatzauswahl“ (Wizz), „Wählen Sie Ihre Sitzplätze aus“ (Opodo).

Anzumerken ist, dass die Buchung eines Fluges ohne Zusatzservices einem Hürdenlauf gleicht. Sind Konsument:innen darin geübt und routiniert, fällt dieser Hürdenlauf zur Vermeidung von Zusatzkosten leichter, fraglich ist, wie überfordernd so gestaltete Buchungsprozesse technikfernen oder vulnerablen Verbraucher:innen fallen.

## 4.1 Case Study „Ryan Air“

### 4.1.1 Dokumentation

**Dokumentationsgrundlage:** Screenshots des Buchungsprozesses von 17.04.2024 und Oktober, bzw. September 2023. Bitte zu beachten, dass der Buchungsprozess regelmäßig verändert wird und die Heranziehung der Beispiele insofern nur mit Hinweis auf Datum erfolgen sollte.

Der erste Schritt im Buchungsprozess von Ryanair ist die Auswahl von Hinflug und Rückflug, die jeweils einzeln bepreist sind – es fehlt zu diesem Zeitpunkt die Information, was in diesem Preis inkludiert ist. Im zweiten Schritt werden vier Pakete vorgestellt – der in Schritt eins angezeigte Flugpreis ist aus der Kategorie „Basic“ – die günstigste Variante. Es sind drei weitere Tarife angeführt – „Regular“, „Plus“ und „Flexi Plus“.

**Wien -> Zadar**  
Hin- und Rückflug - 22 Sept. - 24 Sept. - 1 A. [Suche bearbeiten](#)

**Ihre ausgewählten Flüge**

- 22 SEPT. 20:20 Wien -> Zadar (FR 4803) 1 Stunden 5 Minuten - Durchgeführt von Malta Air 21:25 Zadar
- 24 SEPT. 18:00 Zadar -> Wien (FR 4804) 1 Stunden 15 Minuten - Durchgeführt von Laudis Europe 19:15 Wien

**Wählen Sie Ihr Paket**

	BASIC	REGULAR	PLUS	FLEXI PLUS
<b>1 kleines Gepäckstück</b> <small>Muss unter den Sitzplatz vor Ihnen passen</small>	✓	✓	✓	✓
<b>Reservierter Sitzplatz</b> <small>Ausgenommen der Sitzplatz des Piloten!</small>		✓	✓	✓
<b>10 kg Gepäckstück für das Gepäckfach</b> <small>Nehmen Sie es mit an Bord</small>		✓	✓	✓
<b>Gepäckstück bis 20 kg</b> <small>Siehe ab Kleidung und Flüssigkeiten mitnehmen!</small>		✓	✓	✓
<b>Priority Boarding</b> <small>Einmaliger Zugang zu den Gepäckfächern</small>		✓	✓	✓
<b>Kostenlos online einchecken</b> <small>Stornieren Sie sich mehr Zeit am Flughafen</small>	✓	✓	✓	✓
<b>Kostenloses Check-in am Flughafen</b> <small>Bis 60 Minuten vor Abflug</small>	✓	✓	✓	✓
<b>Flüge gebührenfrei ändern</b> <small>Sie bezahlen lediglich den eventuell anfallenden Preisveränderer!</small>	✓	✓	✓	✓
<b>Auf einen früheren Flug umbuchen</b> <small>Flexibilität am Reisetag</small>	✓	✓	✓	✓

**Wählen Sie Ihr Paket**  
Weiter für 78,92 € | +22,25 € je Flug | +31,49 € je Flug | +73,75 € je Flug

**Sie verpassen keine Sonderaktion und können sich jederzeit abmelden.**  
Diese Angebote sollten Sie nicht

Abbildung 28: Ryanair-Tarife (Screenshot, 17.04.2024).

Die Optionen sind in einer Tabellenform dargestellt. Auffällig bei der **visuellen Gestaltung** ist, dass es zwar keine Vorauswahl gibt, aber der zuvor gewählte Flugpreistarif aus Schritt 1 teilweise ausgegraut ist. Von den drei anderen Tarifen ist der Plus-Tarif in Gelb hervorgehoben, die Tarife „Regular“ und „Flexi Plus“ sind in blau gehalten. Im **Wording** auffällig ist die Zeile „Reservierter Sitzplatz“, die für den Basic-Tarif nicht angekreuzt ist.

BASIC	REGULAR	PLUS	FLEXI PLUS
<small>Reisen mit leichtem Gepäck</small>	<small>Sitzplatz und 10 kg Bordgepäck wählen</small>	<small>Perfekt für längere Reisen</small>	<small>Unser flexibelstes Paket</small>
Weiter für 78,92 €	+22,25 € je Flug	+31,49 € je Flug	+73,75 € je Flug

Abbildung 29: Ryan Air: Tarife-Preisdarstellung (Screenshot, 17.04.2024)

Bei der **Preisdarstellung** auffällig ist, dass nur für den günstigsten Tarif die Gesamtsumme angezeigt wird, die weiteren Tarife sind nur hinsichtlich ihres Aufschlags je Flug beziffert. Daraus folgt, dass der günstigste Tarif (Basic) mit der höchsten Zahl beziffert ist (78,92 €). Bei den drei anderen Tarifen wird der Aufpreis je Flug genannt, der zum Basic-Tarif hinzukommt – es ist keine Gesamtsumme zu sehen.

### Wahl des Flugtarifs

Bei Auswahl des Basic-Tarifs, erscheint ein Pop-Up Fenster, mit dem Titel „Der REGULAR Tarif ist ideal für Ihre Reise“. In dem Pop-Up Fenster ist eine Tabelle, in der die Tarife „Basic“ und „Regular“ verglichen werden. Wichtig anzumerken ist: Nur bei

Auswahl des „Basic“-Tarifs gibt es ein solches Pop-Up, die Entscheidung für jede andere Option leitet den User direkt zum nächsten Buchungsschritt weiter.

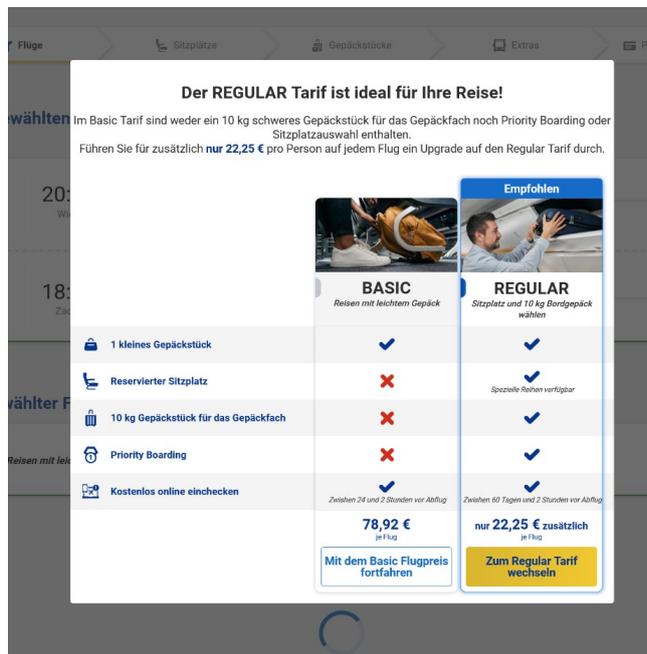


Abbildung 30: Ryanair Pop-Up bei Auswahl des Basic-Tarifs. (Screenshot, 17.04.2024).

**Visuelle Beschreibung** des Pop-Up: Die Tabelle des Pop-Up unterscheidet sich visuell von der Tabelle zum Vergleich aller Tarife. Im Unterschied dazu gibt es neben den Häkchen (diese symbolisieren inkludierte Leistungen) auch rote Kreuze – u.a. bei den Zeilen „Reservierter Sitzplatz“, „10kg Gepäckstück“ und „Priority Boarding“. Der „Regular Tarif“ ist visuell hervorgehoben, als wäre es eine Vorauswahl – das ist nicht der Fall. Der Button zur Auswahl von „Basic“ ist ausgegraut, wohingegen der Button für „Regular“ gelb hinterlegt ist.

**Wordings:** Der „Regular Tarif“ erhält den Titel „Empfohlen“.

**Option:** Sobald ein Tarif gewählt ist (egal welcher) folgt eine Seite, die ein Login oder eine Registrierung verlangt – diese kann auch übergangen werden („später einloggen“) und man kommt zu einer Seite, bei der ein Sitzplatz reserviert werden kann.

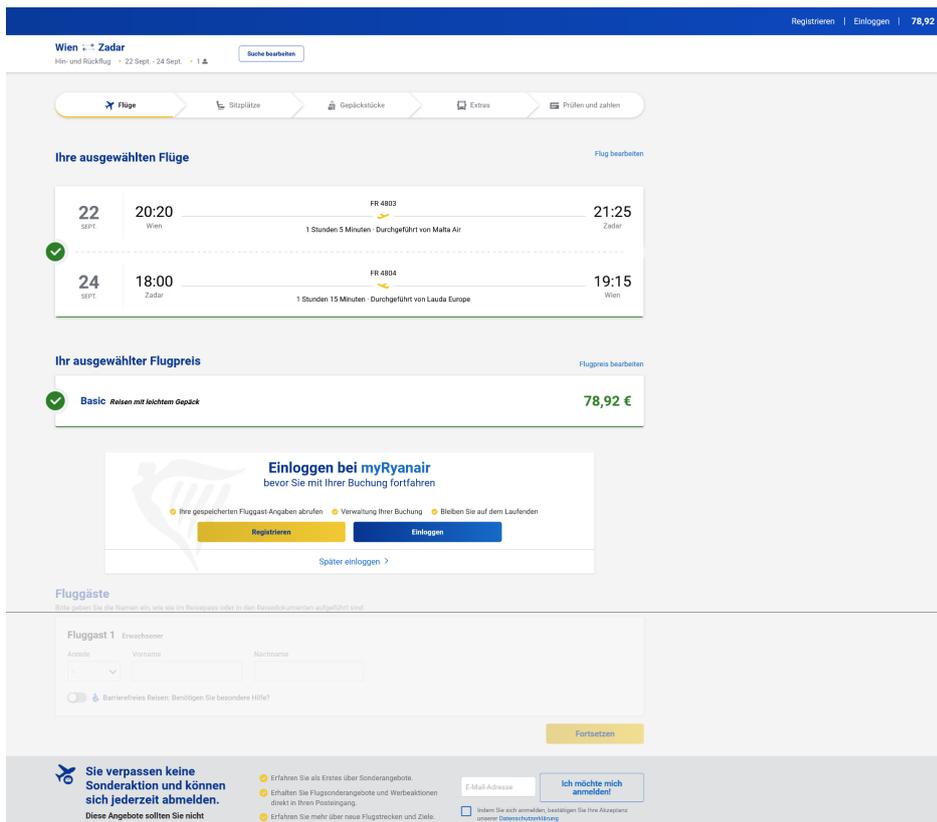


Abbildung 31: Ryanair Gesamtpreis Ansicht. (Screenshot, 17.04.2024).

### Wahl der Sitzplatzreservierung

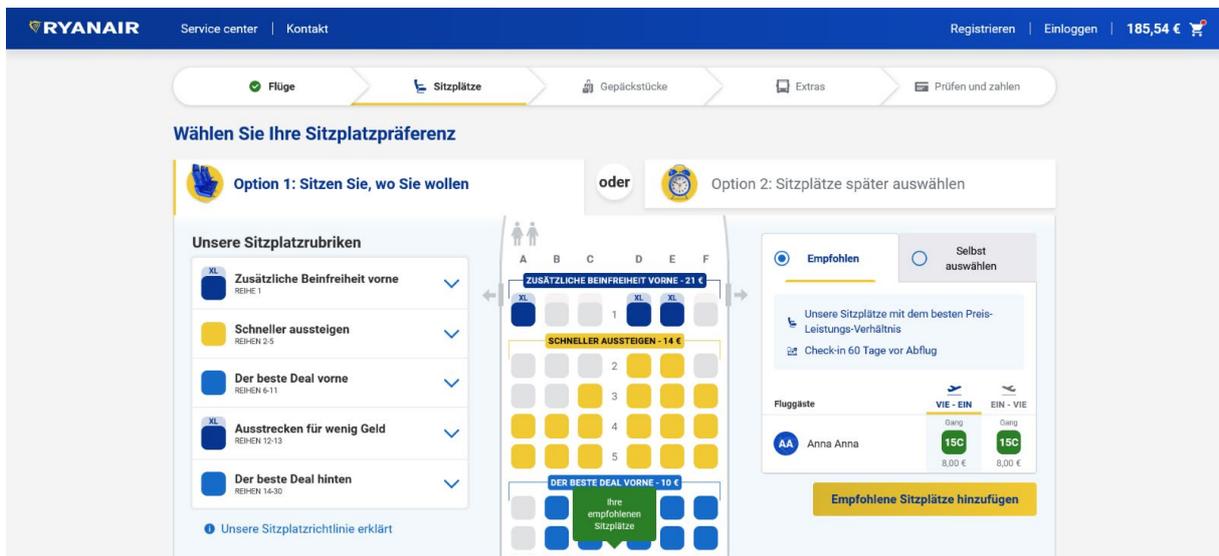


Abbildung 32: Ryanair Sitzplatzauswahl (Screenshot, 17.04.2024).

**Kosten:** Die Sitzplatzreservierungen kosten von 8-21 Euro pro Sitzplatz je Flug. An dieser Stelle des Buchungsprozesses ist der Preis (gesamt) am rechten, oberen Bildschirmrand neben dem Warenkorb zu sehen.

**Vorauswahl:** Bei Auswahl der Tarifs Basic gibt es eine Vorauswahl – die im Test zu unterschiedlichen Sitzplatzkategorien führt. Einmal kommt es zur Vorauswahl

„Empfohlen“ der günstigsten Sitzplatzkategorie („Der beste Deal hinten“, 8 Euro), und einmal der zweitgünstigsten Sitzplatzkategorie („Der beste Deal vorne“, 10 Euro). Die Vorauswahl betrifft beide Flüge und kann mit einem Button „Empfohlene Sitzplätze hinzufügen“, der in Gelb hervorgehoben ist, nochmals bestätigt werden – es gibt vordergründig keinen anderen Button, der eine alternative Option des Fortkommens im Buchungsprozess eröffnet. Um aus der Vorauswahl zu kommen, gibt es zwei ausgegraute Optionen. Oben ist neben dem Titel „Option 1: Sitzen Sie, wo Sie wollen“, die „Option 2: Sitzplätze später auswählen“ ersichtlich. Bei der Vorauswahl „Empfohlen“ ist daneben ein ausgegrauter Button „Selbst auswählen“.

**Was passiert bei Klick auf „Selbst auswählen“:** Es können die Sitzplatzreservierungen pro Flug in den fünf Kategorien selbst ausgewählt werden.

**Was passiert bei Klick auf „Option 2“:** Es erscheint eine Seite mit einem Banner mit dem Titel „Bevor Sie ohne Sitzplatz fortfahren, informieren wir Sie über Folgendes“. Die Information, dass es jedenfalls eine Sitzplatzreservierung geben wird, ist in kleinerer Schrift in der Unterüberschrift angeführt – „[...] wir werden Ihnen nach dem Zufallsprinzip einen Sitzplatz zuweisen“. Drei Informationen werden mit Usern geteilt: (1) Vermeiden Sie einen Platz in der Mitte“, (2) Sitzplatzverfügbarkeit“, (3) Derzeit bester Preis.

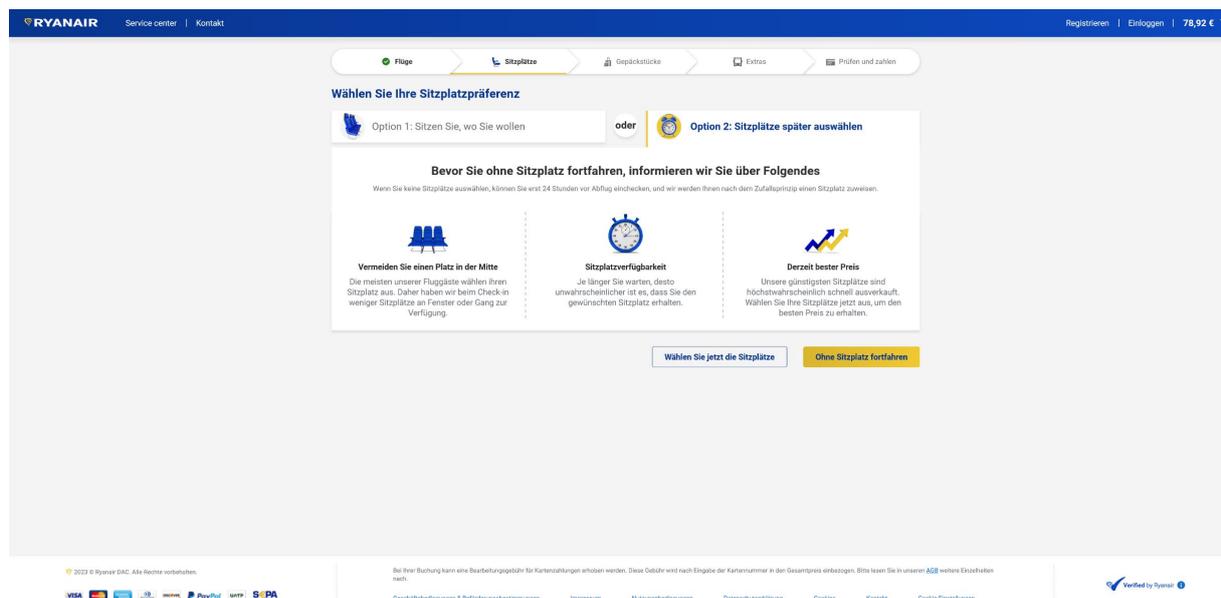


Abbildung 33: Ryanair Sitzplatzauswahl – Option 2 (Screenshot, 17.04.2024).

Die zwei Buttons der Seite unterscheiden sich visuell. In Gelb hervorgehoben ist ein Button „Ohne Sitzplatz fortfahren“, der zweite Button „Wählen Sie jetzt die Sitzplätze“ ist ein Zurück-Button zur Sitzplatzauswahl.

**Was passiert bei Klick auf „Ohne Sitzplatz fortfahren“:** Es erscheint ein Pop-Up Fenster mit dem Titel „Sie haben sich für eine zufällig Sitzplatzzuweisung entschieden“. Die zwei Buttons sind visuell klar unterscheidbar. Gelb hervorgehoben und blau leuchtend ist „Wählen Sie jetzt die Sitzplätze“ suggeriert eine Vorauswahl (fälschlicherweise) und ist in der Funktion ein simpler Zurück-Button zur Sitzplatzauswahl. Alternativ „Mit der zufälligen Zuteilung fortfahren“ ist nicht als

Button gestaltet, sondern als in Fett und blauer Schrift gehaltener Link. Nach Klick auf „Mit der zufälligen Zuteilung fortfahren“ ist der Prozess beendet.

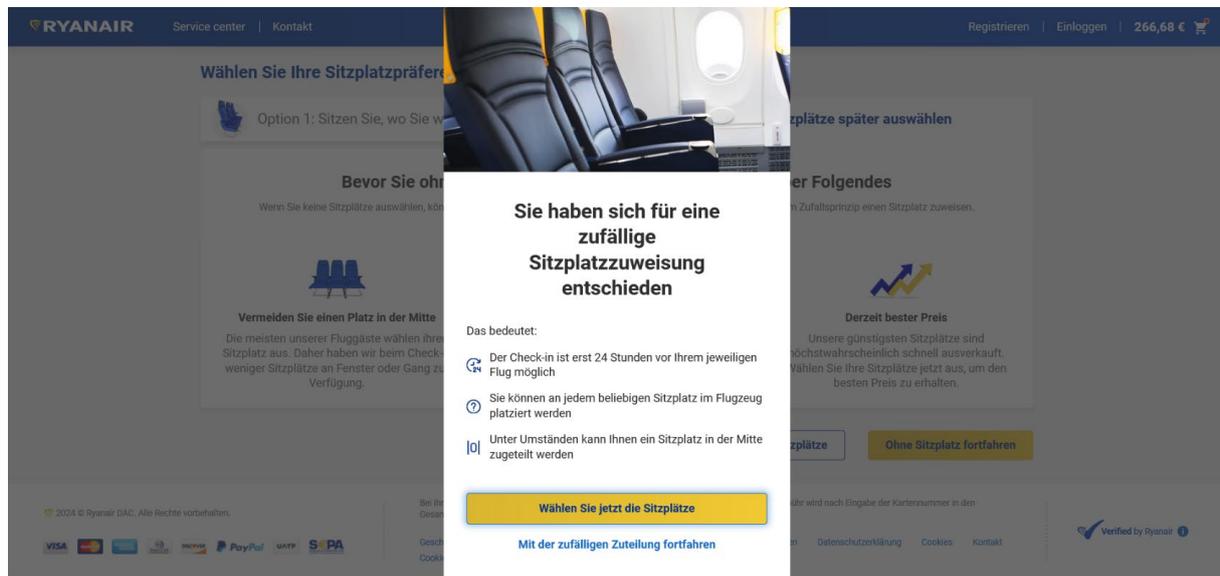


Abbildung 34: Ryanair Sitzplatz Pop-Up (Screenshot, 17.04.2024).

### Fehler bei der Sitzplatzreservierung zum Nachteil von Konsument:innen:

Wählt jemand selbst je Flug einen Sitzplatz aus (Siehe Schritt 1 der Sitzplatzauswahl: „Option 1: Sitzen Sie, wo Sie wollen“ – Button „Selbst auswählen“), entscheidet jedoch ohne Sitzplatzreservierung fortzufahren, so wird die Auswahl nur für den zuletzt gewählten Flug korrigiert. Es erscheint am Ende des Buchungsprozesses die Angabe, dass ein Sitzplatz weiter reserviert ist – eine Möglichkeit aus bereits gewählten Sitzplätzen, zu einer völlig freien und somit kostenlosen Sitzplatzzuteilung zu kommen, ist technisch nicht vorhanden.

### Gepäckauswahl:

**Fall 1:** Im ersten Schritt wurde der „Basic“-Tarif gewählt, der nur ein kleines Handgepäck (Rucksack-Größe) beinhaltet. Nach dem Schritt der optionalen, kostenpflichtigen Sitzplatz-Auswahl, erfolgt trotz der bereits getroffenen Entscheidung ein nochmaliger Check zu Gepäckwünschen. Es ist im Fall der Auswahl des „Basic“ Tarifs keine Gepäckoption vorausgewählt.

**Basic-Tarif weiterverfolgen:** Da nichts vorausgewählt ist, heißt dies: Um die bereits getroffene Entscheidung im Basic-Tarif zu verfolgen, muss nochmals getrennt geklickt werden auf „Nur 1 kleine Tasche“. Bestätigt die Konsument:in die bereits getroffene Entscheidung erscheint ein mit rotem Warnzeichen versehenes Pop-Up, das vor zusätzlichen Kosten bei Missachtung der getroffenen Gepäckwahl warnt. Danach kann mit „Fortsetzen“ der Buchungsprozess weitergeführt werden.

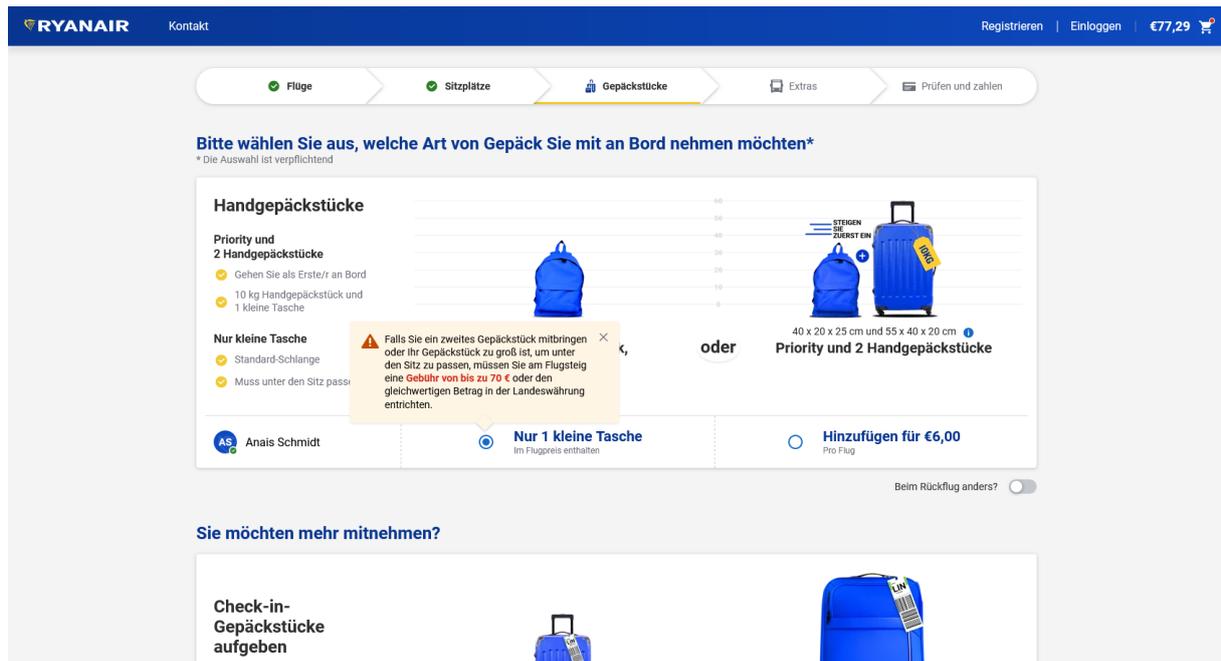


Abbildung 35: Ryanair Gepäcksauswahl (Screenshot, 17.10.2023).

**Fall 2 – Auswahl Regular-Tarif:** Bei Auswahl des Regular-Tarifs sind zwei Handgepäckstücke inkludiert (Rucksack und 10kg). Hier zeigt sich der Unterschied zu Basic insofern bei der Gepäckauswahl nach der Sitzplatzreservierung keine Entscheidung nochmals bestätigt werden muss, sondern nur eine Erweiterung möglich ist. Am Ende der Seite ist ein Button „Fortsetzen“.

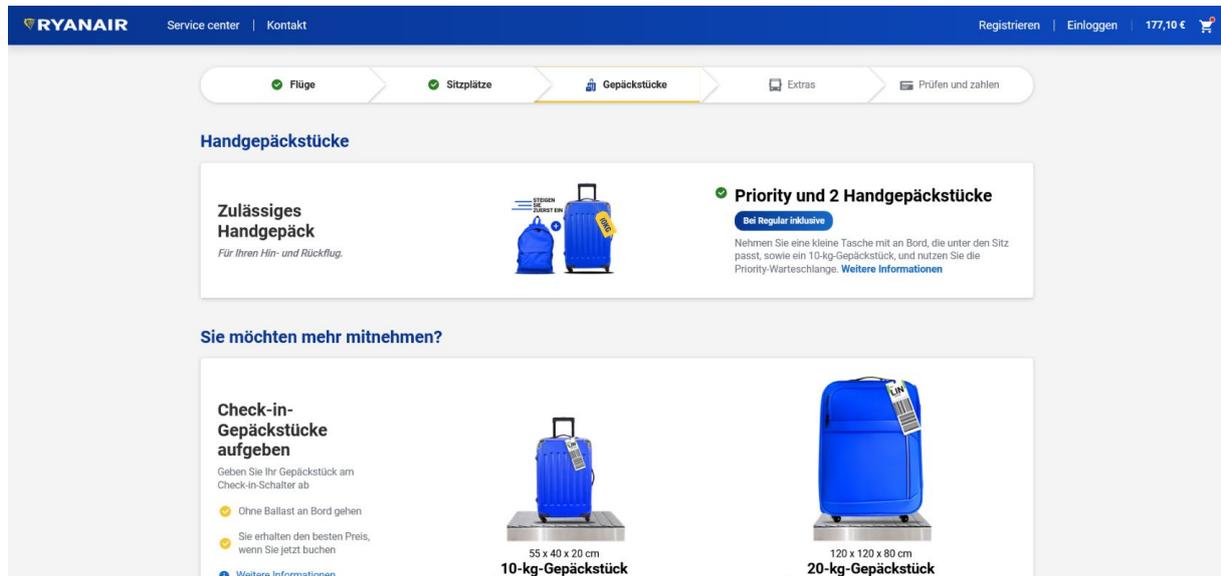


Abbildung 36: Ryanair Gepäck bei Regular Tarif (Screenshot, 17.10.2023).

**Fall 3 – Auswahl Plus-Tarif:** Bei Auswahl des Tarifs Plus ist ein Handgepäckstück (Rucksack) und ein Abgabe-Gepäck (20kg) inkludiert. Beim Schritt Gepäckstück wird der Konsument wieder vor die schon getroffenen Entscheidung gestellt mit der Frage

„Bitte wählen Sie aus, welche Art von Gepäck Sie mit an Bord nehmen möchten?“ Es ist keine Vorauswahl getroffen – in grauer Schrift ist unter „nur 1 kleine Tasche“ vermerkt, dass diese Option im Flugpreis enthalten ist. Eine Vorauswahl getroffen ist bei 20kg Gepäckstück mit dem gelb hinterlegten Hinweis „1 Gepäckstück bei Plus inklusive“.

**Fall 4 – Auswahl Tarif Flexi Plus:** Bei Auswahl des Tarifs „Flexi Plus“ sind zwei Handgepäckstücke inkludiert. Dies muss nicht nochmals bestätigt werden, aber es kann noch ein Gepäck zur Abgabe hinzugefügt werden gegen einen Aufpreis.

Somit gleichen sich Fall 1 (Basic Tarif) und Fall 3 (Plus Tarif) sowie Fall 2 (Regular Tarif) und Fall 4(Flexi Plus Tarif) in der Gestaltung der Gepäcksauswahl.

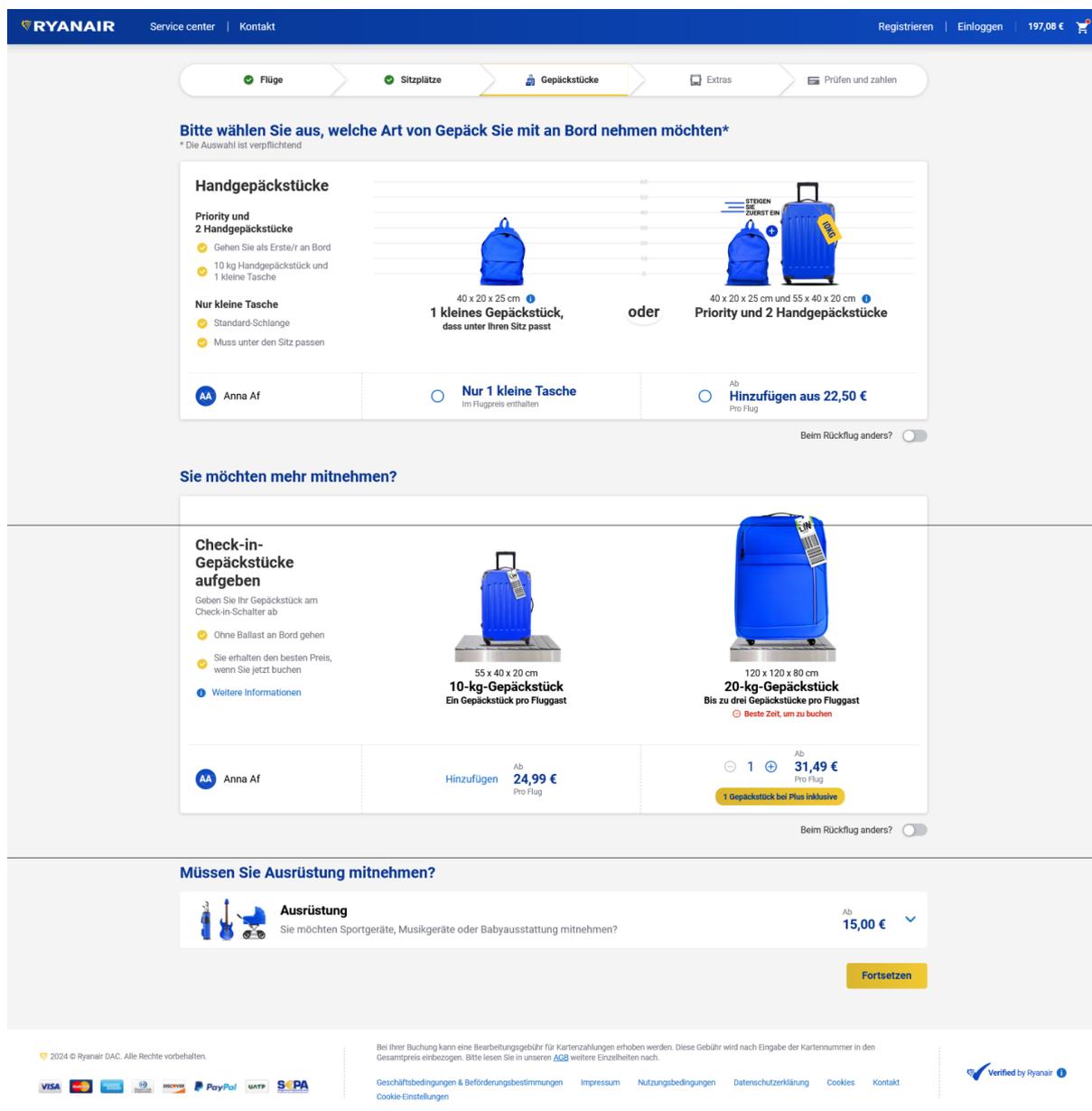


Abbildung 37: Ryanair Gepäck bei Plus Tarif (Screenshot, 17.04.2024).

## Zusatzservice Versicherung

Im vorletzten Schritt des Buchungsprozesses „Extras“ werden Reiseversicherungen angeboten. Es werden **drei Optionen** angeboten – eine „Standardversicherung“, „Versicherung Plus“ und eine „Jahresversicherung“. Als wir keine Zusatzservices auswählen und auf „Fortsetzen“ klicken, kommt es zu einem Pop-Up Fenster.

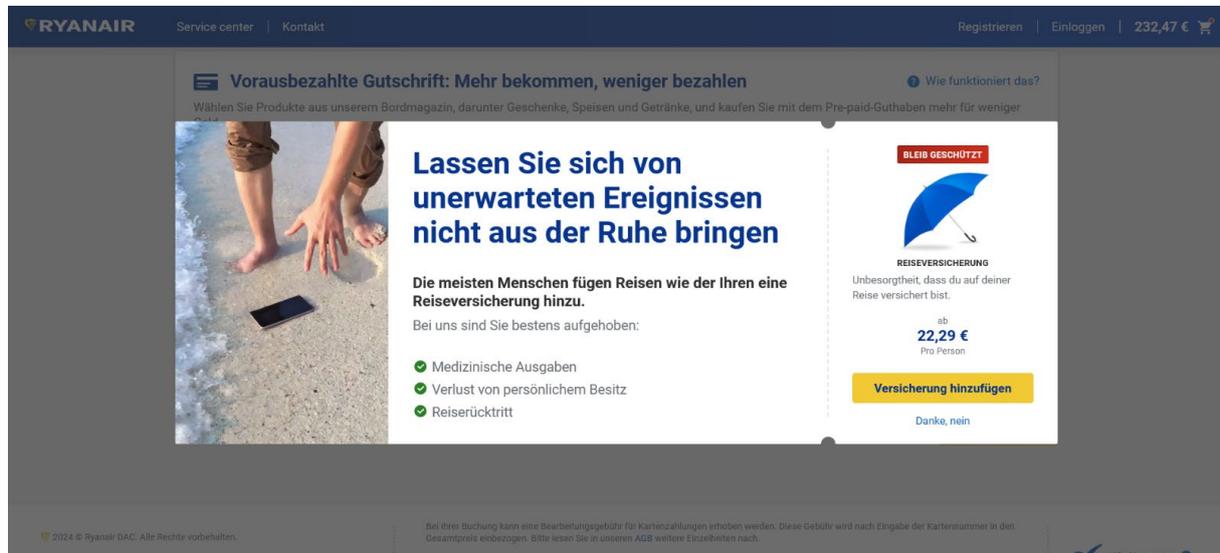


Abbildung 38: Ryanair Pop-Up Versicherungen (Screenshot, 17.04.2024).

**Wordings:** Unter dem Titel „Lassen Sie sich von unerwarteten Ereignissen nicht aus der Ruhe bringen“ wird die Reiseversicherung beworben mit der Angabe „Die meisten Menschen fügen Reisen wie der Ihren eine Reiseversicherung hinzu“.

**Visuelles:** Es gibt nur einen Button „Versicherung hinzufügen“, der gelb ist. Darunter ist der Text „Danke, nein“ als Link, in blau gehalten, platziert.

**Kosten:** Verwiesen wird auf den Standard-Tarif der Versicherung, also die günstigste verfügbare Option.

Klickt jemand beim Pop-Up auf „Versicherung hinzufügen“ gelangt man zur Auswahl der Versicherungspakete und kann aus den drei Optionen auswählen (teilweise nur aus zwei der drei, weil keine Jahresversicherung ausgewählt werden kann). Dabei ist die teurere Versicherung plus visuell hervorgehoben.

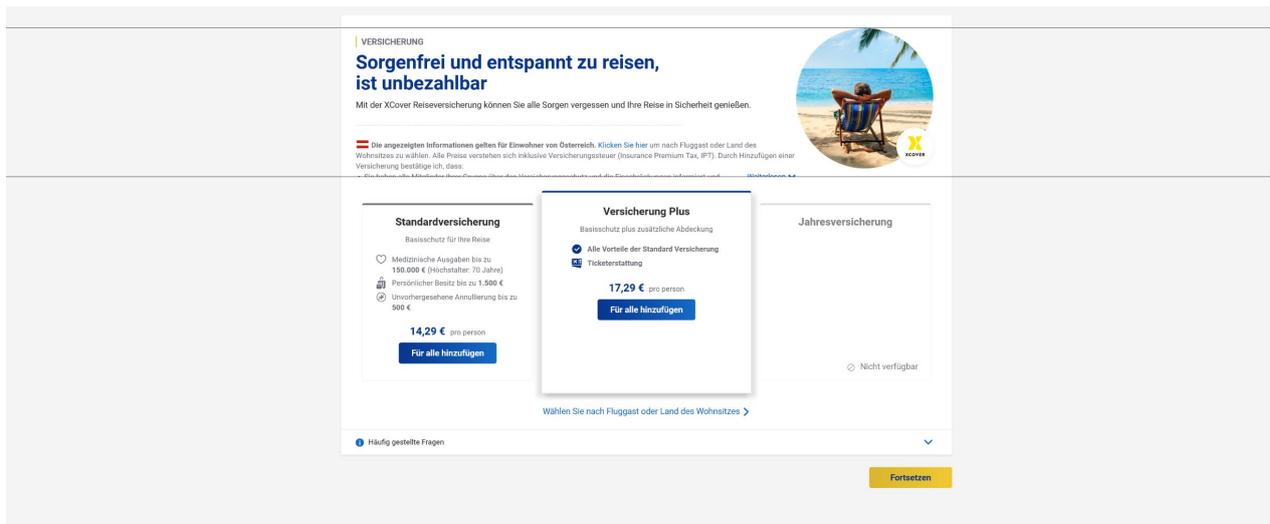


Abbildung 39: Ryanair Versicherungen (Screenshot, 04.09.2023).

## Buchungsprozess Abschluss

Auf der letzten Seite des Buchungsprozesses ist eine Vorauswahl getroffen hinsichtlich eines Abos zu Werbung von Ryanair, die entfernt werden muss, um keine Marketing-Mitteilungen von dem Unternehmen in Form von E-Mail, SMS oder Push-Benachrichtigungen zu erhalten. Das Wording: „Ryanair-Abonnenten erhalten vorzeitigen Zugang zu exklusiven Rabatten auf Flüge und Produkte sowie aktuelle Informationen zu neuen Reisezielen, die nur über Marketing-Mitteilungen angeboten werden. Wenn Sie diese Angebote nicht per E-Mail, SMS oder Push-Benachrichtigung erhalten möchten, entfernen Sie bitte das Häkchen in diesem Feld.“

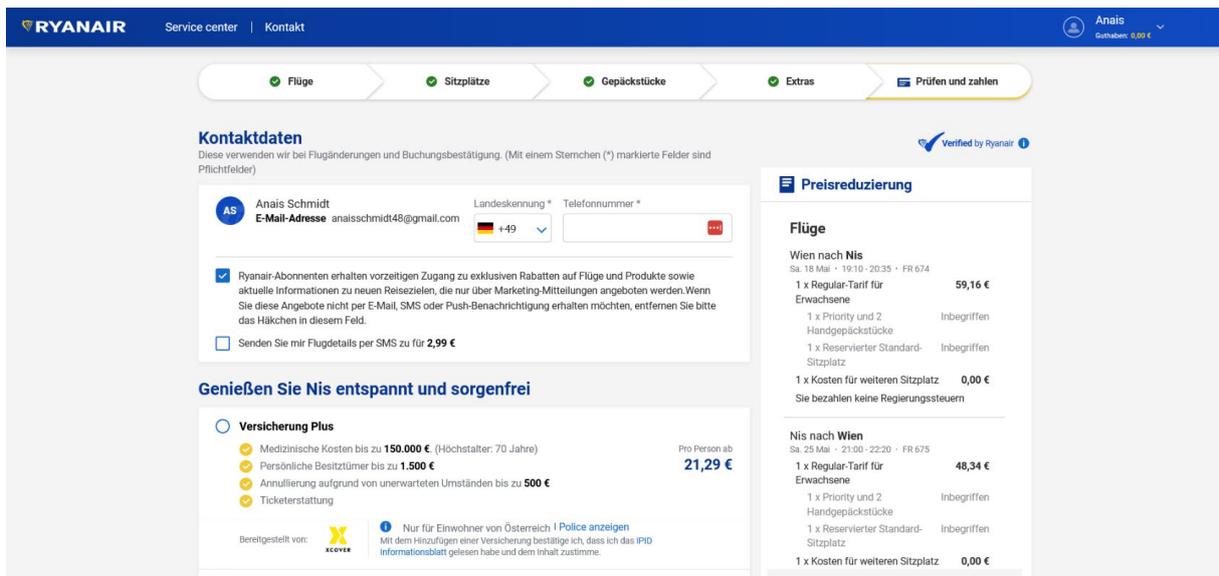


Abbildung 40: Ryanair Vorauswahl Newsletter und Benachrichtigungen (Screenshot, 17.04.2024).

## 4.1.2 Analyse

### Ryanair – undurchsichtige Tarifpakete

Tarifpakete sind eine limitierte Vorauswahl von Kombi-Angeboten – im Idealfall reduzieren sie die Komplexität, indem sie naheliegende gute Optionen zusammenfassen. Der Vergleich der Tarife von Ryan Air lässt jedoch folgende Schlussfolgerung zu: Die Pakete werden nicht im Sinne von Verbraucher:innen eingesetzt.

In keinem der angebotenen Tarifpakete gibt es eine Option mit Handgepäck (10kg) und Abgabegepäck. Die Option eines Flugs mit Handgepäck ist in der Erstauswahl mit Regular zu treffen, allerdings über eine kostenpflichtige Sitzplatzwahl teurer, als wenn ausgehend von der günstigsten Basic-Tarif-Option der Aufpreis für ein Handgepäck zusätzlich gezahlt wird. Anders gesagt: Die zwei Tarife Flugticket mit Handgepäck, Flugticket mit Handgepäck und Abgabegepäck sind keine Optionen, die im Buchungsprozess vorab zusammengestellt werden. Man kann sie zusammenstellen, dann stellen sie günstigere Optionen dar als die Kombi-Tarife (**Price Comparison Prevention**).

Im Folgenden werden die einzelnen Pakete mit den inkl. Leistungen als Variablen dargestellt, um die Komplexität des Auswahlprozesses bzw. die Unmöglichkeit des Preis-Vergleichs für Konsument:innen zu illustrieren. Die Preise der Variablen sind je Flug unterschiedlich, daher kann hier keine allgemeine Aussage darüber getroffen werden. Die angeführten Preise beziehen sich auf ein Beispiel, eines Flugs ausgehend vom Flughafen Wien. Die Tarifauswahl ist gestaltet, sodass ein Kostenüberblick und Preisvergleich während des Buchungsprozesses verunmöglicht wird.

### Tariftabelle – Vergleich

Tarife inklusive Zusatzleistungen	Einzelne Bestandteile des Tarifs	Preis in Euro
Basic Tarif (T <sub>Basic</sub> )	G <sub>kl</sub> , S <sub>random</sub>	152,90 Euro
Basic plus Aufpreis für Handgepäck	G <sub>kl</sub> , G <sub>Hand</sub> , S <sub>random</sub> , inkl. P <sub>priority</sub>	193,90 Euro
Basic plus Aufpreis für Handgepäck und Abgabegepäck	G <sub>kl</sub> , G <sub>hand</sub> , G <sub>grCheck</sub> , P <sub>priority</sub>	247,38 Euro
Regular Tarif (T <sub>Reg</sub> )	G <sub>kl</sub> , G <sub>Hand</sub> , S <sub>hinten</sub> , P <sub>priority</sub>	213,90 Euro
Regular plus Aufpreis für Abgabegepäck	G <sub>kl</sub> , G <sub>Hand</sub> , G <sub>grCheck</sub> , S <sub>hinten</sub> , P <sub>priority</sub>	267,38 Euro
Basic plus Aufpreis für Regular Services	G <sub>kl</sub> , G <sub>Hand</sub> , S <sub>hinten</sub> , P <sub>priority</sub>	213,90 Euro
Plus Tarif (T <sub>Plus</sub> )	G <sub>kl</sub> , G <sub>grCheck</sub> , S <sub>hinten</sub>	226,38 Euro
Plus Tarif mit Aufpreis für kleines Handgepäck	G <sub>kl</sub> , G <sub>Hand</sub> , G <sub>grCheck</sub> , S <sub>hinten</sub> inkl. P <sub>priority</sub>	267,38 Euro
Basic plus Aufpreise für Plus Tarif Services	G <sub>kl</sub> , G <sub>grCheck</sub> , S <sub>hinten</sub>	226,38 Euro
Flexi Plus Tarif (T <sub>Flex</sub> ) Auf diesen Service kann nicht aufgerüstet werden.	G <sub>kl</sub> , G <sub>Hand</sub> , S <sub>alle</sub> , F <sub>Fast Track</sub> , P <sub>priority</sub>	344,30 Euro

Tabelle 1 Vergleich der Tarifpakete mit frei zusammengestellten Zusatzservice-Paketen. <sup>42</sup>

<sup>42</sup> Es wurden die folgenden Abkürzungen verwendet: Basic Tarif (T<sub>Basic</sub>), Regular Tarif (T<sub>Reg</sub>), Plus Tarif (T<sub>Plus</sub>), Flexi Plus Tarif (T<sub>Flex</sub>). Hinsichtlich Sitzplätze: Sitzplatz „Zusätzliche Beinfreiheit vorne“: 21 EUR (S<sub>Bein</sub>), Sitzplatz „Schneller Aussteigen“: 14 EUR (S<sub>exit</sub>), Sitzplatz „Der beste

## Ryanair – Zusatzservices

Die erste neutrale Vergleichbarkeit der Angebote beim Billigfluggesellschaft Ryanair nutzt z. B. zunächst eine neutrale Darstellung in Tabellenform der zu buchenden Leistungen, bei denen unter der Formulierung „Reservierter Sitzplatz“ bei einem der vier angebotenen Tarife kein blauer Haken zu sehen ist. Dies kann als das Dark Pattern „**Trick Wording**“ eingeordnet werden, denn mit Flugbuchung ist jedenfalls ein Sitzplatz garantiert. Die Darstellung in der Tabelle mit dem fehlenden Haken stellt dies in Frage (siehe Abb.28). Wird an dieser Stelle trotzdem der günstigste Tarif gewählt und damit auf das Zusatzservice eines Wunsch-Sitzplatzes verzichtet, verändert sich das UX-Design zu dieser Angabe. Ein Pop-Up unterbricht den Prozess, um abermals den Basic- und der Regular-Tarif gegenüberzustellen, mit anderen Design-Entscheidungen – dies wird als „**Deliberate Misdirection**“ oder „**Tagging**“ bezeichnet. Statt eines fehlenden blauen Hakens erscheint unter der Formulierung „Reservierter Sitzplatz“ beim Basic-Tarif ein rotes Kreuz, das suggeriert es werde kein Sitzplatz reserviert (siehe Abb. 32-34). Dies kann als „**Sneaking**“ definiert werden, bei dem ein User zu einer Entscheidung gedrängt unter Vortäuschung irreführender oder falscher Tatsachen. Gespielt wird in diesem Fall durch die grafische Hervorhebung eines „roten Kreuzes“ mit dem Wording „reservierter Sitzplatz“, dass mit der Entscheidung für den günstigsten Tarif auch eine Entscheidung für einen Flug ohne Sitzplatz suggeriert wird (**Deliberate Misdirection, Sneaking, Trick Wording**).

Wird die Entscheidung beibehalten keine kostenpflichtige Sitzplatzreservierung vorzunehmen, sehen User eine Seite bei der zwei Optionen zu sehen sind, die zweite angezeigte ist „Bevor Sie ohne Sitzplatz fortfahren, ...“ und ist begleitet von drei Ratschlägen (siehe Abb.33). Die gewählte Formulierung „ohne Sitzplatz fortfahren“ suggeriert fälschlicherweise, dass ein Flug ohne Sitzplatz gebucht würde. Auch die Ratschläge können als suggestiv bezeichnet werden: Der erste Vorschlag „Vermeiden Sie einen Platz in der Mitte“ suggeriert, dass ohne zusätzlich gekaufte Reservierung ein Platz in der Mitte wahrscheinlich sein könnte. Der zweite Vorschlag betitelt mit „Sitzplatzverfügbarkeit“ suggeriert, dass die späte Reservierung zu einem Sitzplatzverfügbarkeitsproblem führen könnte. „Derzeit bester Preis“ gibt an, dass die günstigsten Sitzplätze schnell ausverkauft sind, bzw. die Plätze zu einem späteren Zeitpunkt teurer werden – laut unseren Aufzeichnungen verändern sich die Preise der Sitzkategorien nicht, dies ist jedoch noch weiters zu prüfen (**Trick Wording, Confirm Shaming**). Zwei Buttons auf dieser Seite sind visuell unterschiedlich und auch begrifflich wertend. In Gelb hervorgehoben ist ein Button „Ohne Sitzplatz fortfahren“, der zweite Button „Wählen Sie jetzt die Sitzplätze“ ist ein Zurück-Button zur

---

Deal vorne“: 8-10 EUR ( $S_{\text{vorn}}$ ), Sitzplatz „Der beste Deal hinten“: 8 EUR ( $S_{\text{hinten}}$ ), Sitzplatz „Ausstrecken für wenig Geld“: 15 EUR ( $S_{\text{xl}}$ ), Sitzplatz „später auswählen – automatisch auswählen“: 0 EUR ( $S_{\text{random}}$ ). Hinsichtlich Gepäck: 1 kleine Tasche/kleines Gepäckstück (passt unter den Sitzplatz, 40x20x25cm): 0 EUR ( $G_{\text{kl}}$ ), 2 Handgepäckstücke (1 kleine Tasche und 1 Handgepäckskoffer, 10kg, 55x40x20cm): ab 10 EUR ( $G_{\text{Hand}}$ ), 10-kg-Gepäckstück (55x40x20cm, Check-in-Gepäckstück): ab 10 EUR ( $G_{\text{klCheck}}$ ), 20-kg-Gepäckstück (120x120x80cm, Check-in-Gepäckstück): ab 19,90 EUR ( $G_{\text{grCheck}}$ ), Variablen Versicherung: Versicherung Standard: ab 12,90 EUR (variabel) ( $V_{\text{Stand}}$ ), Versicherung Plus: ab XXX ( $V_{\text{Plus}}$ ), Versicherung Jährlich: ab XXX ( $V_{\text{Jahr}}$ ), Variablen Priority: Fast Track Sicherheitskontrolle: ab 6 EUR ( $P_{\text{security}}$ ), Priority Boarding: ab 6 EUR ( $P_{\text{priority}}$ )

Sitzplatzauswahl. Eine neutrale Formulierung wie „Weiter“ fehlt – es handelt sich um tendenziöse Formulierung die als „**Confirmshaming**“ und „**Tagging**“ eingeordnet werden können (**Deliberate Misdirection, Tagging, Confirmshaming, Trick Wording**).

Fahren die Kund:innen ohne kostenpflichtige Sitzplatzreservierung fort, werden sie mit einem Pop-Up konfrontiert, das die zuvor mehrmals getroffene Entscheidung abermals in Frage stellt (siehe Abb. 34, **Nagging, Obstruction**). Die Sprache, die in dem Pop-Up verwendet wird, suggeriert den Kund:innen, dass es zu Ihrem Nachteil ist, keine kostenpflichtige Sitzplatzreservierung vorzunehmen (**Confirmshaming**). Sie werden auf die Nachteile hingewiesen wie „Check-In ist erst 24 Stunden vor dem Flug möglich“; „Sie können an jedem beliebigen Sitzplatz im Flugzeug platziert werden“, etc. Zudem ist die Button Gestaltung wie auch bei der nicht getroffenen Sitzplatzreservierung tendenziös: „Wählen Sie jetzt die Sitzplätze“ ist als gelber Button gestaltet, der blau hinterlegt ist, ein Design, das eine Vorauswahl suggeriert (**Tagging, Deliberate Misdirection**). Bei diesem Button handelt es sich um einen simplen „Zurück-Button“ der wieder zur kostenpflichtigen Sitzplatzauswahl führt. Will man weiterhin bei der Entscheidung bleiben, keine kostenpflichtige Reservierung vorzunehmen, muss man auf einen blauen Link unter dem Button klicken, der nicht als Button gekennzeichnet oder hervorgehoben ist.

Bei Ryanair weist bei der Auswahl des Basic-Tarifs ein Warnhinweis darauf hin, dass kein zusätzliches Gepäckstück gebucht wurde. In diesem Fall, darf nur eine kleine Handtasche (kein Handgepäckskoffer) mitgeführt werden (siehe Abb. 35). Die Beschreibung dieser Option könnte als „**Confirm Shaming**“ beschreiben werden, da die Optionen beschrieben werden mit „Nur 1 kleine Tasche“ – wird diese Option gewählt werden Kund:innen auf mögliche Zusatzkosten am Flughafen hingewiesen. Alle Hinweise und Formulierung sind darauf zugeschnitten, Reisende dazu zu bringen, ein zusätzliches Handgepäckstück für einen Aufpreis dazubuchen.

Wird bei Ryan Air keine Versicherung gewählt, wirbt ein Pop-Up um nochmaliges Überdenken der Entscheidung. Das Wording kann als Dark Pattern „**Fake Social Proof**“ eingeordnet werden: „Die meisten Menschen fügen Reisen wie der Ihren eine Reiseversicherung hinzu“. Dazu kommt, dass auf diesem nur ein Button zu sehen ist mit dem Text „Versicherung hinzufügen“ – um bei der schon getroffenen Entscheidung zu bleiben, müssen User auf den Text unten „Danke, nein“ klicken, der als Link gesetzt ist und visuell untergeht (siehe Abb. 38) (**Nagging, Deliberate Misdirection, Fake Social Proof, Confirm Shaming**). Zusätzlich ist der Empfang des Newsletters bzw. von Marketing-Botschaften beim Abschluss der Buchung vorausgewählt (siehe Abb. 40., **Preselection**).

**Rechtliche Einordnung:** Eine Geschäftspraxis gilt als aggressiv, wenn sie im konkreten Fall unter Berücksichtigung aller tatsächlichen Umstände die Entscheidungs- oder Verhaltensfreiheit des Durchschnittsverbrauchers in Bezug auf das Produkt durch unzulässige Beeinflussung tatsächlich oder voraussichtlich erheblich beeinträchtigt und diesen tatsächlich oder voraussichtlich dazu veranlasst, eine geschäftliche Entscheidung zu treffen, die er andernfalls nicht getroffen hätte (Art. 8 UGP-RL). Es ist daher fraglich, ob die Verwendung von in dieser Analyse identifizierten Dark Patterns als unzulässige Beeinflussung gemäß Art. 8 UGP-RL eingestuft werden kann.

## 4.2 Case Study „Austrian Airlines“

### 4.2.1 Dokumentation

**Dokumentationsgrundlage:** Screenshots des Buchungsprozesses von 18.04.2024. Bitte zu beachten, dass der Buchungsprozess regelmäßig verändert wird und die Heranziehung der Beispiele insofern nur mit Hinweis auf Datum erfolgen sollte.

#### Wahl des Flugtarifs

Im Buchungsprozess vergleichbar wird anhand eines Datums eine Auswahl mit jeweils einzeln bepreisten Flügen angezeigt. Danach folgt eine Auswahl nach Uhrzeit. Bei der Auswahl der Uhrzeit gibt es auf ersten Blick zwei Tarife zur Auswahl – „Economy“ und „Business“. Der Klick auf jeden dieser Tarife führt zu weiteren Optionen.

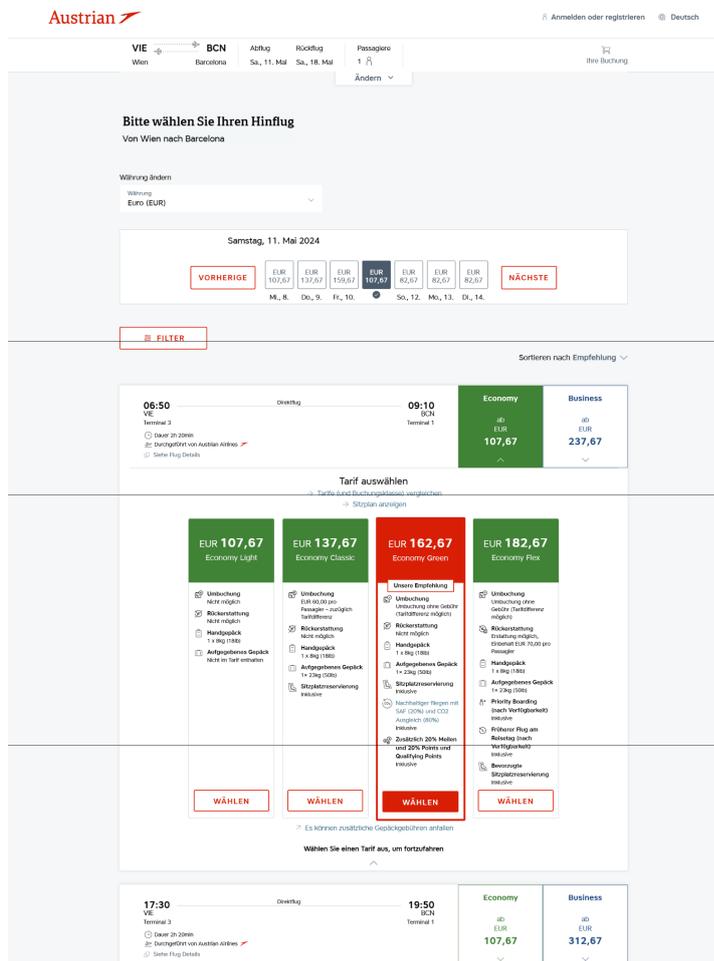


Abbildung 41: Austrian Tarife Economy (Screenshot, 18.04.2024).

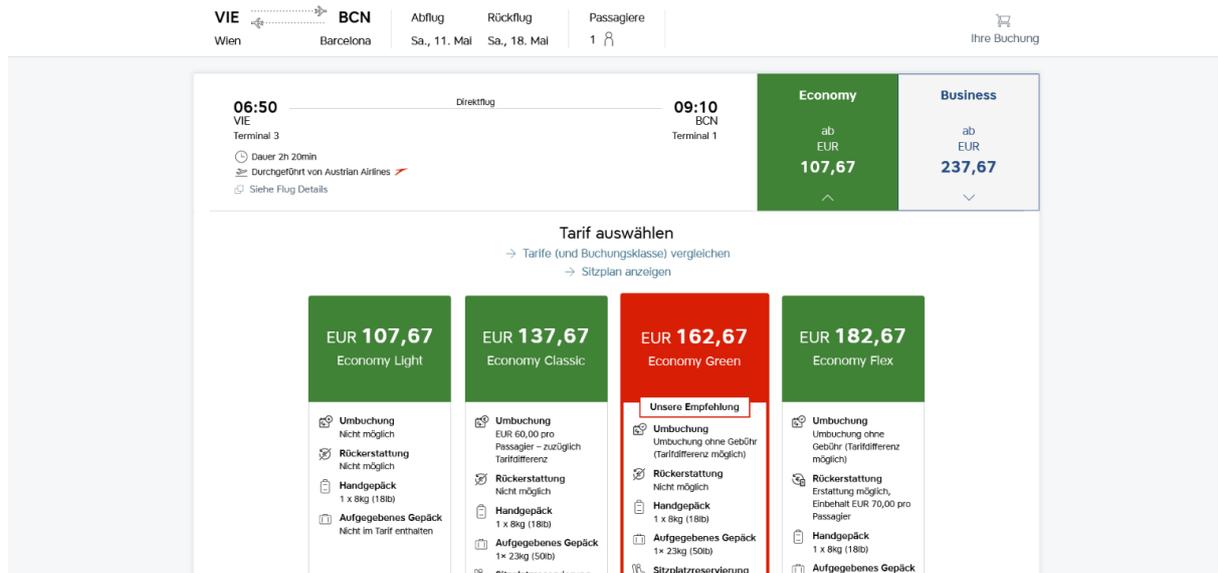


Abbildung 42: Austrian Tarife Preise (Screenshot, 18.04.2024).

**Visuell:** Diese Optionen sind nebeneinander mit Gesamtpreis aufgeführt. Auch hier gibt es keine Vorauswahl aber eine visuelle Hervorhebung einer Option („Economy Green“) mit der Unterschrift „Unsere Empfehlung“, die eine Vorauswahl suggeriert. Der Economy Green Tarif erhält außerdem das Label „Unsere Empfehlung“. Die Buttons sind gleich gestaltet. Ebenso gibt es bei Business Unterkategorien, von denen die „ökologische“ Variante „Business Green“ hervorgehoben und empfohlen wird.

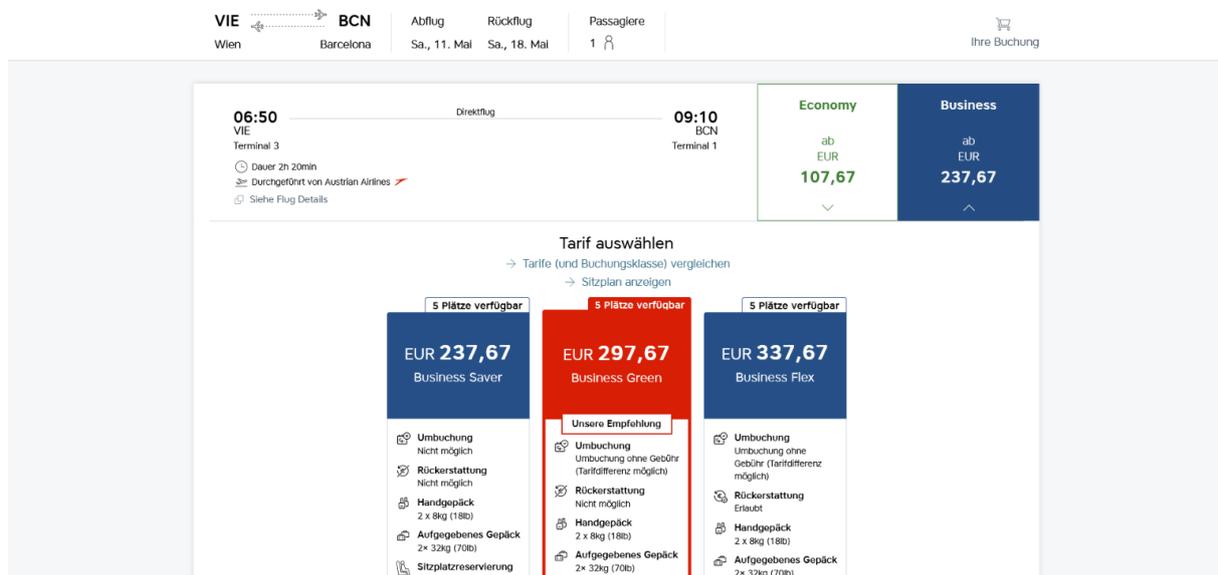


Abbildung 43: Austrian Business Tarife (Screenshot, 18.04.2024).

**Gepäck:** Alle Economy-Optionen inkludieren ein Handgepäck und die Angabe „Sitzplatzreservierung inklusive“ fehlt nur bei „Economy Light“. Bei Economy Light fehlt die Angabe „Sitzplatzreservierung inklusive“, aber es wird nicht als fehlend hervorgehoben und keine Verunsicherung erzeugt. Alle Economy Optionen mit Ausnahme Light inkludieren auch ein Abgabegepäck.

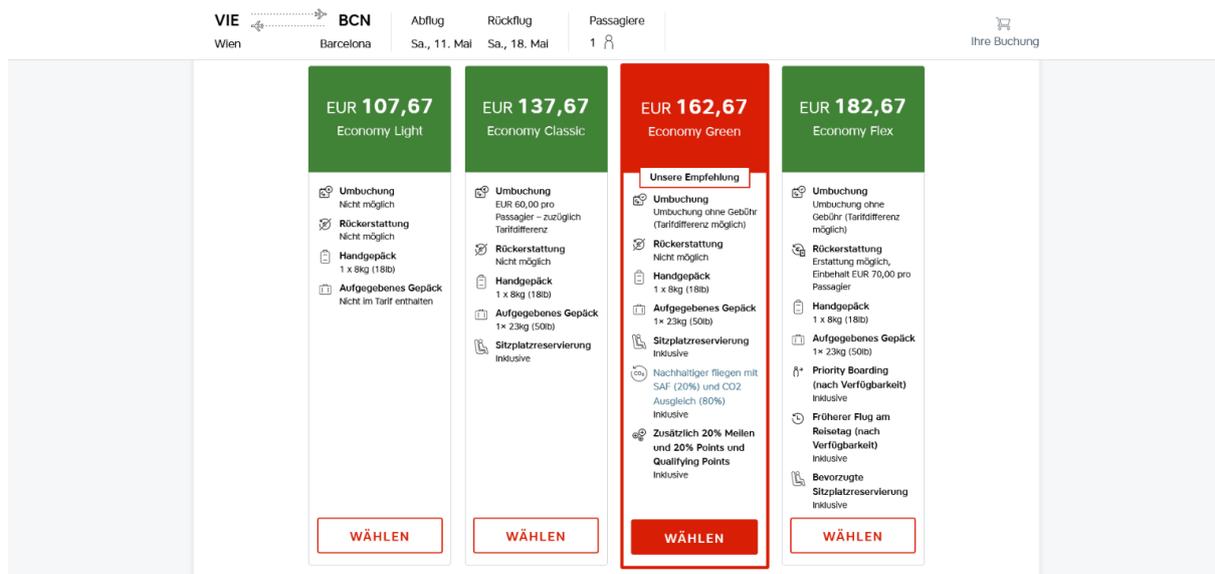


Abbildung 44: Austrian Economy Preise inkludierte Leistungen (Screenshot, 18.04.2024).

Bei Auswahl der günstigsten Variante (Economy Light) folgen keine weiteren Aufforderungen die Entscheidung zu ändern, Gepäck oder Versicherung hinzuzufügen oder eine kostenpflichtige Sitzplatzauswahl. Diese Möglichkeit erscheint nach Angabe der Passagierdaten auf unaufdringliche Art und Weise.

### Preisdarstellung und Preisvergleich

Der Preisvergleich zeigt, dass ein Aufbuchen von Sitzplatz und Gepäck zur Abgabe zusätzlich zum billigsten Tarif insgesamt teurer ist als die Option gleich anfangs zu wählen. Kostet der Economy Light Tarif (inkl. Handgepäck  $G_{Hand}$ ) 123,67 EUR, der Economy Classic Tarif (inkl. Handgepäck, Aufgabegepäck und Sitzplatz:  $G_{Hand} + G_{grCheck} + S_{frei}$ ) 153,67 EUR. Bucht man jedoch zu dem günstigsten Economy Light Tarif (123,67 EUR) ein zusätzliches Aufgabegepäck (30 EUR) und einen frei wählbaren Sitzplatz (16 EUR) hinzu, kommt man auf Extrakosten von über 46 EUR und somit auf einen Gesamtpreis von 169,67 EUR. Das sind 16 EUR mehr, als wenn die Kund:innen anfänglich den Economy Preis gewählt hätten.

In der Economy Tarifgruppe ist der Economy Green Tarif (173,67 EUR) um 50 Euro teurer als der günstigste Economy Light Tarif (123,67 EUR), der gleiche Preisunterschied besteht in der Business Tarifgruppe zwischen dem günstigsten Business Tarif (Business Saver) und dem Business Green Tarif (423,67 vs. 473,67 EUR, Differenz 50 EUR).

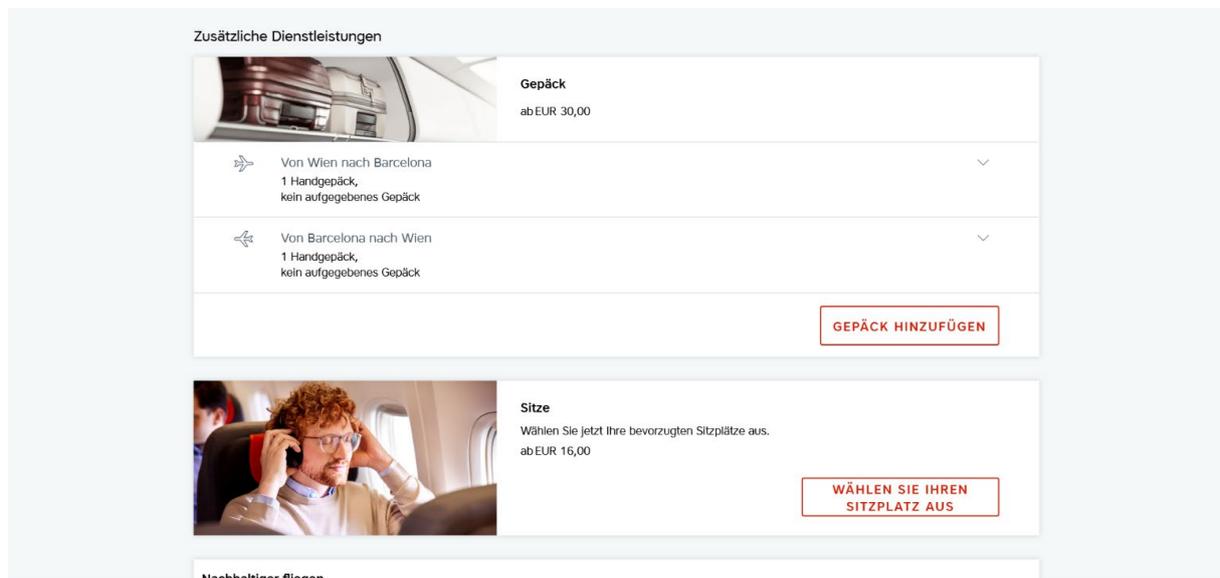


Abbildung 45: Austrian Zusatzleistungen Sitzplätze und Gepäck (Screenshot 18.04.2024).

## 4.2.2 Analyse

In der Tarifauswahl bei Austrian Airlines wird zunächst der billigste Tarif in der Economy Klasse und daneben der billigste Tarif der Business Klasse angezeigt. Beim Klick auf Economy oder Business werden die einzelnen Tarifoptionen in der Tarifgruppe angezeigt. Bei beiden Tarifgruppen sind die „Green“-Tarife visuell hervorgehoben (**Deliberate Misdirection, Tagging**).

Anzumerken ist, dass bei Austrian die Tarifoption Economy Classic für Kund:innen günstiger ist als die Zusatzservices (1 zusätzliches Aufgabepäck und manuelle Sitzplatzauswahl) später extra hinzuzufügen. Bucht man ein zusätzliches Aufgabepäck und einen Sitzplatz hinzu, entstehen extra Kosten von 16 EUR, als wenn die Kund:innen anfänglich den Economy Preis gewählt hätten (**Comparison Prevention**).

**Rechtliche Einschätzung:** Zur Verbesserung der Transparenz und um eine besser informierte Entscheidung bei der Buchung treffen zu können, wäre es sinnvoll, dass die Verbraucher:innen bei der Wahl der Tarifoption konkrete Informationen über die Kosten der Zusatzservices erhalten.

Im Falle der Austrian Airlines ist ab Anfang des Prozesses bereits transparent, insofern entlang der vier Pakete formuliert wird, dass ab dem Basic-Tarif eine Sitzplatzreservierung inklusive ist (in 3 der 4 Tarife). Es gibt beim günstigsten Economy Light-Tarif zwar keine Angabe zum Sitzplatz (z. B. Sitzplatzzuweisung nach Zufall), allerdings auch keine verunsichernde Formulierung, die suggerieren könnte, dass es sich um eine Flugbuchung ohne Sitzplatz handelt. In weiterer Folge folgen auch bei Auswahl der günstigsten Variante (Economy Light) keine weiteren Aufforderungen eine kostenpflichtige Sitzplatzauswahl zu buchen. Diese Möglichkeit erscheint erstmalig nach Eingabe der Passagierdaten (kein Pop-Up, unaufdringlich).

Einzig bei Austrian Airlines wird die zusätzliche Auswahl von Aufgabepäck ohne erkennbares Nagging oder Confirmshaming gestaltet. Bei der Auswahl von

Zusatzservices gibt es die Option zusätzliche Aufgabegepäckstücke zu buchen. Die Option ist farblich schlicht gehalten und die Kund:innen werden nicht gedrängt, zusätzliche Services zu buchen (siehe Abb. 45).

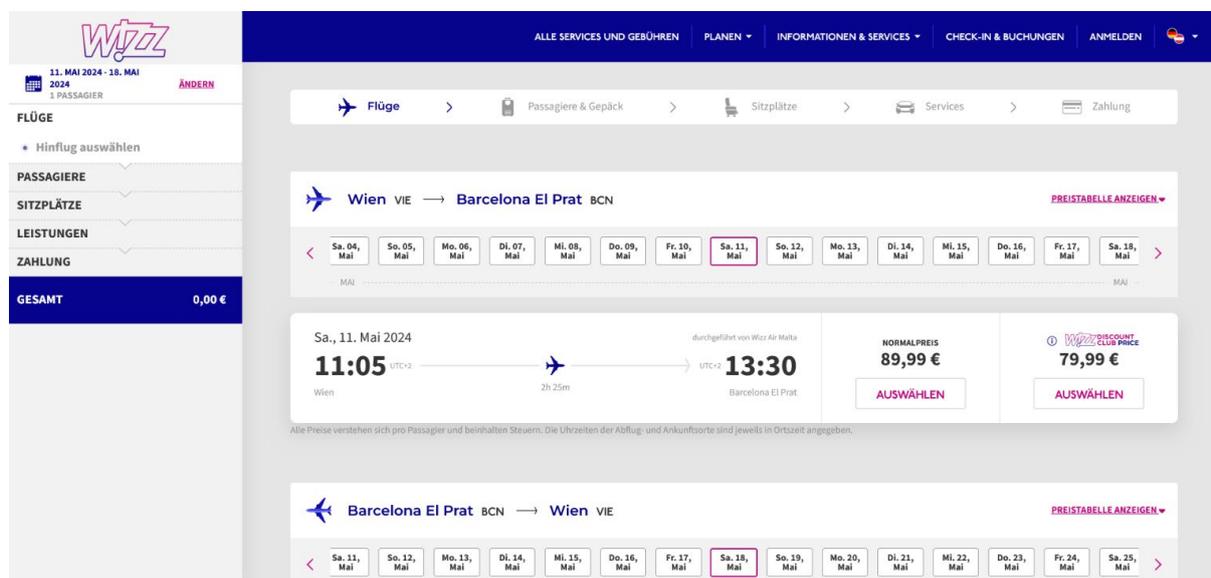
Auch wird nicht gesondert auf die Buchung einer Versicherung hingewiesen, alle Zusatzservices wurden ähnlich unauffällig wie zusätzliche Sitzplatzreservierungen oder Zusatzgepäck beworben (siehe Abb. 45).

## 4.3 Case Study „Wizz Air“

### 4.3.1 Dokumentation

**Dokumentationsgrundlage:** Screenshots des Buchungsprozesses von 18.04.2024 und 03.05.2024. Zu beachten ist, dass der Buchungsprozess regelmäßig verändert wird und die Beispiele insofern nur mit Hinweis auf Datum verwendet werden sollten.

Der Buchungsprozess bei Wizz Air startet mit Angabe eines Wunschdatums, gefolgt von einer möglichen Auswahl an Flügen mit Uhrzeit. Angeführt wird je Flug ein „Normalpreis“ und ein günstigerer „Wizz Discount Club“-Preis. Eine Übersicht der Preiszusammensetzung auf der linken Seite der Website schlüsselt laufend die Kosten der ausgewählten Services auf.



The screenshot displays the Wizz Air booking process. On the left, a sidebar shows the booking details: 11. Mai 2024 - 18. Mai 2024, 1 Passagier, and a total price of 0,00 €. The main area shows a flight selection calendar for the route Wien (VIE) to Barcelona El Prat (BCN). The selected date is Saturday, May 11, 2024. The flight card shows a departure time of 11:05 from Wien and an arrival time of 13:30 at Barcelona El Prat, with a 2h 25m duration. Two pricing options are presented: a Normalpreis of 89,99 € and a Wizz Discount Club Price of 79,99 €. The interface also includes a navigation menu at the top and a calendar view for the return flight from Barcelona El Prat to Wien.

Abbildung 46. WizzAir Flugauswahl (Screenshot, 18.04.2024).

Bei Auswahl des Normalpreises erscheint eine Übersicht zu drei Tarifpaketen: „Alles Drin & Voll Flexibel“, „Packen & Sparen“ und „Einfach Reisen“. Visuell ist der Normalpreis ausgegraut, auch der Button hat keine Farbe. Angegeben wird der Gesamtpreis beim Normalpreis, wohingegen die zwei anderen Pakete mit dem preislichen Aufschlag je Flug angegeben sind.

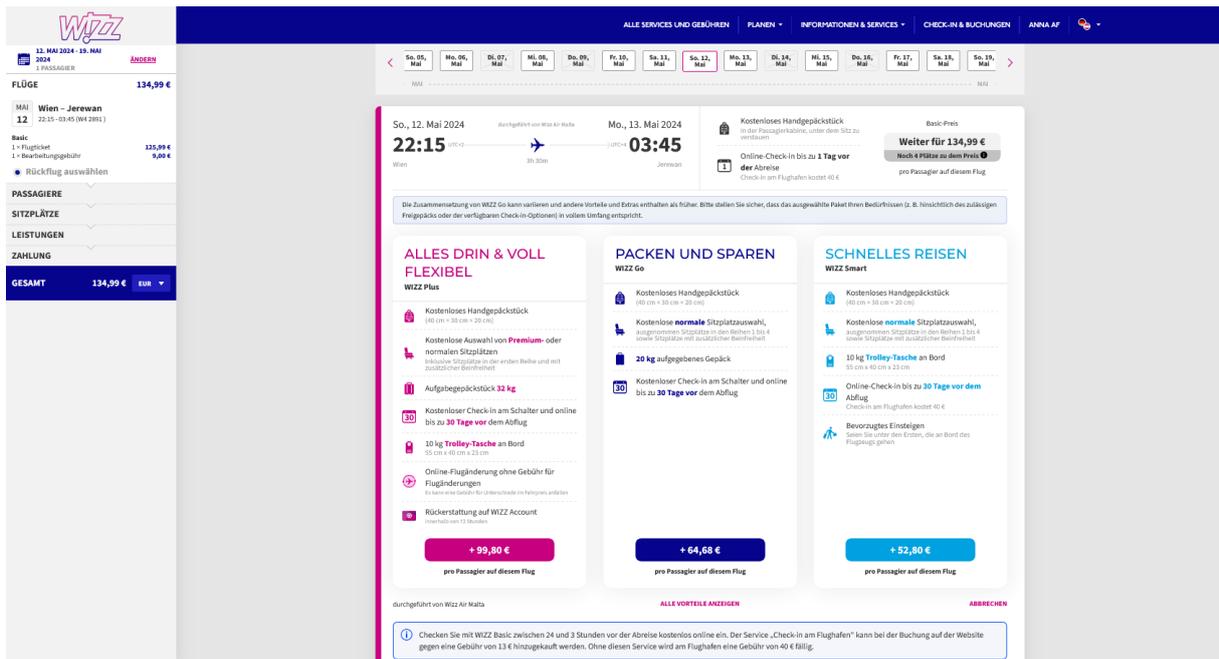


Abbildung 47: Auswahl der Flugtarife WizzAir (Screenshot, 03.05.2024).

Ähnlich ist das Prozedere bei Auswahl des „Wizz Discount Club“-Preises. Der Tarif erscheint unter dem Wording „Einfach Reisen“ und „Basic“, ausgegraut, und auch hier sind die zwei weiteren Tarife nicht mit Gesamtpreis angezeigt, sondern mit dem Aufschlag auf den Preis. Die Auswahl für den Tarif muss für den Hin- und für den Rückflug getroffen werden.

Im Vergleich zwischen Abbildung 47 und Abbildung 48 werden die schnellen Veränderungen in der Gestaltung der Websites ersichtlich. Zwischen der Dokumentation der beiden Screenshots liegen ca. zwei Wochen, doch die Darstellung der Tarifpakete hat sich signifikant verändert.

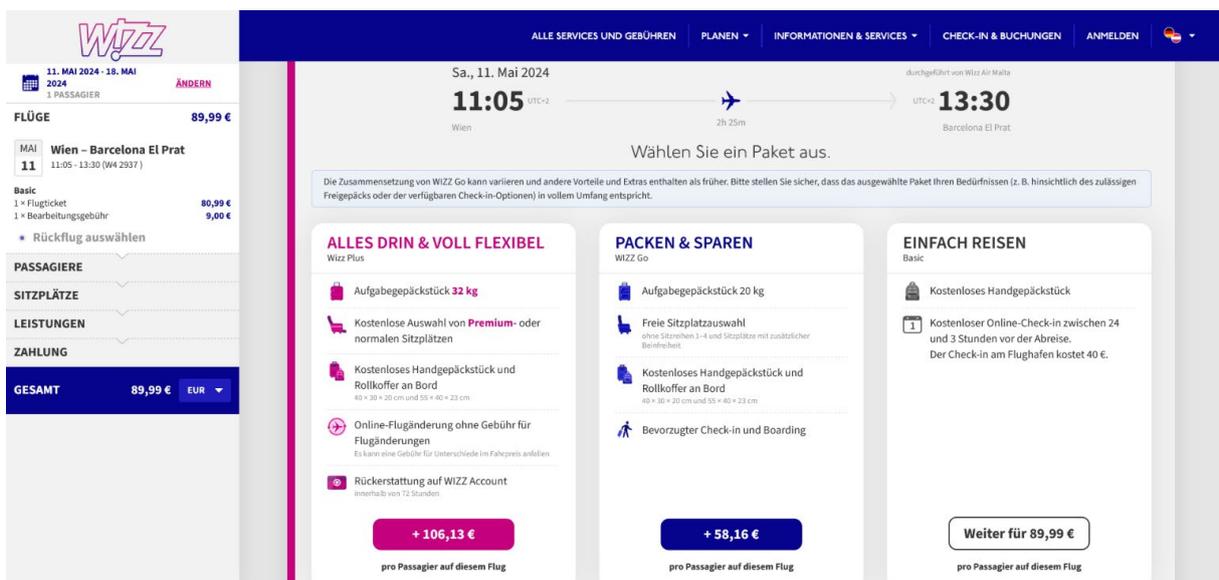


Abbildung 48: Wizz Tarifauswahl (Screenshot, 18.04.2024).

## Sitzplatzauswahl

Nach Auswahl der Tarife je Flug kommt es zur Sitzplatzauswahl.

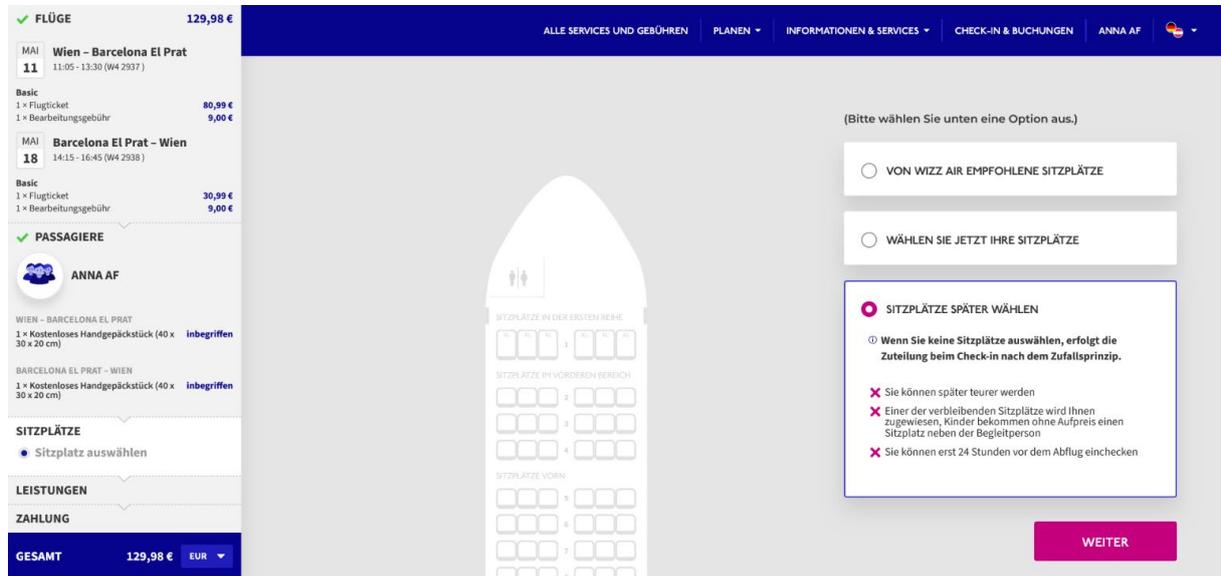


Abbildung 49: Wizz Sitzplatzauswahl (Screenshot, 18.04.2024).

Hervorgehoben (ausgeklappt) ist dabei auf der rechten Seite die Option „von Wizz Air empfohlene Sitzplätze“. Möchte man nicht zusätzlich für die Sitzplatzauswahl zahlen, bleibt die Option „Sitzplätze später wählen“. Diese ist mit dem Hinweis versehen: „Wenn Sie keine Sitzplätze auswählen, erfolgt die Zuteilung beim Check-In nach dem Zufallsprinzip“.

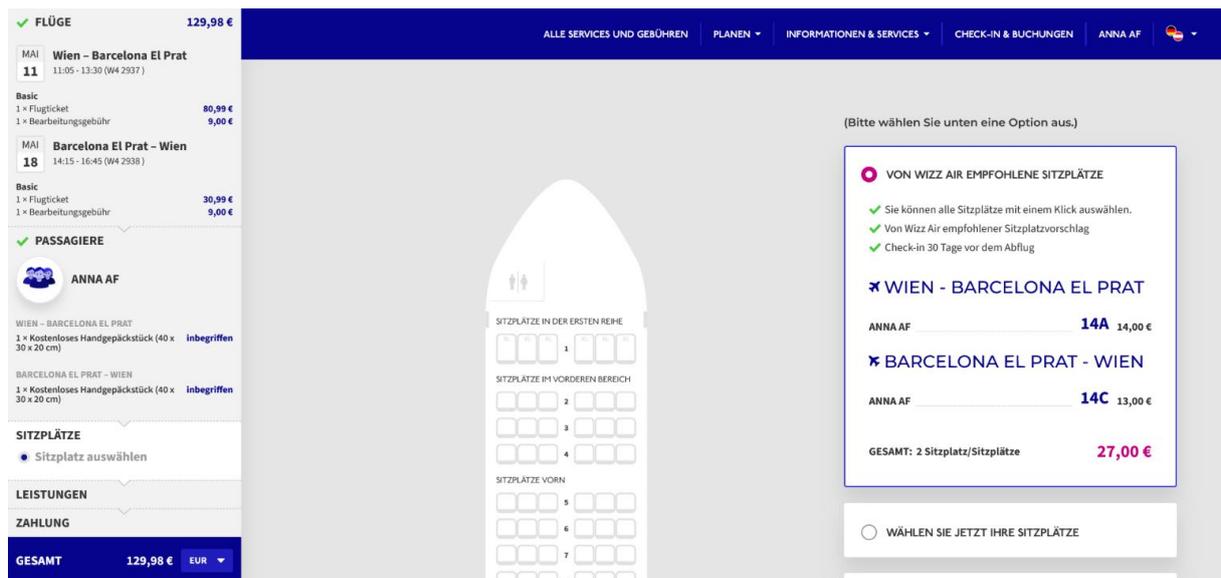


Abbildung 50: Wizz Empfohlene Sitzplatzauswahl (Screenshot, 18.04.2024).

## Abomodell Wizz-Club

**Wizz-Club:** nach Auswahl der Flüge, Login, Sitzplatz und Versicherungsoptionen (neutral gehalten), kommt eine Seite zum Wizz Discount Club. Auf dieser Seite wird für den Wizz Discount Club, ein Abo-Modell, geworben. Visuell auffällig ist der Button unten auf der Seite – hier befindet sich nur ein Button mit der Aufschrift „Mitglied werden“. Möchte man kein Mitglied im Wizz Discount Club werden, ist weiter unten auf der Seite ein Link gesetzt „nein, ich möchte nicht 20 Euro sparen“, um diesen zu sehen, muss jedoch ans Ende der Seite gescrollt werden.

Die Mitgliedschaft kostet 39,99 Euro jährlich. Beworben wird der Wizz Discount Club mit „JETZT SPAREN: 20 EUR“, darunter steht in kleiner, aber fetter Schrift „Der Jahresbetrag für die Mitgliedschaft beträgt 39,90 EUR“. Auch rechts in einer blauen Box sind Rabatte aufgelistet, auf den Flugpreis gäbe es für Mitglieder 10 Euro Rabatt, auf Aufgabegepäck 5 Euro. Jedoch ist unklar, wo der Rabatt angewandt wurde bzw. wird. Außer des kleinen Hinweises in Textform wird nicht klar, dass es zu jährlichen Kosten von über 30 Euro kommen wird, und dass hier ein Abo abgeschlossen wird. Die Konsument:innen bekommen auch hier keinen Überblick über die Gesamtkosten des Abonnements.

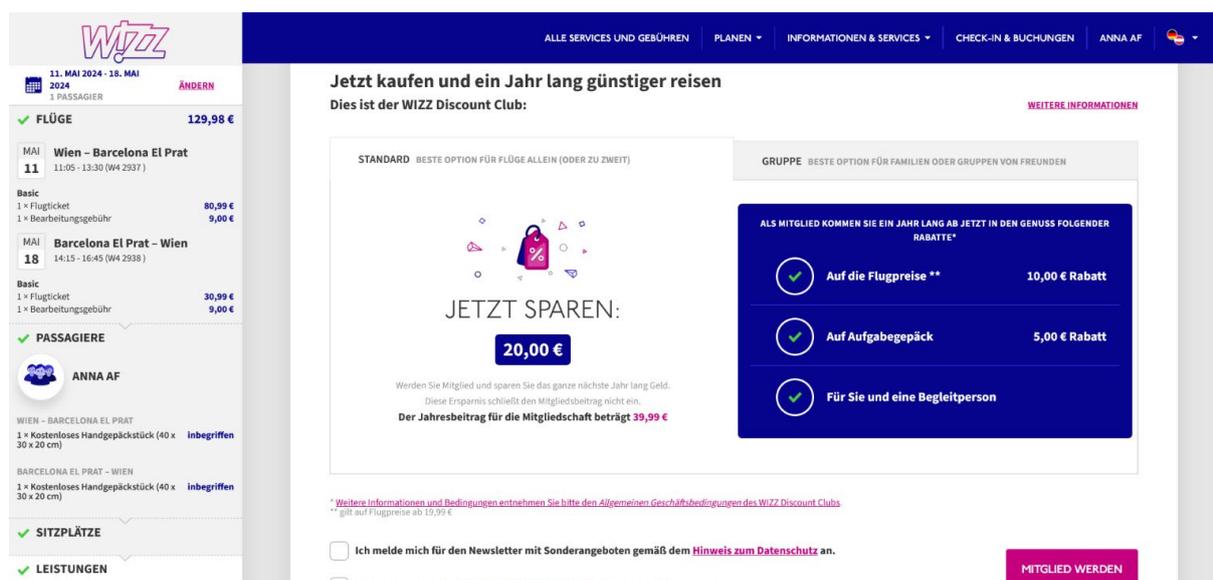


Abbildung 51: Wizz Anzeige Wizz Discount Club „Mitglied werden“ (Screenshot, 18.04.2024).

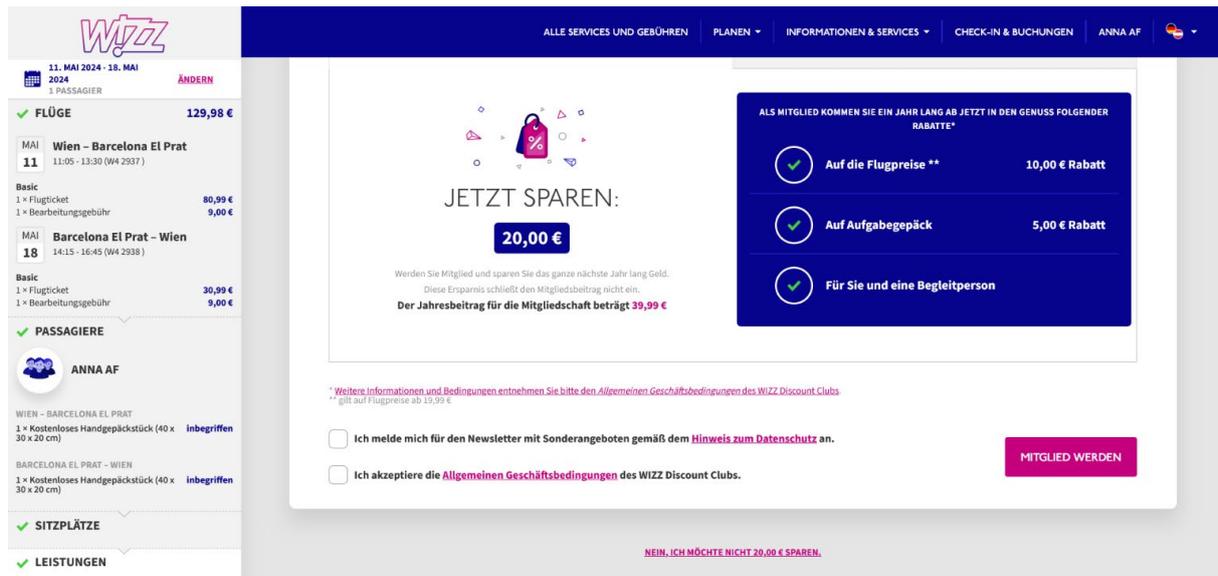


Abbildung 52: Wizz Discount Club – schwieriges Opt-Out (Screenshot, 18.04.2024).

Wizz Air bietet zusätzlich zahlreiche Zusatzleistungen an. Es kann von Wizz Priority (Priority Check-in und Handgepäck) über Auto-Check-in (ein automatisches Check-in durch das System, 50 Stunden vor Abflug), Check-in am Flughafen, Parken am Flughafen, Flughafentransfer, Security Fast Track, Mietwägen, Exclusive Lounge Zugang bis zur Reiseversicherung alles gebucht werden. Die Formulierungen sind hier neutral gehalten, lediglich einzelne Zusatzservices sind mit einem Banner in dunkelblau und der Überschrift „EMPFEHLUNG“ gekennzeichnet.

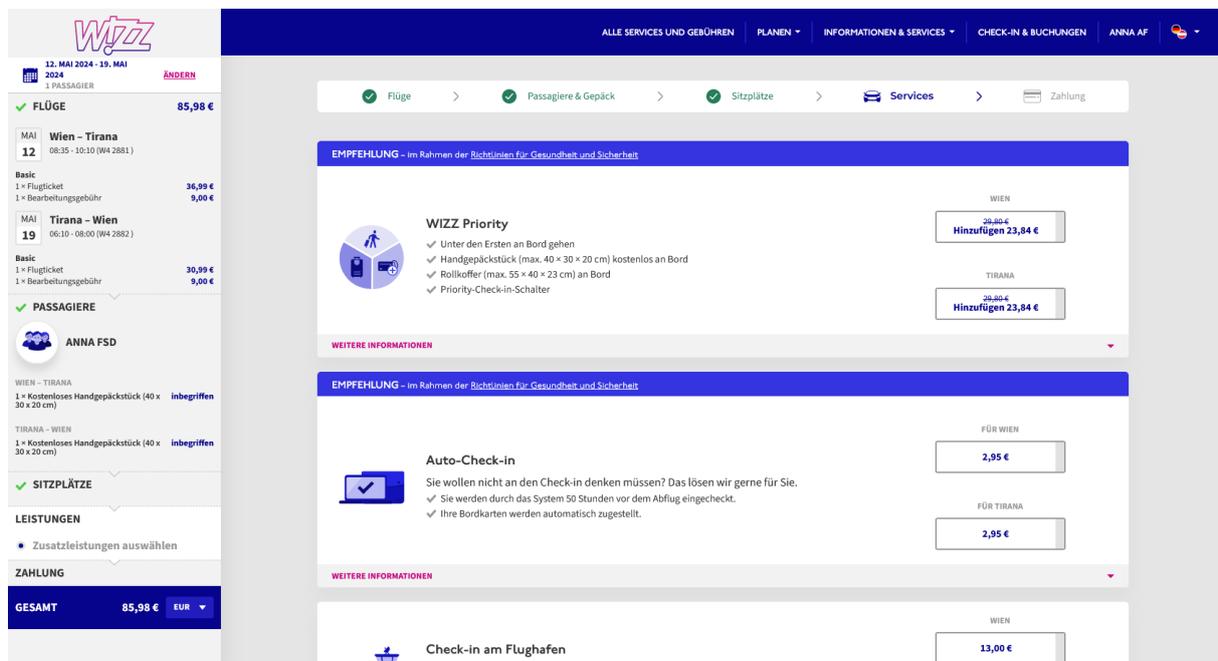


Abbildung 53: Zusatzservices von Wizz Air (Screenshot, 03.05.2024).

### 4.3.2 Analyse

#### Nagging für die Auswahl des „Wizz Discount Clubs“

Bucht man bei Wizz Air einen Flug, hat man direkt bei der Zeit- bzw. Datumsauswahl des Fluges die Option, den um 10 Euro teureren Normalpreis zu wählen, oder den vergünstigten Wizz Discount Club Preis. Wählt man im ersten Schritt die teurere Normalpreis Variante, wird man zunächst gefragt, ob man ein zusätzliches Tarifpaket auswählen will. Die Auswahl besteht zwischen dem „Alles drin & voll flexibel“, „Packen und Sparen“, und „Schnelles Reisen“ Tarif, die alle farblich hervorgehoben sind. Will man diese Pakete nicht auswählen, gibt es einen ausgegrauten Button der mit „Weiter für 45,99 EUR“ beschriftet ist. Bei der Auswahl des Rückfluges wiederholt sich dieser Prozess. Diese Art des Buchungsvorganges, kann als „**Nagging**“ beschrieben werden, da sich die Kund:innen immer wieder gegen das Wizz Abo-Modell des Wizz Discount Club sowie gegen die teureren Tarif-Pakete entscheiden müssen. Zudem wird ein transparenter Vergleich der Preise verhindert (**Comparison Prevention, Nagging**).

Auch später im Buchungsprozess, werden Kund:innen nochmals dazu aufgefordert, Discount Club Mitglieder zu werden, in Form einer Werbeseite. Die Buttons auf der Werbeseite für den Wizz Air Discount Club sind tendenziös gestaltet (**Tagging, Deliberate Misdirection**). Es wird nur ein Button aufgeführt, dieser ist pink ausgefüllt und beschriftet mit den Worten „MITGLIED WERDEN“. Wollen Kund:innen kein Mitglied werden, ist auf den ersten Blick keine Alternative sichtbar. Um kein Mitglied zu werden, muss zum Ende der Seite gescrollt werden, hier findet sich ein unscheinbarer Link in pink gehalten auf dem steht „NEIN, ICH MÖCHTE NICHT 20,00 EUR SPAREN“. Die emotional tendenziöse Formulierung kann als „**Confirm Shaming**“ eingeordnet werden, zudem sind die Prozesse tendenziös gestaltet (**Confirm Shaming, Deliberate Misdirection**). Mit dem Klick auf den Link, wird man weitergeleitet zur Bezahlseite.

#### Trickwording und Confirmshaming bei der Sitzplatzauswahl

Bleibt man bei der ursprünglichen Entscheidung und wählt keine Tarife oder Zusatzservices, erscheint nach der Auswahl der Sitzplätze eine Werbeseite für den Wizz Discount Club. Die gesamte Seite dient der Bewerbung des Abonnements, ohne dass klar benannt wird, dass es sich beim Discount Club um ein Abo-Modell handelt. Taktiken des „**Trick Wording**“ und „**Confirm Shaming**“ werden angewandt, um Kund:innen zum Abo Abschluss zu motivieren. Geworben wird mit Formulierungen wie „JETZT SPAREN“, „Jetzt kaufen und ein Jahr lang günstiger reisen“, „Als Mitglied kommen sie ein Jahr lang ab jetzt in den Genuss folgender Rabatte“. Die Rabatte betragen faktisch 10 Euro Rabatt auf den Flugpreis sowie 5 Euro Rabatt auf das Aufgabegepäck. Die Mitgliedschaft kostet 39,99 Euro pro Jahr. Stellt man die Kosten der Mitgliedschaft (39,99) der Ersparnis (15,00) gegenüber wird klar, dass mindestens drei Reisen via Wizz Air gebucht werden müssten, dass sich die Kosten für das Abo amortisieren (**Trick Wording, Confirm Shaming, Comparison Prevention, Hidden Costs**).

Die Gestaltung der Gepäcka Auswahl bei Wizz Air ist was Preisoptionen für sehr ähnliche Leistungen betrifft (10kg Aufgabegepäck versus 10kg Handgepäck) undurchsichtig (**Comparison Prevention**). Wählen die Kund:innen kein Tarifpaket, in

dem ein Hand- oder Aufgabegepäckstück inkludiert ist, können später Hand- sowie Aufgabegepäck hinzugebucht werden. Hier ergeben sich allerdings drastische Preisunterschiede. Bei einem Flug von Wien nach Tirana kostet beispielsweise ein 10kg Aufgabegepäck 12,95 EUR für den Hinflug und 10 EUR für den Rückflug – das ergibt einen insgesamten Aufpreis von 22,95 Euro für ein 10 kg Gepäcksstück. Wählt die Kund:in aber statt dem Aufgabegepäck die Option eines zusätzlichen 10kg Handgepäckstückes (gleiche Größe, gleiches Gewicht wie das Aufgabegepäck) kostet diese Option je 23,84 EUR pro Flug, was einen Gesamtaufpreis von 47,68 EUR ergibt. Der einzige Vorteil, der sich für die Reisenden ergibt, ist ein „Priority Boarding und Priority-Check-in“ wobei das Check-in nicht benötigt wird, da es sich um ein zusätzliches Handgepäck handelt, nicht um ein Aufgabegepäck. Die Preisgestaltung ist hier nicht intuitiv und verhindert somit ein für Kund:innen verständliches mental budgeting (**Comparison Prevention**).

Das Angebot einer kostenpflichtigen Sitzplatzauswahl wird im Falle von Wizz Air mit „Sitzplatzauswahl“ unmissverständlich formuliert. Erst später im Buchungsprozess wird ein Dark Pattern genutzt: Im weiteren Buchungsprozess erscheint jedenfalls nochmals eine Seite für die kostenpflichtige Sitzplatzauswahl. Hervorgehoben (ausgeklappt) ist dabei auf der rechten Seite ein Tab mit „von Wizz Air empfohlene Sitzplätze“. Trotz der zuvor getroffenen Entscheidung gegen das Zusatzservice, müssen User nochmals die Entscheidung treffen mit dem Hinweis: „Wenn Sie keine Sitzplätze auswählen, erfolgt die Zuteilung beim Checkin nach dem Zufallsprinzip“ (**Nagging**).

Bei Wizz Air waren keine gesonderten Dark Patterns bei der Buchung von Zusatzservices wie Versicherungen zu erkennen, es musste lediglich bestätigt werden, dass man ohne Reiseversicherung reisen will. Bestimmte Services wurden als „Empfehlung“ hervorgehoben, was auch als Werbemaßnahme beurteilt werden kann.

**Rechtliche Einordnung:** Durch die Verwendung von „**Nagging**“ bei der Auswahl des „Wizz Discount Clubs“ und „**Trickwording**“ und „**Confirmshaming**“ bei der Sitzplatzauswahl werden Verbraucher:innen tatsächlich oder voraussichtlich zu einer geschäftlichen Entscheidung veranlasst, die sie sonst nicht getroffen hätten. Es stellt sich daher die Frage, ob die Verwendung dieser Dark Patterns als aggressive Geschäftspraktik wegen unzulässiger Beeinflussung im Sinne von Art. 8 UGP-RL anzusehen ist.

## 4.4 Case Study „Opodo“

### 4.4.1 Dokumentation

**Dokumentationsgrundlage:** Screenshots des Buchungsprozesses von 18.04.2024 und Vorrecherchen im April 2023. Bitte zu beachten, dass der Buchungsprozess regelmäßig verändert wird und die Heranziehung der Beispiele insofern nur mit Hinweis auf Datum erfolgen sollte.

Die Flugbuchung bei Opodo verläuft analog zu den anderen Beispielen mit der Auswahl der gewünschten Flugdaten und des jeweiligen Flugs anhand der Uhrzeit. Zu diesem Zeitpunkt wird ein Preis angezeigt, es handelt sich jedoch ausschließlich um den „Prime-Preis“ – ein ermäßigter Preis, der mit einem Abo einhergeht. Es gibt keine Angabe zum Preis für den Flug ohne Abo.

The screenshot displays the Opodo search results for a flight from Wien to Barcelona. The search parameters are: Origin: Wien, Destination: Barcelona, Departure: Sa. 11/05, Return: Sa. 18/05, Passengers: 1. The results show a 'Genius Deal' for a round trip. The outbound flight (HINFLUG) is on Vueling, departing at 14:30 from Schwechat (VIE) to El Prat (BCN) at 16:55. The return flight (RÜCKFLUG) is on Wizz Air Malta, departing at 14:15 from El Prat (BCN) to Schwechat (VIE) at 16:45. The Prime price is €88, and the non-Prime price is €132. A 'Auswählen' button is present. The page also features a 'Preisalarm' section, a 'Hotel' advertisement, and a 'Feedback' button.

Abbildung 54: Opodo erste Ansicht des Preises, Prime-Deal. (Screenshot, 18.04.2024).

Neben den zu wählenden Flügen ist je ein Button, orange eingefärbt mit dem Text „Auswählen“. Es ist auf den ersten Blick nicht ersichtlich, dass es sich damit um eine Entscheidung für ein Abo handelt. Um auf den regulären Preis zu wechseln, braucht es einen Klick auf die links im Fenster zu sehende Ziffer. In grauer Schrift ist vermerkt „Nicht ermäßigter Tarif: EUR 132“. Der nicht ermäßigte Tarif, also der Flugpreis ohne Abo, ist in diesem Fall um 44 EUR teurer als der Flug inklusive Abo.

The screenshot shows the non-Prime price for the same flight search. The search criteria are: Origin: Barcelona, Destination: Wien. The non-Prime price is €132. A 'Auswählen' button is present. The page also features the Opodo Prime logo and a 'Prime entdecken' button.

Abbildung 55: Opodo nicht ermäßigter Tarif. (Screenshot, 18.04.2024).

Wählt ein User den Prime-Preis aus (Button „Auswählen“), geht es wie sonst weiter. Bis zum Ende kommt es zu keinem prägnanten Hinweis, dass ein Abo abgeschlossen wird und zu welchen Konditionen. Nur bei Aufschlüsselung der Kosten ist rechts vermerkt: „Gratis Probabo“ mit der Preisangabe 0 Euro.



The screenshot shows a price breakdown for Opodo Prime. It lists the following items and prices:

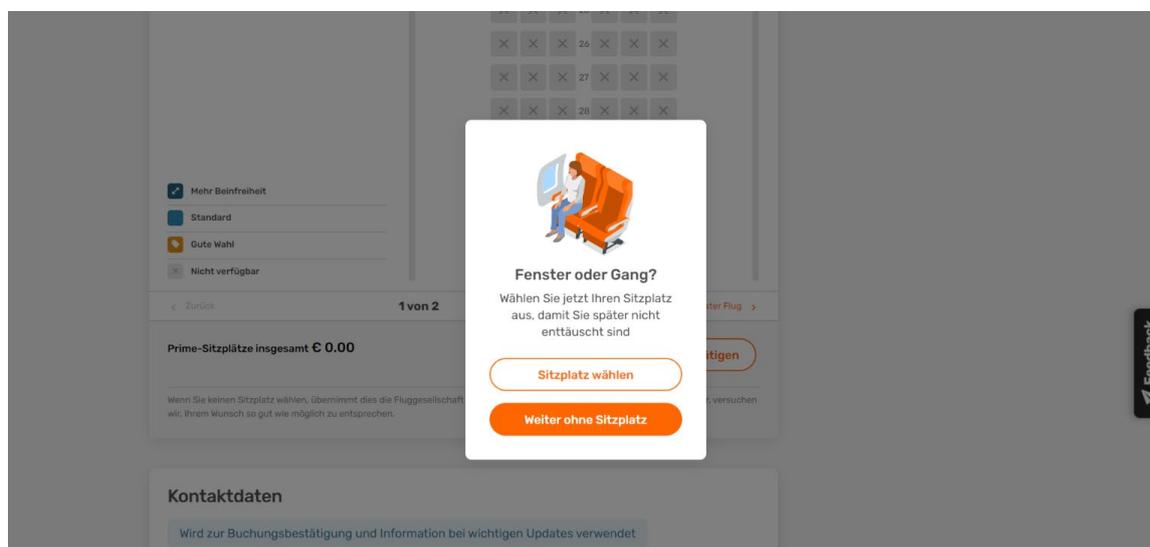
Item	Price
Reisen mit Basic-Support	
Normalpreis	€ 131.59
Prime-Rabatt	-€ 44.80
Gratis-Probabo	€ 0.00
<b>Gesamtpreis</b>	<b>€ 86.79</b>

Below the price breakdown, it states: "Steuern und Zahlungsentgelt inbegriffen". At the bottom, there is a green box with a checkmark and the text "Flexible Reisedaten hinzufügen" and an information icon.

Abbildung 56: Opodo Preisaufschlüsselung (Screenshot, 18.04.2024).

## Wahl des Sitzplatzes

Die Entscheidung keinen Sitzplatz extra gegen Gebühr auszuwählen, führt zu einem Pop-Up mit dem Titel „Fenster oder Gang?“ und zwei Buttons: „Weiter ohne Sitzplatz“ oder „Sitzplatz wählen“. Farblich hervorgehoben ist der Button „Weiter ohne Sitzplatz“.



The screenshot shows a pop-up window titled "Fenster oder Gang?" with the text: "Wählen Sie jetzt Ihren Sitzplatz aus, damit Sie später nicht enttäuscht sind". There are two buttons: "Sitzplatz wählen" and "Weiter ohne Sitzplatz". The "Weiter ohne Sitzplatz" button is highlighted in orange. In the background, a seat selection grid is visible with some seats marked 'X'. Below the pop-up, there are sections for "Kontaktdaten" and "Prime-Sitzplätze insgesamt € 0.00".

Abbildung 57: Opodo - Pop-Up "Weiter ohne Sitzplatz". (Screenshot, 18.04.2024).

## Kundenservice als Zusatzservice

Im Buchungsprozess werden User vor die Frage gestellt, welches Kundenservice-Paket sie in Anspruch nehmen wollen. Drei Tarife gibt es zur Auswahl: „Basic-Support“, „Standard-Support“ und „Premium-Support“. Wählt ein User den Basic-Support aus, folgt ein Pop-Up mit Infragestellung dieser Entscheidung: „Ist Basic-Support ausreichend?“.

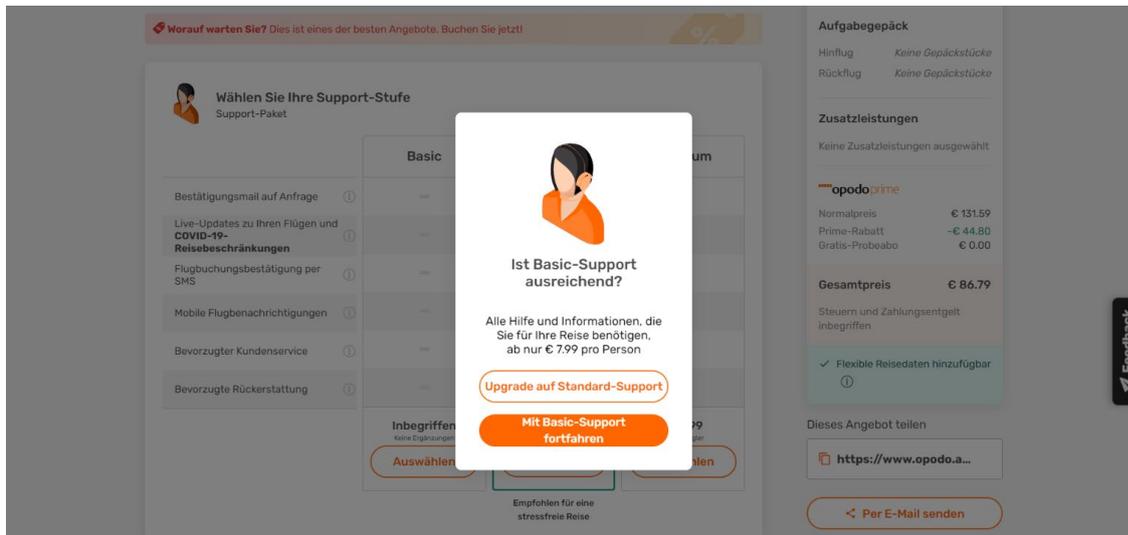


Abbildung 58: Opodo, Pop-Up mit Nachfrage zu Kundenservice (Screenshot, 18.04.2024).

## Opodo Prime

Erst nach diesen Schritten (Abfragen zu Zusatzservices wie Support, Versicherungen, etc.) erscheint vor der Bezahlung, bei einem Klick auf „Weiter“ die Info zu Prime Plus, dem Abo-Modell von Opodo.

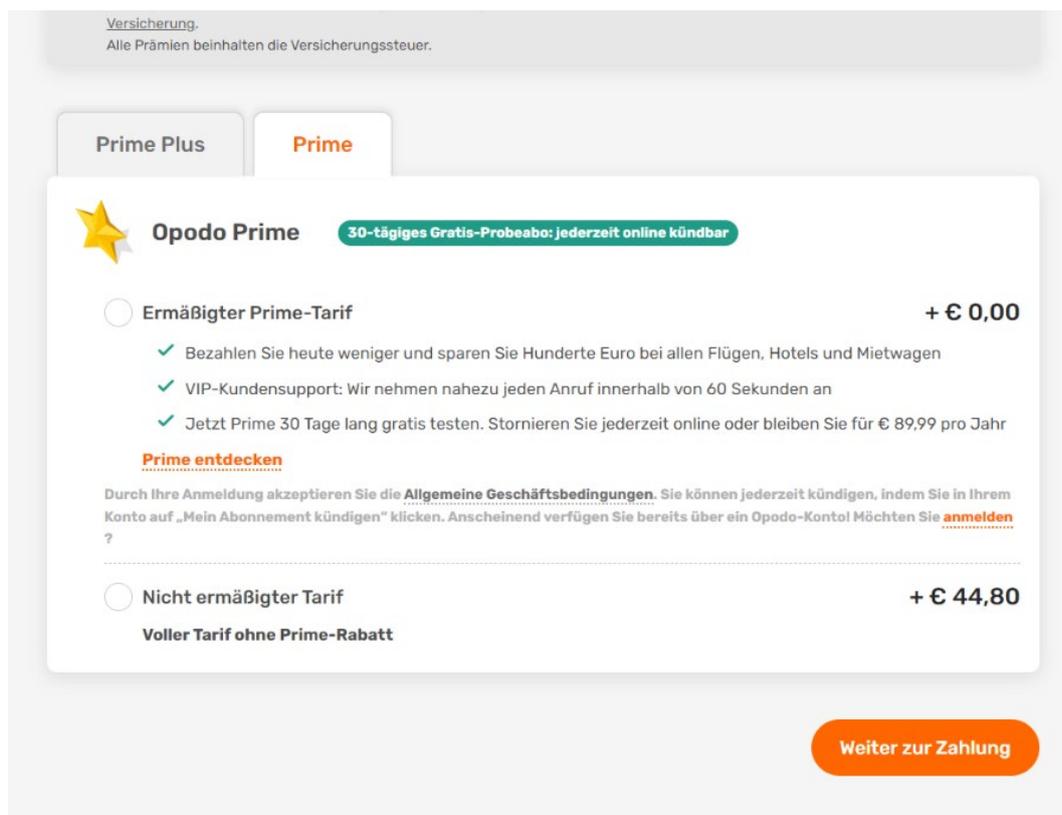


Abbildung 59: Opodo Prime Anzeige vor Kaufabschluss (Screenshot, 18.04.2024).

Hier muss nochmals das Prime-Abo ausgewählt, bzw. abgewählt werden. Gewählt werden kann zwischen zwei Abo-Modellen, neben Prime Plus auch Prime – beides vorerst kostenlos, nach einem Monat betragen die Kosten 89 bzw. 99 Euro pro Jahr.

Keines der Abos ist vorausgewählt, die Beschreibungen der Abos sind jedoch wertend. Formulierungen wie „ermäßigter Prime-Tarif“, „30-tägiges Gratis-Probeabo jederzeit online kündbar“, „Großartig! Sie erhalten ein 30-tägiges Gratis-Probeabo für Prime“, „+0,00“ stehen neutral bis negativen formulierten Beschreibungen gegenüber. Bei Nichtauswahl von Prime oder Prime Plus steht lediglich die Formulierung „Nicht ermäßigter Tarif“ und „+44,80“.

Schlüsselt man die Kosten auf, ist der nicht ermäßigte Tarif trotzdem günstiger, da die Abo-Kosten von 89 bzw. 99 Euro nicht als Teil des Gesamtpreises aufgeführt werden.

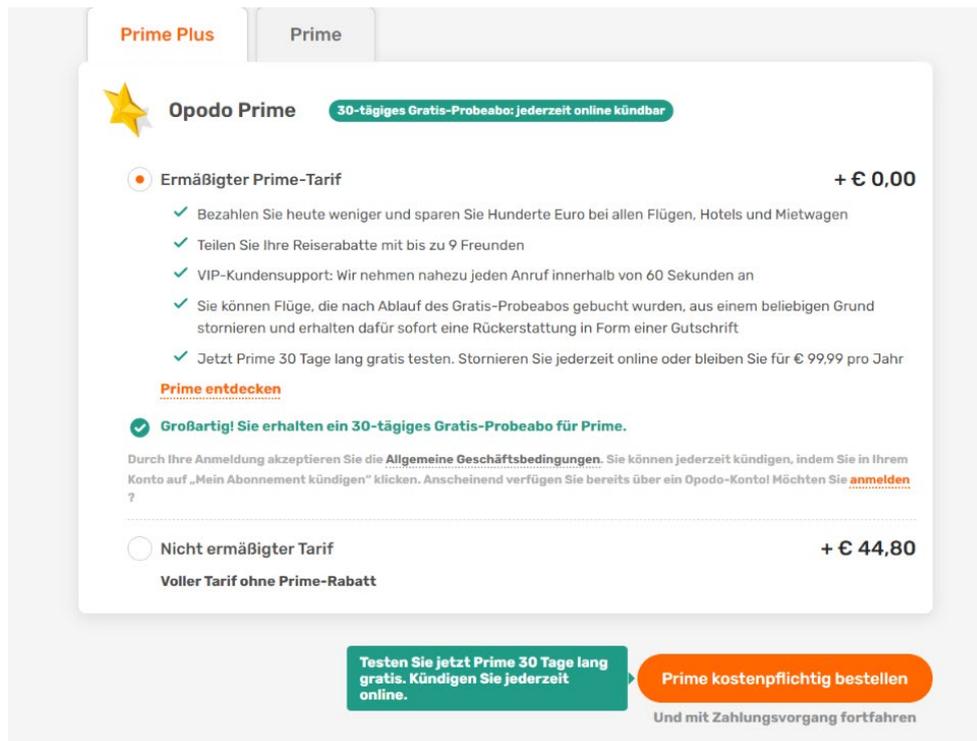


Abbildung 60: Opodo Prime Anzeige - Button-Lösung (Screenshot, 18.04.2024).

Bei der Auswahl des Abo-Modells, in diesem Beispiel „Prime Plus“, führt der Klick auf den orangen gefärbten Button mit der Aufschrift „Prime kostenpflichtig bestellen“ zur Bezahlung. Hier ist die Buttonlösung korrekt umgesetzt, obgleich auch der Gesamtpreis (Kosten inklusive Abo-Kosten) nicht aufgeführt wird.

Bei der Bezahlseite folgt eine weitere Entscheidung, bzw. Nachfrage. Hier wird zusätzlich ein flexibler Tarif angeboten, bei dem eine Datumsänderung der Flüge möglich ist. Es erscheinen zwei Buttons, links ein dezenter Button in weiß mit der Aufschrift „Jetzt kaufen“ mit dem ursprünglichen Preis. Rechts daneben ein oranger Button, der visuell auffälliger ist, mit der Aufschrift „Option für Datumsänderung“ und einem teureren Preis (104,75 EUR statt 86,79 EUR).

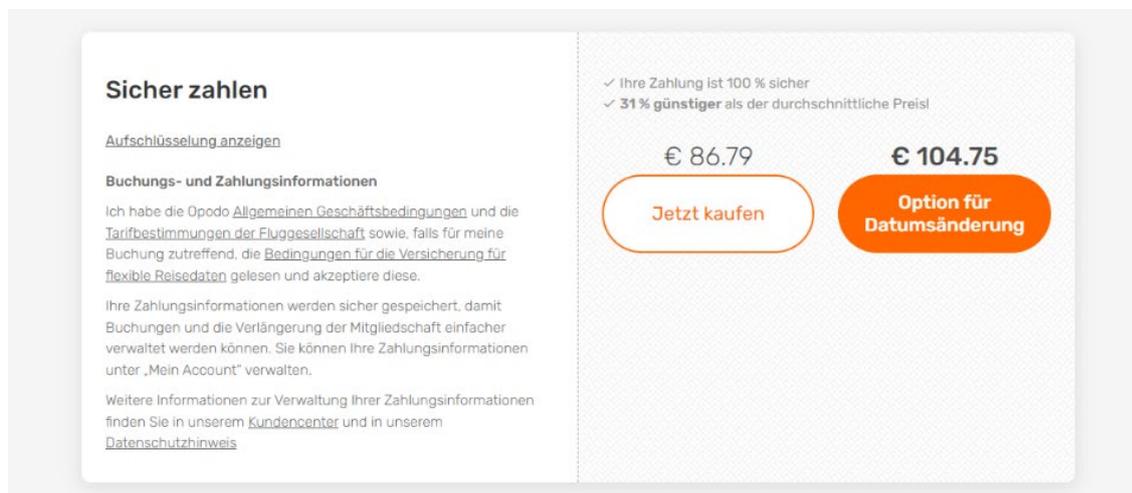


Abbildung 61: Zusatzleistung buchen, Option für Datumsänderung (Screenshot, 18.04.2024).

## 4.4.2 Analyse

Bei Opodo gestaltet sich die Buchung einer Flugreise ohne einen Abo-Abschluss schwierig. Verbraucherinnen und Verbrauchern werden diverse visuelle Stolpersteine gelegt (**Obstruction, Nagging**), um sie dazu zu bringen, Opodo Prime-Mitglieder (Opodo Abo-Modell) zu werden. Dabei auffällig ist insbesondere der „Auswählen“ Button, mit dem ein Flug ausgewählt wird und der zu den weiteren Schritten im Buchungsprozess führt. Klickt der User auf diesen Button, der auf den ersten Blick die einzige Möglichkeit darstellt mit dem Buchungsprozess fortzufahren, wird automatisch das Prime-Abo ausgewählt (**Hidden Subscription, Hidden Costs**).

Der Flugpreis, bzw. der Gesamtpreis der Reise wird dann in Folge nur inklusive des Prime-Rabatts angezeigt, die Aufschlüsselung des Gesamtpreises beinhaltet allerdings nicht die Kosten für das Abonnement (**Hidden Costs**). Dass man ein Abonnement abschließt, wird erst wieder im letzten Schritt vor dem Buchungsabschluss ersichtlich. Hier ist die letzte Option die Auswahl zwischen dem Prime Plus Abonnement oder dem Prime Abonnement. Bei dieser Auswahl sehen sich Kund:innen mit „**Confirm Shaming**“ und tendenziösen Formulierungen konfrontiert. Die Abo-Modelle werden blumig beschrieben mit Formulierungen wie „Ermäßigter Prime-Tarif“, „Bezahlen Sie heute weniger und sparen Sie Hunderte Euro“, „15-tägiges Gratis-Probearbeit: jederzeit online kündbar“. Auch bei der Auswahl der Abo-Modelle wird der Gesamtpreis der Reise, der immer am rechten Bildschirmrand sichtbar ist, nicht aktualisiert (**Hidden Costs**).

Die 84,99 Euro Kosten, die für das Abonnement (Prime Plus) anfallen, sollte es nicht nach 15 Tagen gekündigt werden, scheinen somit zu keinem Zeitpunkt auf (**Hidden Costs, Hidden Subscription**). Hierfür müssen Verbraucherinnen und Verbraucher das Kleingedruckte in der Beschreibung von Prime Plus und Prime Abo lesen. Wird die 14-tägige Kündigungsfrist nicht eingehalten (Kündigung muss 24 Stunden vor der Frist bei Opodo einlangen), wird das Abonnement für ein Jahr abgeschlossen und unter den für die Flugbuchung angegebenen Rechnungsdaten in Rechnung gestellt. Wird auch nach einem Jahr nicht gekündigt, verlängert sich das Abonnement auf unbestimmte Zeit (siehe Opodo AGB Geschäftsbedingungen Prime).<sup>43</sup>

Auch Opodo bedient sich an „**Confirm Shaming**“, bei der Nichtauswahl von kostenpflichtigen Sitzplätzen. Hier erscheint ein Pop-Up und unterbricht den Prozess der Buchung mit der suggestiven Frage: „Fenster oder Gang? Wählen Sie jetzt Ihren Sitzplatz aus, damit Sie später nicht enttäuscht sind.“ (**Confirm Shaming**). Darunter erscheinen zwei Buttons, in Weiß, orange umrandet „Sitzplatz wählen“ und nur in orange „Weiter ohne Sitzplatz“. Die Formulierung selbst suggeriert, dass bei „Weiter ohne Sitzplatz“ ein Flug gebucht wird, bei dem kein Sitzplatz garantiert ist, was nicht den Tatsachen entspricht (**Trick Wording**). Die grafische Gestaltung der Buttons steht im Gegensatz zu der Absicht, die hinter dieser Formulierung vermutet werden kann – denn visuell hervorgehoben wird die Option „Weiter ohne Sitzplatz“. Bucht man via Opodo eine Reise ohne Zusatzversicherung, weist auch hier ein Pop-Up darauf hin, dass keine Versicherung ausgewählt wurde (**Nagging**). Zudem kommt in dem Pop-Up Text „**Confirm Shaming**“ zum Einsatz, mit suggestiven Formulierungen, die Reisende

---

<sup>43</sup> Opodo Prime AGB, <https://www.opodo.at/prime/agb-uebersicht/>

dazu bringen sollen eine Versicherung abzuschließen: „Gehen Sie keine unnötigen Risiken ein! Versichern Sie Ihre Reise!“

**Rechtliche Einschätzung:** Das Vorliegen eines besonderen Preisvorteils ist in diesem Fall davon abhängig, dass die Verbraucher:innen ein Abonnement abschließen. Dies wird den Verbraucher:innen jedoch bis zum letzten Schritt vor dem Buchungsabschluss nicht eindeutig kommuniziert. Die verwendeten Gestaltungstechniken sind somit manipulativ, da sie geeignet sind, die Verbraucher:innen über den tatsächlichen Preis der Buchung und das Vorhandensein eines Preisvorteils zu täuschen. Die Gestaltung und Verwendung von Dark Patterns könnte daher als irreführende Geschäftspraxis im Sinne von Art. 7 Abs. 2 UGP-RL angesehen werden. Zudem können die emotionalen Botschaften können Verbraucher:innen zu Geschäftsentscheidungen veranlassen, die sie ansonsten nicht getroffen hätten. Bei der Nutzung solcher Gestaltungstechniken müssen die Betreiber:innen daher sicherstellen, dass die Verbraucher:innen gleichzeitig darüber informiert werden, welche Risiken sie ohne Versicherung übernehmen müssten bzw. welche konkreten Vorteile sie durch den Abschluss einer Versicherung hätten. Auch bei der Auswahl des Sitzplatzes muss die Option „Weiter ohne Sitzplatz“ so gestaltet sein, dass die Verbraucher:innen eine klare Vorstellung von den Konsequenzen ihrer Wahl bekommen. Ohne diese Angaben ist es für die Verbraucher:innen nicht möglich, eine informierte geschäftliche Entscheidung zu treffen. Aus diesem Grund könnte die verwendete Gestaltung als irreführende Geschäftspraxis im Sinne von Art. 7 Abs. 1 UGP-RL angesehen werden. Hierzu gibt es auch eine rezente Entscheidung des OGH, der nach einer Klage der Arbeiterkammern entschieden hat, die kostenpflichtige Opodo-Prime-Mitgliedschaft bei Buchung einer Reise sei ungültig. Konsument:innen können demnach Geld für die Mitgliedschaft zurückfordern.<sup>44</sup>

---

<sup>44</sup> (Arbeiterkammer, 2024)

## 5 Registrierungsprozesse auf Social Media

Social Media Plattformen haben eine zentrale Rolle als Vermittler des digitalen Erlebens von Usern. Längst sind sie mehr als Apps, um mit anderen in Kontakt zu treten. Ihre Recommender Systeme schaffen maßgeschneidert personalisierte Erfahrungen; sie prägen, welche Nachrichten User lesen, aber auch welche Konsumententscheidungen sie treffen; dafür nutzen sie die Daten ihrer User. Wo soll hierbei der Hebel der Regulierung ansetzen, dass eben diese Art der datenbasierten, personalisierten Erfahrung, die ja auch den Reiz von Social Media ausmacht, nicht ausgemerzt wird?

Ein wichtiger Hebel in der Stärkung von Userrechten sind Datenschutzeinstellungen. Madejski et al. haben festgestellt, dass die wahrgenommenen Datenschutzeinstellungen von Usern häufig nicht mit den tatsächlich vorgenommenen Einstellungen übereinstimmen.<sup>45</sup> Hinzu kommt, dass die ersten Datenschutzeinstellungen, die Nutzer:innen bei der Anmeldung auf Social-Media-Plattformen vornehmen, oft entscheidend sind für das Schutzniveau ihrer persönlichen Daten.<sup>46</sup> Es gibt jedoch Bedenken hinsichtlich der Wirksamkeit dieser Einstellungen, da die Nutzer:innen ihre Auswirkungen möglicherweise nicht vollständig verstehen.<sup>47</sup> Es gilt daher als wichtig, dass Social-Media-Plattformen klare und benutzerfreundliche Datenschutzeinstellungen bereitstellen, um sicherzustellen, dass die Nutzer:innen fundierte Entscheidungen über ihre Privatsphäre treffen können. Oft werden die Einstellungen, einmal getätigt auch im Laufe des Bestehens des User-Kontos nicht mehr geändert – die Einstellungen bei Registrierung eines neuen Accounts stellen somit einen starken Hebel dar, der die zukünftige User-Experience maßgeblich hinsichtlich Privatsphäre und Personalisierung beeinflusst.<sup>48</sup>

Mit dem Inkrafttreten von diversen Regulierungen (DSA, DMA, DSGVO) wurde hier der Rechtsrahmen gezogen. Nach dem **Digital Markets Act (DMA)** wird ein Unternehmen als „**Torwächter**“ bezeichnet, wenn es einen erheblichen Einfluss auf den Binnenmarkt hat, einen zentralen Plattformdienst bereitstellt, der gewerblichen Nutzer:innen als wichtiges Zugangstor zu Endnutzern dient, und hinsichtlich seiner Tätigkeiten eine gefestigte und dauerhafte Position innehat oder absehbar ist, dass es eine solche Position in naher Zukunft erlangen wird.<sup>49</sup> Am 6. September 2023 ernannte die Europäische Kommission sechs Torwächter im Rahmen des Digital Markets Act: Alphabet, Amazon, Apple, ByteDance, Meta und Microsoft. Es wurden insgesamt 22 zentrale Plattformdienste benannt, die von diesen Torwächtern angeboten werden. Soziale Netzwerke wie TikTok, Facebook, Instagram, YouTube und LinkedIn zählen dazu.<sup>50</sup>

---

<sup>45</sup> (Madejski et al., 2012)

<sup>46</sup> (Litt, 2013)

<sup>47</sup> (Burkell et al., 2013)

<sup>48</sup> (Princi & Krämer, 2020; Sangeeta, 2015)

<sup>49</sup> Artikel 3 Absatz 1 Digital Markets Act

<sup>50</sup> (Europäische Kommission, 2024a), siehe auch: [https://digital-markets-act.ec.europa.eu/gatekeepers\\_en](https://digital-markets-act.ec.europa.eu/gatekeepers_en)

Torwächter verarbeiten personenbezogene Daten von Endnutzer:innen zum Zweck der Bereitstellung von Online-Werbung. Darüber hinaus stellen Dritte, die die Torwächter-Plattform nutzen, den Torwächtern auch personenbezogene Daten ihrer eigenen Endnutzer:innen zur Verfügung, um die Plattformdienste nutzen zu können. Dies verschafft den Torwächtern einen potenziellen Marktvorteil, da ihr Geschäftsmodell datenbasiert ist. Daher verlangt der DMA von den Torwächtern, dass sie die Einwilligung der Endnutzer:innen gemäß der DSGVO einholen, um personenbezogene Daten für ihre datengestützten Geschäftspraktiken zu verarbeiten, und schränkt die Rechtsgrundlagen ein, auf die sie sich dabei stützen können. Folglich sollten Torwächter den Endnutzer:innen die Möglichkeit geben, frei zu entscheiden, ob sie solchen Datenverarbeitungen und Opt-in-Praktiken zustimmen, indem sie eine weniger personalisierte, aber gleichwertige Alternative anbieten, ohne die Nutzung des Kerndienstes der Plattform oder bestimmter Funktionen von der Einwilligung der Endnutzer:innen abhängig zu machen. Hierzu könnte neben der Einwilligung nach dem DSA auch Artikel 6 Absatz 1 Buchstaben c, d und e der DSGVO und nicht Artikel 6 Absatz 1 Buchstaben b und f der DSGVO als Rechtsgrundlage für die Verarbeitung verwendet werden.

Wenn die Einwilligung der Endnutzer:innen für die Datenverarbeitung erforderlich ist, muss die Einwilligung die Bedingungen der DSGVO erfüllen.<sup>51</sup> Torwächter müssen die Endnutzer:innen über die Folgen einer Nichteinwilligung informieren. Damit die Einwilligung freiwillig bleibt, müssen sie eine weniger personalisierte, aber gleichwertige Alternative anbieten, ohne die Nutzung des Kerndienstes der Plattform oder bestimmter Funktionen von der Einwilligung der Endnutzer:innen abhängig zu machen.<sup>52</sup>

Der **Digital Services Act (DSA)** konzentriert sich stärker auf die Regulierung von Online-Inhalten. Die Regulierung gilt bereits für die „sehr großen Online-Plattformen“ (VLOPs). LinkedIn, Facebook, Instagram, TikTok, YouTube, Snapchat und X; diese werden im Rahmen des DSA als VLOPs bezeichnet.<sup>53</sup> Es gibt einige Überschneidungen zwischen Unternehmen, die unter dem DMA als Torwächter und unter dem DSA als VLOPs bezeichnet werden. Unternehmen, die beiden Gesetzen unterliegen, müssen beide Vorschriften einhalten. Nach Art. 28 DSA dürfen Anbieter von Online-Plattformen auf ihrer Schnittstelle keine Werbung anzeigen, die auf Profiling im Sinne der DSGVO unter Verwendung personenbezogener Daten der Endnutzer:innen beruht, wenn sie hinreichende Gewissheit haben, dass die betreffende Person minderjährig ist. Darüber hinaus ist Werbung auf der Grundlage von „Profiling“ von Daten der „besonderen Kategorie“ im Sinne der DSGVO nach dem DSA unzulässig.<sup>54</sup> Mit dem DSA werden Transparenzanforderungen für auf allen Online-Plattformen angezeigte Werbung sowie zusätzliche Transparenzanforderungen und Anforderungen zur Durchführung einer Risikobewertung für potenzielle systemische Risiken für VLOPs eingeführt. Die VLOPs sind nach dem DSA auch verpflichtet, ein Archiv für den gesamten Zeitraum, in dem sie Werbung anzeigen, und für ein Jahr nach der letzten Anzeige der Werbung auf ihren Online-

---

<sup>51</sup> Erwägungsgrund 36 Digital Markets Act

<sup>52</sup> Erwägungsgrund 37 Digital Markets Act

<sup>53</sup> (Europäische Kommission, 2024c)

<sup>54</sup> Artikel 26 Absatz 3 Digital Services Act

Schnittstellen zu erstellen und öffentlich zugänglich zu machen. Dieses Archiv enthält Informationen wie den Inhalt der Werbung, die natürliche oder juristische Person, in deren Namen die Werbung geschaltet wurde, den Zeitraum, in dem die Werbung geschaltet wurde, ob die Werbung für eine oder mehrere bestimmte Nutzergruppen bestimmt war und die Gesamtzahl der erreichten Nutzer:innen.<sup>55</sup>

Die zwei folgenden Case Studies überprüfen angesichts der vorliegenden, vorab kurz skizzierten rechtlichen Rahmenbedingungen, wie User bei der Registrierung eines neuen User-Accounts über ihre Rechte informiert werden – für den Fall eines 16-jährigen Users. Hinsichtlich Personalisierung gab es Nachbesserungen im vergangenen Jahr und so können User aktuell teilweise bestimmen, in welcher Intensität Personalisierung stattfindet und auf welche persönlichen Daten für Werbezwecke zugegriffen werden darf. Doch angesichts der notwendigen Verhandlung zwischen Usern, die zum einen ermächtigt werden wollen, ihre persönlichen Informationen möglichst genau verwalten zu können und zum anderen Interesse daran haben, eine möglichst für sie individuell relevante User-Experience zu erfahren – mit den Interessen der Plattformen sowie der auf diesen tätigen Werbetreibenden an Daten – stellt sich die Frage: Wie werden diese Prozesse gestaltet und lassen sich darin Dark Patterns finden? Dem wurde für TikTok und Instagram auf den Grund gegangen: Wird trotz Verbot personalisierte Werbung ausgegeben? Sind die angelegten Profile automatisch öffentlich oder privat? Werden Dark Patterns eingesetzt, um hier Entscheidungen von Usern in unternehmerische Interessen zu lenken?

---

<sup>55</sup> Artikel 39 Digital Services Act

## 5.1 Case Study „TikTok“

### 5.1.1 Dokumentation

**Dokumentationsgrundlage:** Screenshots vom Registrierungsprozess auf TikTok (Datum: 02 April 2024). Es wurde dafür ein iPhone genutzt und bei der Angabe des Alters auf Minderjährigkeit des Users geachtet (Geburtsdatum 01.03.2008).

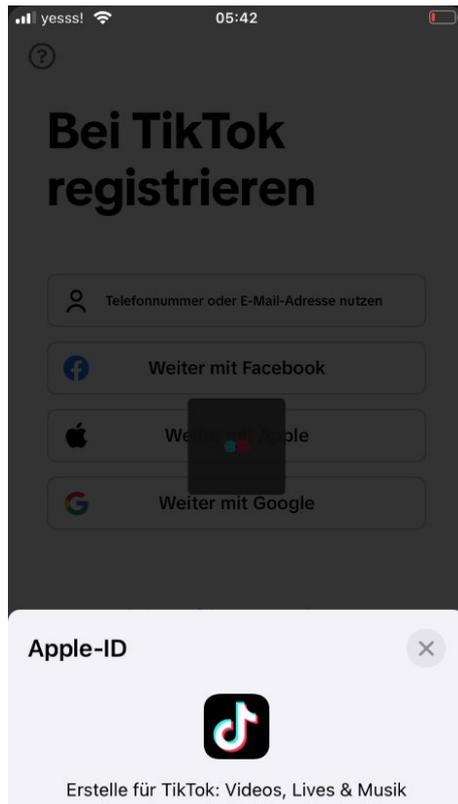


Abbildung 62: Anmeldung bei TikTok mit Apple ID (Screenshot, 02.04.2024).

Nach Download der TikTok-App aus dem Apple App-Store folgt die Registrierung. Dafür kann über die Verwendung der eigenen Telefonnummer oder eine E-Mail-Adresse ein Konto angelegt werden. Zudem gibt es die Option sich via Google, Facebook (Meta) oder mithilfe der Apple-ID zu registrieren. Da die Apple-ID auf dem Gerät schon angelegt war und hier schon die Information hinterlegt wurde, dass die Nutzerin des Smartphones 16 Jahre alt ist, wurde die Option „mit Apple-ID registrieren“ gewählt.

Nach der Registrierung wurde von TikTok darüber informiert, dass die Inhalte auf Grundlage des eigenen Verhaltens (Inhalte, die man ansieht) personalisiert werden (Abb. 63.).

Im nächsten Schritt, wurde gefragt, ob User personalisierte Werbung oder allgemeine Werbung angezeigt bekommen wollen. Beide Auswahlmöglichkeiten waren gleich gestaltet, eine Wertung „möglicherweise weniger relevant“ war im Wording zu finden (Abb. 64.).

📶 yesss! 📶

🔒 05:45



## Nach oben wischen

Videos werden für dich personalisiert auf Grundlage der Inhalte, die du anschaust, denen



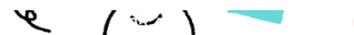
Anschauen

Abbildung 63: Info zu Personalisierung, TikTok (Screenshot, 02.04.2024).

Hierbei handelt es sich um ein Opt-In, das in dieser Form für eine minderjährige Person (simulierte Nutzerin unter 18 Jahren) nicht möglich sein sollte, da personalisierte Werbung für Minderjährige laut DSA in der Europäischen Union verboten ist.

**Personalisierte Werbung:** Die angezeigten Anzeigen werden auf der Grundlage deiner Aktivitäten auf TikTok personalisiert. Wir verwenden auch Daten von Drittanbietern, aber nur, wenn du die Nachverfolgung auf deinem Gerät aktiviert hast.

**Allgemeine Anzeigen:** Die dir angezeigte Werbung ist möglicherweise weniger relevant für dich.



## Wähle, wie Werbung angezeigt wird

Erlaube uns, deine Daten zu verwenden, um dir relevante Werbung zu zeigen, damit TikTok kostenlos bleibt. **Mehr erfahren.** In unserer **Datenschutzerklärung** kannst du auch lesen, wie wir deine Daten nutzen und schützen.

### Personalisierte Werbung

Die angezeigten Anzeigen werden auf der Grundlage deiner Aktivitäten auf TikTok personalisiert. Wir verwenden auch Daten von Drittanbietern, aber nur, wenn du die Nachverfolgung auf deinem Gerät aktiviert hast.

Auswählen

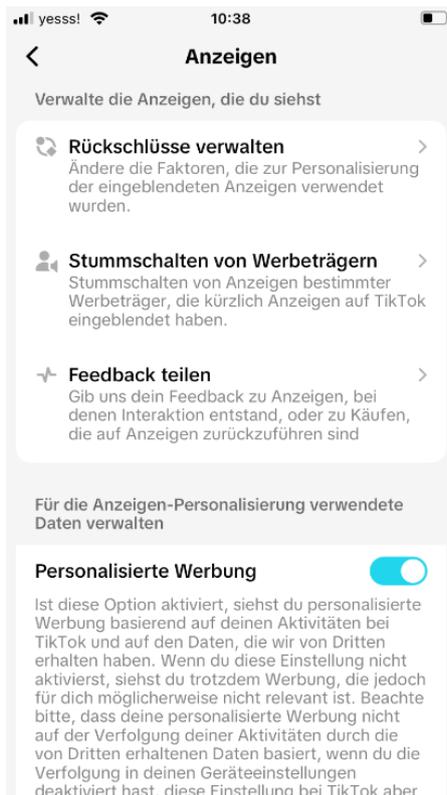
### Allgemeine Anzeigen

Die dir angezeigte Werbung ist möglicherweise weniger relevant für dich.

Auswählen

Du kannst dies in deinen „Anzeigen“-Einstellungen jederzeit aktualisieren.

Abbildung 64: "Wähle wie Werbung angezeigt wird", TikTok (Screenshot, 02.04.2024).



Auch bei nochmaliger Überprüfung: Die Werbeanzeigen auf TikTok werden auch unter Angabe eines Alters unter 18 Jahren personalisiert.

Diese Einstellungen können unter „Einstellungen“> „Anzeigen“ verändert werden.

TikTok fragt bei jedem Öffnen der App danach, auf die Kontakte der Nutzer:in zugreifen zu dürfen: „TikTok möchte auf deine Kontakte zugreifen. Synchronisiere deine Kontakte, um Leute, die du kennst, ganz einfach bei TikTok zu finden. Deine Kontakte werden nur genutzt, damit du dich mit Freund\*innen verbinden kannst.“

Abbildung 65: Einstellungen zu Anzeigen auf TikTok, User-Profil Anna (Screenshot, 02.04.2024).

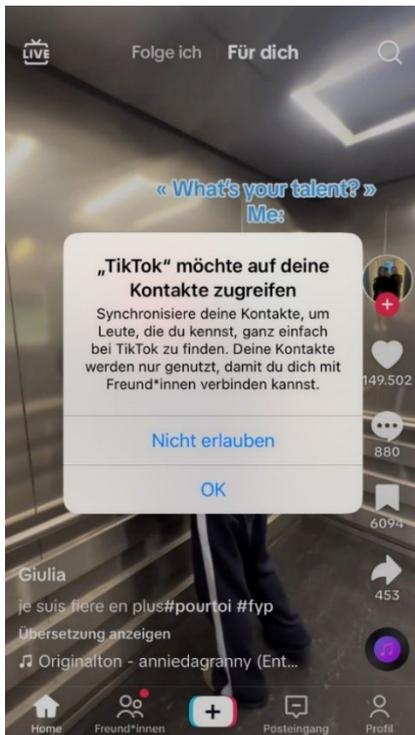


Abbildung 66: Pop-Up auf TikTok (Screenshot, 02.04.2024).



Abbildung 67: Pop-Up auf TikTok (Screenshot, 02.04.2024).

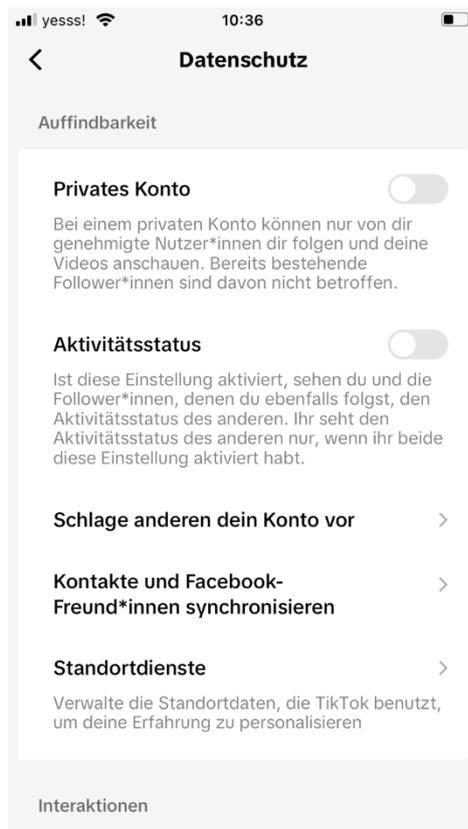


Abbildung 68 Privatsphäre  
Einstellungen TikTok – Privates  
Konto (Screenshot, 02.04.2024).

Wird die Testnutzerin Anna in einem anderen Video getagged (markiert) ist das von allen Accounts aus möglich, egal ob Anna mit dem Profil das sie markiert hat verbunden ist oder nicht. Standardisiert sind auch „Stitches“ (zitieren eines Videos bzw. Video-Antwort auf ein zuvor gepostetes Video) möglich, egal ob Anna mit dem Profil verbunden ist oder nicht.

Die Datenschutzeinstellungen bei TikTok sind standardisiert offen eingestellt.

Standardisiert, ist jedes neue TikTok-Konto öffentlich. Will man, auch als minderjährige Person, wie die Testpersona Anna, ein privates Profil, muss dies manuell umgestellt werden.

Ebenfalls wird das eigene Profil anderen Kontakten automatisiert vorgeschlagen. So ist das TikTok-Profil leicht für andere auffindbar.

Das eigene Profil wird so den eigenen Kontakten, Facebook-Freund:innen sowie Personen, die Links öffnen oder dir senden, vorgeschlagen.

Standardmäßig können alle Kommentare unter den eigenen oder unter fremden Videos von allen gesehen werden, bzw. alle Nutzer:innen von TikTok können ohne Einschränkung unter jedes Video kommentieren.

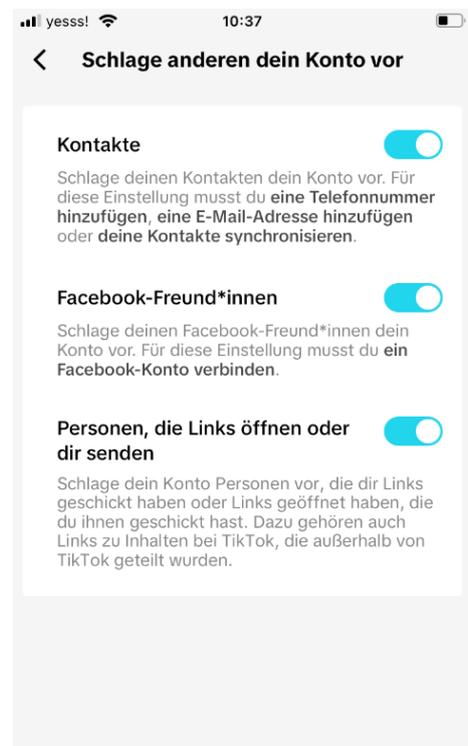


Abbildung 69: Schlage anderen dein Konto  
vor, TikTok (Screenshot, 02.04.2024).

## 5.1.2 Analyse

Die Analyse des dokumentierten Registrierungsprozesses auf TikTok zeigt mehrere problematische Aspekte, die sowohl Dark Patterns als auch mögliche Verstöße im Sinne des Digital Services Act (DSA) darstellen. Insbesondere kritisch ist der dokumentierte Umgang mit minderjährigen Nutzer:innen, da diese eine besonders schutzbedürftige Gruppe darstellen.

Beim Registrierungsprozess bietet TikTok verschiedene Methoden an, die auch zur Altersverifikation genutzt werden können, darunter die Nutzung der Apple-ID, bei der das Alter bereits hinterlegt ist. In diesem Fall wurde eine minderjährige Person (Geburtsdatum 01.03.2008, User-Name Anna) registriert. TikTok scheint das Alter zwar zu erfassen, es werden jedoch keine ausreichend spezifischen Schutzmaßnahmen implementiert. Ein wesentlicher Punkt ist hierbei die Darstellung der Optionen für personalisierte Werbung. Die EU-Vorschriften, insbesondere der DSA, verbieten personalisierte Werbung für Minderjährige. TikTok bietet jedoch die Möglichkeit an, zwischen personalisierter und allgemeiner Werbung zu wählen, auch für die Testpersona Anna, die ihr Alter mit 16 Jahren angegeben hat (Abb. 64, Abb. 65). Obwohl die Formulierung der Auswahlmöglichkeiten keine offensichtlichen Dark Patterns enthält, stellt die Existenz dieser Wahlmöglichkeit für Minderjährige einen klaren Verstoß gegen den DSA dar. Personalisierte Werbung sollte für Minderjährige keine Option sein.

Zudem setzt TikTok standardmäßig auf sehr offene Datenschutzeinstellungen: Das betrifft standardisiert öffentliche Profile, die automatisierte Synchronisation von Kontakten und automatische Profilvorschläge (Abb. 68, Abb. 69). Neue Konten sind standardmäßig öffentlich, was insbesondere für minderjährige Nutzer:innen problematisch ist (**Preselection**). Die Sichtbarkeit muss manuell auf privat umgestellt werden, was viele Minderjährige möglicherweise nicht tun. Die Standardeinstellungen, die die meisten Nutzer:innen beibehalten und nicht manuell, bzw. nachträglich verändern, geben sehr viel vom Nutzerverhalten der:des Einzelnen preis. Bei einem zweiten Versuch wurde ein Konto mit einer 13jährigen Testperson angelegt. Hier bot TikTok eine Reihe an Aufklärungsvideos an, die sich die Nutzer:innen ansehen hätten können. Außerdem war das Profil der 13-jährigen Persona automatisch auf privat gestellt, alle weiteren Share-Funktionen wie das Vorschlagen des Profils waren standardisiert ausgeschaltet.

TikTok fordert bei jedem Öffnen der App den Zugriff auf die Kontakte (Abb. 66, Abb. 67). Diese Praxis könnte als Dark Pattern angesehen werden, da sie Benutzer dazu verleitet, mehr persönliche Daten preiszugeben als notwendig (**Privacy Zuckering, Nagging, Obstruction**). Auch werden Profile automatisiert anderen Kontakten und Facebook-Freund:innen vorgeschlagen, was die Sichtbarkeit und Auffindbarkeit des eigenen Profils erheblich erhöht.

Die Standardkonfiguration erlaubt uneingeschränkte Interaktionen mit dem eigenen Profil und den Inhalten der Nutzer:innen, einschließlich Kommentare und Markierungen durch unbekannte Personen. Diese Standardeinstellungen sind besonders besorgniserregend für minderjährige Nutzer:innen, da sie deren Sicherheit und Privatsphäre gefährden können.

Zudem zeigen die Standardeinstellungen bei TikTok eine klare Tendenz zur Offenheit, was gegen den Grundsatz der Datenminimierung verstößt. Minderjährige Nutzer:innen sind sich oft der Reichweite ihrer Datenfreigabe und der damit verbundenen Risiken nicht bewusst. Diese Praxis kann als manipulative Gestaltung angesehen werden, die Nutzer:innen dazu bringt, mehr persönliche Informationen preiszugeben, als sie beabsichtigen (**Privacy Zuckering**).

Der Registrierungsprozess und die standardisierten Einstellungen bei TikTok zeigen deutliche Hinweise auf den Einsatz von Dark Patterns, insbesondere durch intransparente und offene Standardeinstellungen sowie das Angebot personalisierter Werbung für Minderjährige. Diese Praktiken stehen im Widerspruch zu den Anforderungen des DSA und der DSGVO, die den Schutz der Privatsphäre und der Daten von Nutzer:innen, insbesondere Minderjährigen, sicherstellen sollen.

## 5.2 Case Study „Instagram“

### 5.2.1 Dokumentation

**Dokumentationsgrundlage:** Dokumentiert wurde der Instagram-Registrierungsprozess (02.04.2024) – es wurde dafür ein iPhone genutzt und bei der Angabe des Alters auf Minderjährigkeit geachtet (Geburtsdatum 01.03.2008).

Nach Download und erstmaligen Öffnen der Instagram-App, wird zunächst nach der Zustimmung für Drittanbieter-Cookies gefragt. „Die Verwendung von Cookies durch Instagram erlauben?“ – hier spezifiziert Meta, dass Inhalte und Werbung über Cookies „(sofern wir dir Werbung zeigen)“ angeboten und personalisiert werden.

Die Gestaltung der Buttons ist farblich suggestiv: der „Alle Cookies erlauben“-Button ist in einem hellen und visuell auffälligeren Blau gestaltet, der „Optionale Cookies ablehnen“-Button in unauffälligem Hellgrau. Den Nutzungsbedingungen von Instagram muss zur Verwendung der App zugestimmt werden.

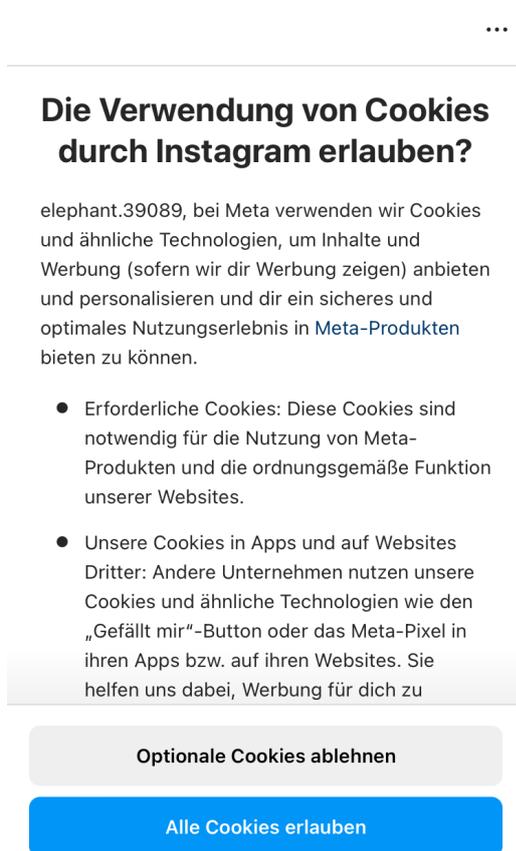


Abbildung 70: Verwendung von Cookies auf Instagram (Screenshot, 02.04.2024).

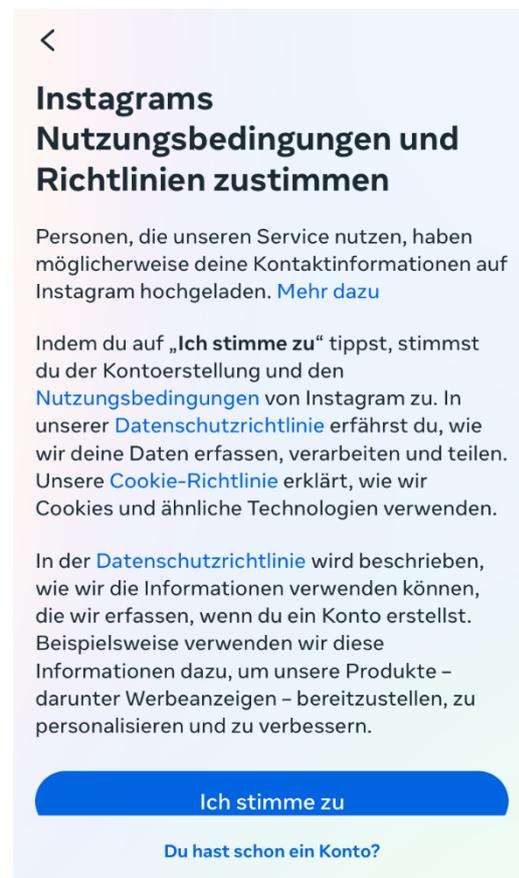


Abbildung 71: Nutzungsbedingungen von Instagram (Screenshot, 02.04.2024).

## Instagram macht mit Freunden noch mehr Spaß. Lass deine Kontakte synchronisieren, um sie zu finden.

Wenn du uns Zugriff auf deine Kontakte gestattest, können wir dir einen besseren Service bieten.

+ Wir verwenden deine Kontakte, um dir dabei zu helfen, dich mit Menschen zu verbinden, die du kennst, und dir Dinge zu empfehlen, die dir wichtig sind.

↻ Deine Kontakte werden dann fortlaufend synchronisiert und sicher auf unseren Servern gespeichert.

⚙ In den Einstellungen kannst du die Synchronisierung jederzeit deaktivieren. [Weitere Infos](#)

Weiter

Abbildung 72: Anfrage Kontakte synchronisieren Instagram (Screenshot, 02.04.2024).

Auch bei der Synchronisierung der Kontakte greift Instagram auf suggestive Formulierungen zurück. „Instagram macht mit Freunden noch mehr Spaß. Lass deine Kontakte synchronisieren, um sie zu finden.“ Danach fragt die App um den Zugang zu den auf dem Smartphone gespeicherten Kontakten.

Die Buttons, um den Zugriff auf die eigenen Kontakte zu bestätigen oder abzulehnen, sind neutral gestaltet. Die Option „nicht erlauben“ wird als erstes angeführt.

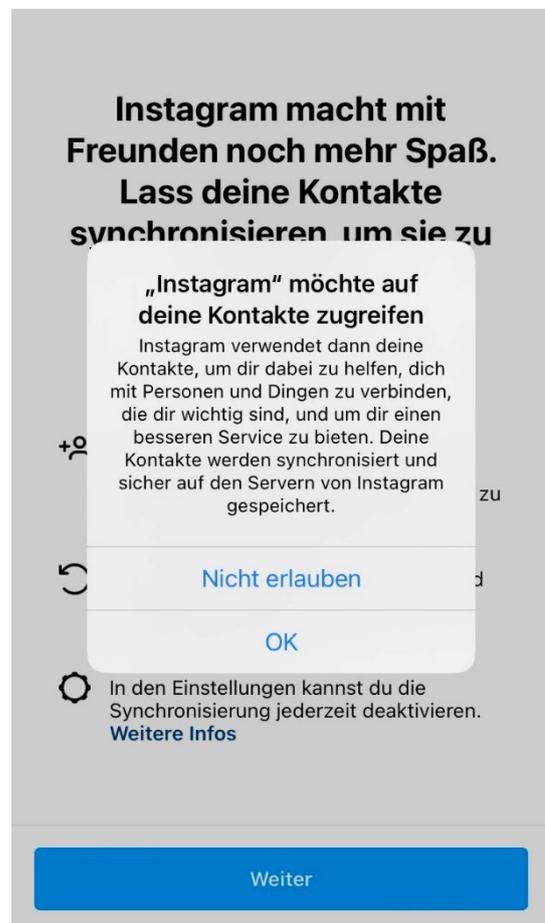


Abbildung 73: Zugriff auf Kontakte Instagram Pop-Up (Screenshot, 02.04.2024).

## Konto-Privatsphäre

Bestimme, wer sehen kann, was du teilst. Du kannst dies jederzeit in den Einstellungen wieder ändern.

- Privat**  
Nur Konten, die du bestätigst, können deine Fotos und Videos sehen.
- 
- Öffentlich**  
Jeder kann deine Fotos und Videos sehen.

Weiter

Abbildung 74: Konto Privatsphäre-Einstellungen Instagram (Screenshot, 02.04.2024).

Im nächsten Schritt fragt die Instagram-App danach, Benachrichtigungen zuzulassen. Hierbei werden verschiedene Designs verwendet, unter dem Titel „Benachrichtigungen aktivieren“, ist der „Aktivieren“-Button in blau gehalten, der Link, um die Aktivierung zu überspringen ist kein Button, sondern ein darunter liegender, nicht farblich hinterlegter Link. Das Opt-Out ist somit nicht als Button gestaltet.

Der nächste Schritt in der Registrierung ist die Angabe des Konto-Typs. Hier müssen User entscheiden, ob sie ein öffentliches oder privates Social Media Profil bevorzugen. Beide Optionen werden als gleichwertig dargestellt, bei der Registrierung vorausgewählt ist das private Instagram-Profil.

Die Auswahl zwischen privatem und öffentlichem Profil wird nüchtern erklärt: „Privat – nur Konten, die du bestätigst, können deine Fotos und Videos sehen“ vs. „Öffentlich – Jeder kann deine Fotos und Videos sehen.“

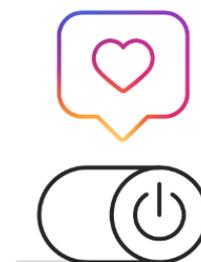
📶 yesss! 📶

01:59



## Benachrichtigungen aktivieren

Bleib immer auf dem Laufenden darüber, wer dir folgt oder deine Beiträge kommentiert und mit „Gefällt mir“ markiert.



Aktivieren

Überspringen

Abbildung 75: Benachrichtigungen aktivieren, Instagram (Screenshot, 02.04.2024).

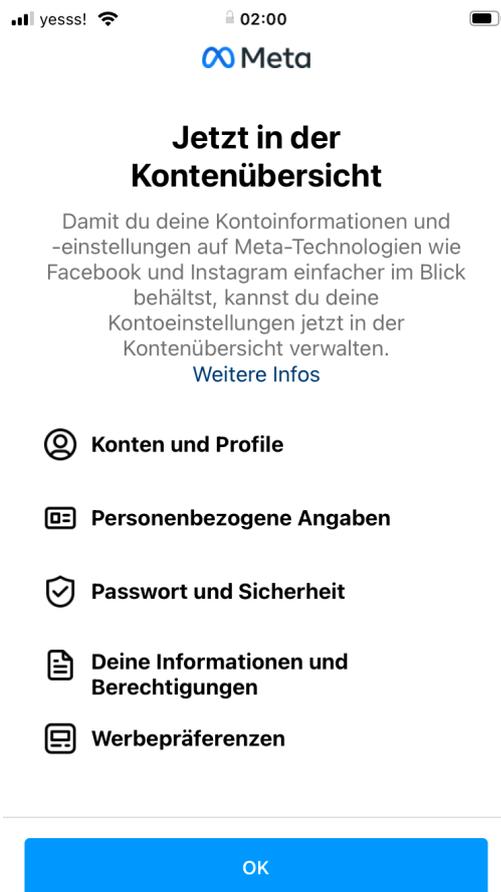


Abbildung 76: Einstellungen Instagram (Screenshot, 02.04.2024).

Zuletzt folgen weitere Informationen im Sinne einer Kontenübersicht, es können weitere Einstellungen und Änderungen der getätigten Einstellungen vorgenommen werden. So können bspw. personenbezogene Angaben, Passwörter, Sicherheitseinstellungen aber auch Werbepräferenzen verändert werden.

Bei Klick auf die Werbepräferenzen wird im Fall unserer Testperson Anna klar, dass diese nicht verändert oder speziell eingestellt werden können, da Anna unter 18 Jahre alt ist.

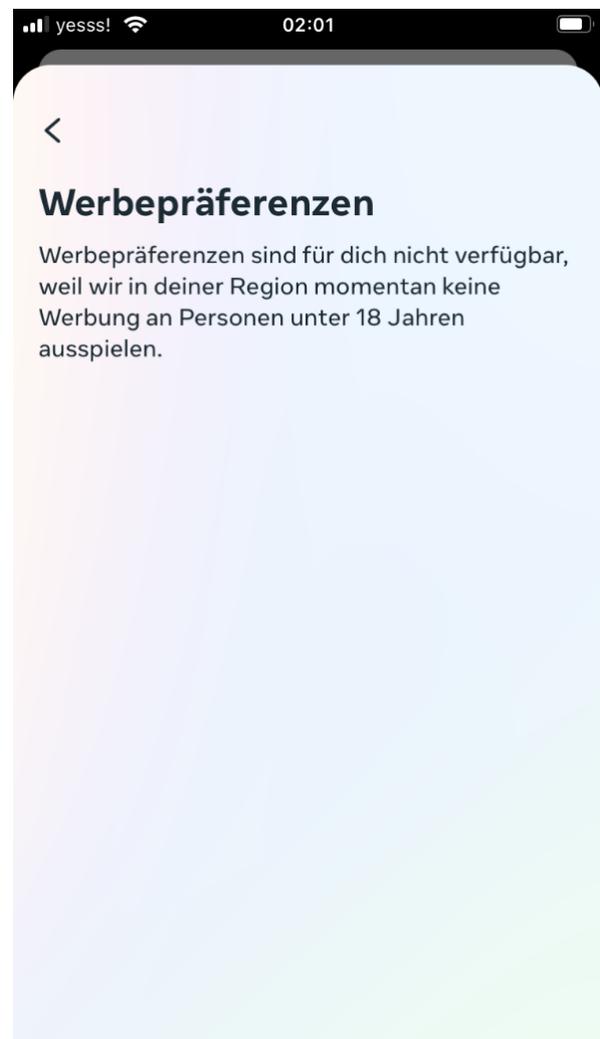


Abbildung 77: Werbepräferenzen Instagram (Screenshot, 02.04.2024).

## 5.2.2 Analyse

Der dokumentierte Registrierungsprozess auf Instagram unterscheidet sich zu dem bei TikTok erheblich. Obwohl Meta auf einige suggestive Designelemente setzt, werden Grundsätze, wie keine personalisierte Werbung für Minderjährige ernst genommen.

Zu Beginn des Registrierungsprozesses wird der User um die Zustimmung zur Verwendung von Drittanbieter-Cookies gebeten. Die Gestaltung der Auswahlmöglichkeiten ist hierbei suggestiv: Der Button „Alle Cookies erlauben“ ist in einem auffälligen Blau gestaltet, während der Button „Optionale Cookies ablehnen“ in einem weniger auffälligen Hellgrau gehalten ist. Diese farbliche Differenzierung ist ein klassisches Dark Pattern, das darauf abzielt, Nutzer:innen zur Zustimmung zu allen Cookies zu verleiten (**Deliberate Misdirection, Tagging**).

Ebenso verhält es sich bei der Zustimmung zu den Nutzungsbedingungen. Diese ist zwar obligatorisch, jedoch wünschenswert wäre größere Transparenz und Klarheit, was genau diese Bedingungen umfassen und welche Datenverarbeitungspraktiken damit einhergehen. Insbesondere für minderjährige Nutzer:innen.

Bei der Frage zur Synchronisierung von Kontakten verwendet Instagram wiederum suggestive Formulierungen, um Nutzer:innen zur Synchronisierung ihrer Kontakte zu bewegen: „Instagram macht mit Freunden noch mehr Spaß. Lass deine Kontakte synchronisieren, um sie zu finden.“ (**Confirmshaming, Emotional Stirring, Privacy Zuckering**) Diese Formulierung zielt darauf ab, Nutzer:innen zu überzeugen, den Zugriff auf ihre Kontakte zu gewähren. Die Buttons zur Bestätigung oder Ablehnung des Zugriffs sind neutral gestaltet, wobei „nicht erlauben“ als erstes angeführt wird. Dies mindert den Eindruck eines Dark Patterns in diesem Schritt, jedoch bleibt die suggestive Formulierung problematisch.

Positiv hervorzuheben ist, dass Instagram eine klare Auswahl zwischen einem öffentlichen und einem privaten Profil bietet. Beide Optionen werden gleichwertig dargestellt, wobei das private Profil vorausgewählt ist. Dies ist positiv zu bewerten, da es den Schutz der Privatsphäre fördert. Die Unterschiede zwischen den beiden Konto-Typen werden eindeutig erklärt, was zur Transparenz beiträgt und Nutzer:innen hilft, informierte Entscheidungen zu treffen.

Die Anfrage, Benachrichtigungen zuzulassen, ist wiederum suggestiv gestaltet. Der „Aktivieren“ Button ist in Blau gehalten, während der Link zum Überspringen der Aktivierung nicht farblich hervorgehoben und nur als Text-Link unter dem Button dargestellt ist. Dies ist ein weiteres Beispiel für ein Dark Pattern, das darauf abzielt, Nutzer:innen zur Aktivierung von Benachrichtigungen zu verleiten (**Deliberate Misdirection, Nagging**).

Nach der Registrierung werden Nutzer:innen über weitere Einstellungsoptionen informiert, darunter personenbezogene Angaben, Passwörter, Sicherheitseinstellungen und Werbepräferenzen. Im Fall der minderjährigen Testperson Anna können die Werbepräferenzen nicht verändert oder speziell eingestellt werden, was den Vorgaben des DSA entspricht, der personalisierte Werbung für Minderjährige verbietet. Dies zeigt, dass Instagram in diesem Punkt die gesetzlichen Anforderungen erfüllt.

Der Registrierungsprozess auf Instagram zeigt sowohl positive als auch negative Aspekte im Hinblick auf Dark Patterns und die Einhaltung des DSA: Die klare Darstellung der Konto-Typen und die standardmäßige Voreinstellung auf ein privates Profil sind im Sinne des Datenschutzes und der Sicherheit positiv zu bewerten. Zudem entspricht die Einschränkung der Werbepräferenzen für Minderjährige den gesetzlichen Vorgaben.

Die Verwendung suggestiver Formulierungen und visueller Hervorhebungen bei der Zustimmung zu Cookies und Benachrichtigungen sind Beispiele für Dark Patterns, die darauf abzielen, Nutzer:innen zu Entscheidungen zu bewegen, die möglicherweise nicht in ihrem besten Interesse sind. Dies steht im Widerspruch zu den Prinzipien der Transparenz und des informierten Einwilligens.

### 5.3 Exkurs: Consent or Pay-Modell von Meta

Das Bundeskartellamt hat Facebook im Jahr 2019 untersagt, Nutzerdaten aus verschiedenen Quellen zusammenzuführen. In seiner Pressemitteilung teilte das Bundeskartellamt mit, dass die Nutzer:innen das soziale Netzwerk nach den Nutzungsbedingungen von Facebook nur unter der Voraussetzung nutzen könnten, dass Facebook auch außerhalb der Facebook-Seite im Internet oder in Smartphone-Apps Daten über die Nutzer:innen sammelt und dem Facebook-Nutzerkonto zuordnet.<sup>56</sup> Diese Verarbeitung erfolgte mit der Absicht, den Nutzer:innen gezielte Werbung zeigen zu können. In diesem Fall ging Meta gegen das Bundeskartellamt vor und der EuGH entschied schließlich, dass die Einwilligung in eine Datenverarbeitung, insbesondere wenn sie als Voraussetzung für die Nutzung eines Dienstes verlangt wird, nur dann rechtmäßig ist, wenn sie freiwillig erfolgt.<sup>57</sup>

Aufgrund der marktbeherrschenden Stellung von Meta kann die in diesem Fall eingeholte Einwilligung nicht als freiwillig angesehen werden. Damit reagierte das Unternehmen auf das EuGH-Urteil vom Juli 2023 mit der Umsetzung eines "Consent or Pay"-Modells. Bei diesem Modell haben die Nutzer:innen die Wahl, entweder dem Tracking für gezielte Werbung zuzustimmen und die Dienste weiterhin kostenlos zu nutzen oder eine jährliche Gebühr zu zahlen und nicht getrackt zu werden.<sup>58</sup>

Am 17. Januar 2024 ersuchte die niederländische Aufsichtsbehörde, die auch im Namen der norwegischen Aufsichtsbehörde und der deutschen (Hamburger) Aufsichtsbehörde handelte, den EDSA um eine Stellungnahme zu „Consent or Pay“-Modellen. Das Ersuchen betrifft die Umstände, unter denen große Online-Plattformen, die eine große Zahl von Nutzer:innen im Europäischen Wirtschaftsraum anziehen, "Consent or Pay"-Modelle zur Datenverarbeitung für verhaltensbezogene Werbung anwenden können, die dem Erfordernis einer wirksamen und insbesondere freiwilligen Einwilligung genügen. Die ersuchenden Behörden wiesen ferner darauf

---

<sup>56</sup> (Bundeskartellamt, 2019)

<sup>57</sup> EuGH C-252/21 Meta gegen Bundeskartellamt

<sup>58</sup> (NOYB, 2024) <https://noyb.eu/de/pay-or-okay-explained-why-more-and-more-websites-make-you-pay-your-privacy>

hin, dass diese Frage unter Berücksichtigung des Urteils des EuGH in der Rechtssache C-252/21 zu beantworten sei.

In seiner Stellungnahme definierte der EDSA „Consent or Pay“-Modelle als Modelle, bei denen ein für die Verarbeitung Verantwortlicher den betroffenen Personen die Wahl zwischen mindestens zwei Optionen für den Zugang zu einem von dem für die Verarbeitung Verantwortlichen angebotenen Online-Dienst bietet. Die betroffene Person kann in die Verarbeitung ihrer personenbezogenen Daten für einen bestimmten Zweck einwilligen oder sich dafür entscheiden, eine Gebühr zu zahlen und Zugang zu dem Online-Dienst zu erhalten, ohne dass ihre personenbezogenen Daten für diesen Zweck verarbeitet werden.<sup>59</sup> Die Stellungnahme der EDSA konzentriert sich auf Modelle, bei denen die Einwilligung zur Verarbeitung personenbezogener Daten für Zwecke der verhaltensbasierten Werbung gegeben wird. In seiner Stellungnahme stellte der EDSA fest, dass "Consent or Pay"-Modelle grundsätzlich nicht den Anforderungen der DSGVO entsprechen. Die Wahl zwischen der Einwilligung in die Nutzung der eigenen Daten zu Werbezwecken und der Möglichkeit, für den Zugang zu einem Dienst zu zahlen, stellt nach Ansicht des EDSA keine ausreichende Wahlfreiheit dar und widerspricht damit dem Grundsatz der freien Einwilligung. Diese Stellungnahme ermutigt die großen Plattformen, alternative Modelle zu entwickeln. Die Industrie sollte andere Möglichkeiten der Monetarisierung in Betracht ziehen und eine dritte Option für die Nutzer:innen anbieten, die weiterhin kostenlos ist, aber z.B. eine andere Form der Werbung beinhaltet, bei der weniger (oder keine) personenbezogenen Daten verarbeitet werden.

---

<sup>59</sup> (European Data Protection Board, 2024) Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Adopted on 17 April 2024

## 6 Tools

Im Rahmen des Projekts PCS wurden Tools zur Detektion, Blockierung und Dokumentation von Dark Patterns gesammelt und analysiert. Ziel war es, einen Überblick über die bereits verfügbaren Tools zu erhalten, sowie auch deren Funktionsweise und Entwicklungspotential zu ermitteln. Ziel des Projektes war es zu evaluieren, inwiefern geeignete Tools bereits am Markt verfügbar sind, die ein Monitoring aus Sicht von Verbraucherschutz erleichtern können.

Im Folgenden werden jene Tools dokumentiert, die auch Konsument:innen empfohlen werden können, um Dark Patterns auf Websites teilweise zu entgehen.

### 6.1 Verhinderung von Tracking & Ausblendung von Cookie Bannern

Die folgenden Tools verhindern das Setzen von Tracking-Cookies, Third-Party-Cookies (Cookies von Drittanbietern) und anderen Personalisierungsversuchen und schützen insofern auch vor personalisierten Dark Patterns.

<b>Name</b>	<b>CookieBlock</b>
	Kostenlos
<b>Ziel</b>	Automatisierte Ablehnung von Cookies
<b>Beschreibung</b>	Das von der ETH Zürich entwickelte Tool nutzt maschinelles Lernen und blockiert alle Cookies auf den besuchten Seiten. Die Anwender:innen können auswählen, welche Cookies sie immer blockieren wollen - somit umgeht die Browser-Erweiterung das individuelle Anklicken von Cookie-Bannern auf jeder neu aufgerufenen Website.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://chrome.google.com/webstore/detail/cookieblock/fbhiolckidkciamgobkocokpelckgnnl?hl=de">https://chrome.google.com/webstore/detail/cookieblock/fbhiolckidkciamgobkocokpelckgnnl?hl=de</a>

<b>Name</b>	<b>Ghostery</b>
	Kostenlose Version verfügbar
<b>Ziel</b>	Personalisiertes Tracking verhindern
<b>Beschreibung</b>	Das Tool erkennt, wenn Websites versuchen, Cookies von Drittanbietern zu installieren und verhindert dies. Das Tracking bei Suchanfragen in Suchmaschinen kann gestoppt werden ( <a href="https://whotracks.me/">https://whotracks.me/</a> ) und es gibt auch eine Suchmaschine ohne Tracking. ( <a href="https://glowstery.com/">https://glowstery.com/</a> ) Die Anwendungen von Ghostery bieten somit einen erweiterten Tracking-Schutz als z.B. Cookie Block.
<b>Anwendung</b>	Browser-Erweiterung, Website, Suchmaschine
<b>Link</b>	<a href="http://www.ghostery.com">www.ghostery.com</a>

<b>Name</b>	<b>Privacy Badger</b>
	Kostenlos
<b>Ziel</b>	Personalisiertes Tracking verhindern
<b>Beschreibung</b>	Privacy Badger ist eine von EFF (Electronic Frontier Foundation) entwickelte Browser-Erweiterung. Der „algorithmic tracker blocker“ Privacy Badger arbeitet nicht mit Blocklisten, sondern erkennt Tracker automatisch und lernt diese zu blockieren.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://privacybadger.org/">https://privacybadger.org/</a>

<b>Name</b>	<b>Tracking Exposed</b>
	Kostenlos
<b>Ziel</b>	Personalisiertes Tracking auf diversen Sozialen Netzwerken als Datenstruktur sichtbar machen.
<b>Beschreibung</b>	Das Tool verhindert Tracking nicht, sondern macht es für die Nutzer:innen sichtbar. Dies geschieht durch das Sammeln und Visualisieren von Tracking-Daten der User und die Darstellung der gesammelten Informationen. Die Daten werden für die Forschungsprojekte von Tracking Exposed verwendet. Der Dienst ist für TikTok, YouTube, Facebook, Pornhub verfügbar.
<b>Anwendung</b>	Browser-Erweiterung, Website-Service
<b>Link</b>	<a href="https://tracking.exposed/">https://tracking.exposed/</a>

<b>Name</b>	<b>I Don't Care About Cookies</b>
	Kostenlos
<b>Ziel</b>	Verhinderung der „Klickarbeit“ zur Ablehnung oder Annahme von Cookie-Bannern.
<b>Beschreibung</b>	Diese Browser-Erweiterung entfernt Cookie-Warnungen von nahezu allen Websites und erspart somit unnötige Klicks. In der Regel blockiert oder verbirgt sie einfach die Cookie-Hinweise. Sollte die Funktion der Website es erfordern, akzeptiert die Erweiterung automatisch die Cookies-Richtlinie. Dabei kann sie entweder alle Arten von Cookies zulassen oder nur die unbedingt notwendigen – abhängig davon, was sich technisch einfacher umsetzen lässt. Wichtig zu beachten ist, dass diese Erweiterung keine Cookies löscht.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://www.i-dont-care-about-cookies.eu/de">https://www.i-dont-care-about-cookies.eu/de</a>

<b>Name</b>	<b>Nervenschoner</b>
	Kostenlos
<b>Ziel</b>	Blockierung von Pop-Ups, darunter Cookie-Banner
<b>Beschreibung</b>	Um die Unterbrechungen durch Cookie-Banner einzudämmen, bietet die Verbraucherzentrale Bayern die Browser-Erweiterung "Nervenschoner" an, welche die meisten Banner erfolgreich unterdrückt.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://www.verbraucherzentrale-bayern.de/nervenschoner">https://www.verbraucherzentrale-bayern.de/nervenschoner</a>

<b>Name</b>	<b>Super Agent</b>
	Kostenlos
<b>Ziel</b>	Blockierung von Cookie-Bannern
<b>Beschreibung</b>	Der Super Agent füllt Cookie-Einwilligungsformulare basierend auf User-Präferenzen aus. User entscheiden, ob und wie sie getracked werden möchten, und stellen sicher, dass ihre Optionen automatisch und ohne Aufwand angewendet werden. Optionale Cookies werden in drei Kategorien eingeteilt: Werbung, Funktion und Leistung. Cookies, die keiner dieser Kategorien eindeutig zuzuordnen sind, werden automatisch abgelehnt.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://chrome.google.com/webstore/detail/super-agent-automatic-coo/neooppigbkahgfdhpbhcccgpimeaafi">https://chrome.google.com/webstore/detail/super-agent-automatic-coo/neooppigbkahgfdhpbhcccgpimeaafi</a>

<b>Name</b>	<b>Hush</b>
	Kostenlos
<b>Ziel</b>	Cookie-Blocker
<b>Beschreibung</b>	Blockiert die Aufforderung zur Annahme von Cookies und invasivem Tracking in Safari auf Mac, iPhone und iPad.
<b>Anwendung</b>	App für iOS (Apple Geräte)
<b>Link</b>	<a href="https://oblador.github.io/hush/">https://oblador.github.io/hush/</a>

<b>Name</b>	<b>Datacentrics</b>
	Kostenlose Testversion
<b>Ziel</b>	Datenschutz-Audit für Websites
<b>Beschreibung</b>	Erfüllt eine Website die Datenschutzerfordernungen? Mit dem Datenschutz-Audit überprüfen User die Nutzung und Risikostufe Ihrer Website hinsichtlich Erstanbieter- und Drittanbieter-Cookies sowie Drittanbieter-Anfragen.
<b>Anwendung</b>	Website, Webservice
<b>Link</b>	<a href="https://usercentrics.com/de/data-privacy-audit/">https://usercentrics.com/de/data-privacy-audit/</a>

## 6.2 Ausblendung von Werbung und Empfehlungen

<b>Name</b>	<b>AdAnalyst</b>
	Kostenlos
<b>Ziel</b>	Sichtbarmachung der Personalisierung von Werbung auf Facebook
<b>Beschreibung</b>	Das Tool ist für Facebook und zeigt Konsument:innen an, welche Werbeanzeigen auf sie zugeschnitten sind, wer bzw. welche Gruppen die gleiche Werbung sehen, und welche Information das Unternehmen über einen hat. Damit hofft das Entwicklungsteam auf mehr Transparenz bei Facebook-Werbung. Es handelt sich um das Ergebnis von Forschungsprojekten. In seiner Funktionalität ist es außerhalb von den USA noch eingeschränkt.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://adanalyst.mpi-sws.org">https://adanalyst.mpi-sws.org</a>

<b>Name</b>	<b>AdAway</b>
	Kostenlos
<b>Ziel</b>	Werbeblocker für Android
<b>Beschreibung</b>	AdAway ist ein quelloffener Werbeblocker für Android, der die Hosts-Datei verwendet. Er kann nicht in offiziellen Stores heruntergeladen werden.
<b>Anwendung</b>	App
<b>Link</b>	<a href="https://adaway.org/">https://adaway.org/</a>

<b>Name</b>	<b>YouChoose.ai</b>
	Kostenlos
<b>Ziel</b>	Ausblendung von Werbung und algorithmischen Empfehlungen
<b>Beschreibung</b>	Das Tool blendet empfohlene Videos aus, die auf YouTube neben dem gerade abgespielten Video angezeigt werden. Ziel ist es, das Empfehlungssystem von YouTube zu umgehen.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="http://www.youchoose.ai">www.youchoose.ai</a>

<b>Name</b>	<b>Consent Blocker</b>
	Kostenlos
<b>Ziel</b>	Blockierung von Google Consent (Ad-Blocker)
<b>Beschreibung</b>	Ein Werbeblocker für Einwilligungen, früher bekannt als Google Consent. Blockiert Einwilligungsdialoge, indem er entweder die Einwilligungs-Cookies/Speicherelemente einfügt oder Anfragen an die Einwilligungsmanagement-Plattform blockiert.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://addons.mozilla.org/de/firefox/addon/google-consent/">https://addons.mozilla.org/de/firefox/addon/google-consent/</a>

<b>Name</b>	<b>Blockada</b>
	Kostenlos
<b>Ziel</b>	Blockierung von Werbung
<b>Beschreibung</b>	Blockada ist ein Werbeblocker und die Datenschutz-App für Android und iOS. Sie wird von der Open-Source-Community unterstützt und aktiv weiterentwickelt.
<b>Anwendung</b>	App
<b>Link</b>	<a href="https://blokada.org">https://blokada.org</a>

## 6.3 Ausblendung & Highlighting von Dark Patterns

<b>Name</b>	<b>Dark Patterns Recognition (Insite)</b>
	Kostenlos
<b>Ziel</b>	Highlighting von Dark Patterns auf Onlineshops
<b>Beschreibung</b>	Erkennung und Hervorhebung von Dark Patterns auf Shopping-Websites, mit einer Erklärung zu den erkannten Dark Patterns als Pop-up.
<b>Anwendung</b>	GitHub Repository / Erweiterung
<b>Link</b>	<a href="https://github.com/NicholasTung/dark-patterns-recognition#dark-patterns-recognition-insite">https://github.com/NicholasTung/dark-patterns-recognition#dark-patterns-recognition-insite</a>

<b>Name</b>	<b>Dark Patterns</b>
	Kostenlos
<b>Ziel</b>	Highlighting von Dark Patterns die zuvor gemeldet wurden
<b>Beschreibung</b>	Diese Browser-Erweiterung ist noch in der Beta-Phase und verfügt bislang nur über begrenzte Daten. Ziel ist, dass mit wachsender Datenbank mehr Dark Patterns gekennzeichnet werden, die zuvor von Usern gemeldet worden sind.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://chromewebstore.google.com/detail/dark-patterns/mmodaifhembdmcmgcmmlfceflekmkoc?pli=1">https://chromewebstore.google.com/detail/dark-patterns/mmodaifhembdmcmgcmmlfceflekmkoc?pli=1</a>

<b>Name</b>	<b>AppGenie / Grease Droid</b>
	Kostenlos
<b>Ziel</b>	Werkzeugkasten zur Veränderung von Apps
<b>Beschreibung</b>	Ein community-gesteuertes Framework zur Modifikation von Apps, mit dem Ziel Dark Patterns zu entfernen. Es soll auch Nicht-Experten ermöglichen, Dark Patterns in Apps selektiv zu deaktivieren. Das Framework ist nur für Android Apps anwendbar und braucht erhebliches technisches Vorwissen, um umsetzbar zu sein.
<b>Anwendung</b>	GitHub Repository
<b>Link</b>	<a href="https://github.com/OxfordHCC/greasedroid">https://github.com/OxfordHCC/greasedroid</a> <a href="https://arxiv.org/abs/2102.11819">https://arxiv.org/abs/2102.11819</a>

<b>Name</b>	<b>DapDe Pattern Highlighter</b>
	Kostenlos
<b>Ziel</b>	Highlighten von Dark Patterns
<b>Beschreibung</b>	Dieses im Rahmen eines Forschungsprojekts entwickelte Tool funktioniert ähnlich wie ein Werbeblocker, hebt jedoch Dark Patterns hervor, anstatt sie zu blockieren. Ziel ist es, zur Bewusstseinsbildung beizutragen. Zusätzlich sind Informationen über diese Dark Patterns verlinkt.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://github.com/Dapde/Pattern-Highlighter">https://github.com/Dapde/Pattern-Highlighter</a>

<b>Name</b>	<b>Trick Question Detection</b>
	Kostenlos
<b>Ziel</b>	Erkennung von Fangfragen
<b>Beschreibung</b>	Algorithmus zur Erkennung des Dark Patterns der "Fangfrage" auf Websites. Dieses Projekt wurde im Rahmen eines Bachelor-Abschlusses entwickelt und ist veröffentlicht für Entwickler:innen.
<b>Anwendung</b>	GitHub, Code
<b>Link</b>	<a href="https://github.com/xrenegade100/trick-question-detection">https://github.com/xrenegade100/trick-question-detection</a>

## 6.4 Erkennung und Dokumentation von Verstößen

<b>Name</b>	<b>Crawler: Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites</b>
	Kostenlos
<b>Ziel</b>	Webscraping & Dokumentation von Dark Patterns
<b>Beschreibung</b>	Veröffentlichung der Daten und des Codes für das Forschungspapier "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites".
<b>Anwendung</b>	Webscraping-Tool / GitHub
<b>Link</b>	<a href="https://github.com/aruneshmathur/dark-patterns">https://github.com/aruneshmathur/dark-patterns</a>

<b>Name</b>	<b>Cookie Dialog Compliance (formerly Dark Patterns Project)</b>
	Kostenlos
<b>Ziel</b>	Registrierung der Anzahl an Klicks für das Ablehnen von Cookie-Bannern
<b>Beschreibung</b>	Dieses Tool erfasst, wie viele Klicks nötig sind, um Cookies auf einer Website abzulehnen. Dieses Werkzeug wurde für das „Cookie Dialog Compliance“-Projekt entwickelt und ist hilfreich für technische Dokumentationen. Es ist nicht für Endnutzer:innen gedacht. Die Lösung besteht aus einer Chrome-Erweiterung und einem PHP-Backend, welches das Fat-Free Framework verwendet.
<b>Anwendung</b>	Chrome, GitHub
<b>Link</b>	<a href="https://github.com/koenberkhout/dark-patterns-project">https://github.com/koenberkhout/dark-patterns-project</a>

<b>Name</b>	<b>Distill.io</b>
	Kostenlos
<b>Ziel</b>	Dokumentation von Veränderungen auf Websites
<b>Beschreibung</b>	Übersichtliche Auflistung von Änderungen auf Websites. Es können ganze Seiten oder Teile einer Website ausgewählt werden. Das Intervall, in dem Veränderungen geprüft und dokumentiert werden, kann von 5 Sekunden bis zu mehreren Tagen festgelegt werden. Verschiedene Aktionen können bei Änderungen ausgelöst werden, z. B. E-Mail- oder SMS-Benachrichtigungen, lokale Pop-Ups oder Audio-Sounds. Die Browser-Erweiterung ermöglicht ein umfassendes Monitoring und funktioniert gut, sofern keine websitebedingten Blockierungen dies verhindern.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://github.com/koenberkhout/dark-patterns-project">https://github.com/koenberkhout/dark-patterns-project</a>

<b>Name</b>	<b>ShareX</b>
	Kostenlos
<b>Ziel</b>	Dokumentation
<b>Beschreibung</b>	ShareX ist ein Open Source-Tool für Screenshots, Screencasts und Datei-Sharing. Es ermöglicht das Erfassen und Bearbeiten von Screenshots, die Aufnahme von Bildschirmvideos und das einfache Hochladen und Teilen von Dateien. Das Tool unterstützt zahlreiche Cloud-Dienste, bietet umfangreiche Automatisierungsoptionen und ist stark anpassbar. User können ihre Aufnahmen und Dateien nahtlos in ihre bevorzugten Cloud-Speicher integrieren (z. B. Dropbox) und erhalten Freigabelinks.
<b>Anwendung</b>	Desktop Tool
<b>Link</b>	<a href="https://getsharex.com/">https://getsharex.com/</a>

<b>Name</b>	<b>Awesome Screenshot</b>
	Kostenlos
<b>Ziel</b>	Dokumentation
<b>Beschreibung</b>	Awesome Screenshot ist ein Tool für die Aufnahme und Bearbeitung von Screenshots und Bildschirmvideos. Es bietet Funktionen wie das Erfassen ganzer Websites oder ausgewählter Bereiche. Zusätzlich ermöglicht es die Aufnahme von Bildschirmvideos mit oder ohne Audio. Die erstellten Screenshots und Videos können direkt in die Cloud hochgeladen und einfach geteilt werden. Das Tool ist als Browser-Erweiterung verfügbar und unterstützt sowohl Chrome als auch Firefox.
<b>Anwendung</b>	Browser-Erweiterung
<b>Link</b>	<a href="https://www.awesomescreenshot.com/">https://www.awesomescreenshot.com/</a>

<b>Name</b>	<b>Nimbus</b>
	Kostenlos
<b>Ziel</b>	Website-Dokumentation
<b>Beschreibung</b>	<b>Nimbus</b> ist ein Tool für Screenshots und Bildschirmaufnahmen, verfügbar als Browser-Erweiterung und eigenständige Software. Es ermöglicht das Erfassen und Bearbeiten von Screenshots sowie die Aufnahme von Bildschirmvideos mit Audio. User können ihre Aufnahmen mit Anmerkungen versehen und direkt in der Cloud speichern oder teilen. Nimbus unterstützt Integrationen mit Google Drive und Dropbox und ist für verschiedene Betriebssysteme und Browser verfügbar.
<b>Anwendung</b>	Browser-Erweiterung, Software
<b>Link</b>	<a href="https://addons.mozilla.org/en-GB/firefox/addon/nimbus-screenshot/?src=search">https://addons.mozilla.org/en-GB/firefox/addon/nimbus-screenshot/?src=search</a>

## 6.5 Fallstricke in der automatisierten Detektion von Dark Patterns

Die automatisierte Erkennung von Dark Patterns auf Websites und in Apps ist herausfordernd. Der Begriff umfasst eine Vielzahl von Praktiken, die sich fundamental voneinander unterscheiden, sowohl typologisch als auch in ihrer technischen Umsetzung.<sup>60</sup> Es sind z. B. andere technische Ansätze erforderlich, um einen Countdown hinsichtlich seiner Echtheit zu untersuchen, oder den Text einer Button-Lösung auf mögliche Manipulationen hin zu bewerten. Um einen umfassenden Detektor für Dark Patterns zu entwickeln, müsste ein System entworfen werden, das in der Lage ist, unterschiedliche Elemente auf einer Website und in einer App (d.h. fixe Elemente sowie Prozessstrukturen) zu analysieren. Zu den dafür notwendigen Methoden zählen

<sup>60</sup> (Gray et al., 2023; Kitkowska, 2023; Luguri & Strahilevitz, 2021; Mathur et al., 2021)

jene zur Extraktion der Inhalte, gefolgt von Textanalysen, um manipulative Formulierungen zu erkennen, sowie Algorithmen zur Überprüfung von Interaktionen, um unfaire Prozesse zu dokumentieren.<sup>61</sup> Voraussetzung für eine automatische Erkennung von Dark Patterns sind klare Definitionen von eindeutigen Merkmalen, die zur Identifizierung und Bewertung eindeutiger Dark Pattern wie „Hard to cancel“ herangezogen werden können.<sup>62</sup>

Das Problem ist, dass nur manche Dark Patterns auf ersten Blick als eindeutig rechtswidrig identifiziert werden können. Meistens muss zwischen aggressivem Design und klaren Verstößen gegen Verbraucherschutzgesetze unterschieden werden, was eine Abwägung von Argumenten voraussetzt und nicht rein aufgrund von Mustererkennung eine klare Entscheidung ermöglicht.<sup>63</sup> Während ein Countdown technisch recht einfach als echt oder fake identifiziert werden kann, ist die Erwägung, ob ein Kündigungsprozess unnötig erschwert wird, mittels automatisierter Methoden bereits schwieriger umsetzbar. Die Bewertung, ob ein Text zu manipulativ ist, erfordert ebenfalls mehr Interpretation als eine einfache maschinelle 1-0-Lösung.<sup>64</sup> Hierfür wären fortgeschrittene KI-Technologien erforderlich, die semantische Analysen und kontextuelle Bewertungen durchführen können. Um solche Algorithmen zu trainieren, bräuchte es allerdings entsprechende Trainingsdaten aus der Rechtsdurchsetzung. Angesichts der Neuheit des Phänomens in dieser Domäne liegt jedoch kein ausreichender Datensatz dazu vor.

Darüber hinaus kommen Dark Patterns auch bei der Gestaltung von Prozessen zum Einsatz.<sup>65</sup> Hier wäre eine Lösung erforderlich, die Prozesse durchspielt – was ebenfalls sehr aufwendig ist. Die OECD berichtet, dass sich wissenschaftliche Vorhaben, die auf die automatisierte Detektion abzielen, nur eingeschränkte Elemente von Dark Patterns beachten können.<sup>66</sup> Möglich wäre umfassender auf das Thema zu blicken, doch dies würde die Implementierung von Automatisierungs- und Simulationstechnologien erfordern, die in der Lage sind, Benutzerinteraktionen nachzubilden und die Benutzererfahrung systematisch zu bewerten.<sup>67</sup> Solche Technologien müssten nicht nur die technischen Aspekte, sondern auch die psychologischen Auswirkungen auf die Nutzer:innen berücksichtigen.<sup>68</sup> Doch wie können solche technologischen Lösungen entwickelt werden, wenn dafür ein programmatisch umzusetzendes Verständnis zur Vulnerabilität von Usern vorliegen müsste, welches nicht nur demographisch gefasst werden kann, sondern auch situativ und individuell beeinflusst wird?

Hinzu kommt, dass Websites und Apps ihre Struktur häufig ändern oder das Crawling technisch blockieren, was einen hohen Aufwand für die Entwickler bedeutet, da nach jeder Änderung entsprechende Anpassungen vorgenommen werden müssen. Ein weiteres technisches Erfordernis wäre daher die Entwicklung adaptiver Crawling- und

---

<sup>61</sup> Vgl. (Kocyigit et al., 2023; Kodandaram et al., 2023; Raju et al., 2022)

<sup>62</sup> (Mathur et al., 2021)

<sup>63</sup> (Baroni et al., 2021; Kitkowska, 2023; Luguri & Strahilevitz, 2021; Shi et al., 2024)

<sup>64</sup> (Kodandaram et al., 2023; Shi et al., 2024)

<sup>65</sup> (Gray et al., 2018; Kuklenko, 2024; Tiangpanich & Nimkoompai, 2022)

<sup>66</sup> (OECD, 2022), S. 11

<sup>67</sup> (Ellwanger et al., 2017; Li et al., 2024; Souza et al., 2019)

<sup>68</sup> (Distler, 2021)

Parsing-Mechanismen, die sich dynamisch an strukturelle Änderungen anpassen können.<sup>69</sup>

Die Entwicklung eines Blueprints für ein Tool stellte sich daher als herausfordernd da, die technische Beschreibung des Prozesses findet sich im Annex dieser Studie (siehe **9 Technischer Annex**).

Zusammenfassend lässt sich feststellen, dass die Entwicklung technischer Werkzeuge zur automatisierten Erkennung von Dark Patterns auf Websites und in Apps eine außerordentlich komplexe Aufgabe darstellt. Die Vielfalt der Praktiken und deren unterschiedliche technische Umsetzungen erschweren eine einheitliche Erkennung erheblich. Darüber hinaus sind präzise Definitionen und umfangreiche Trainingsdaten unerlässlich, um die erforderlichen semantischen und kontextuellen Analysen durchführen zu können, die notwendig sind, um Dark Patterns korrekt zu identifizieren. Trotz dieser erheblichen Herausforderungen gibt es bereits einige Werkzeuge auf dem Markt, die in der Lage sind, bestimmte Aspekte von Dark Patterns zu erkennen und somit eine spürbare Arbeitserleichterung zu bieten. Einige dieser Werkzeuge wurden in den vorhergehenden Kapiteln präsentiert und teils auch im Projektrahmen getestet.

Herausgestochen ist jedenfalls das Open Source Tool Eagle, das auch bei der Erhebung von potenziellen Verstößen (siehe Kapitel 3, 4, 5) vom Projektteam intensiv genutzt wurde.<sup>70</sup>

---

<sup>69</sup> (Liu et al., 2011)

<sup>70</sup> Eagle, online: <https://en.eagle.cool/>

## 7 Schlussfolgerungen

Die vorliegende Studie illustriert die Komplexität der Umsetzung des Verbots von Dark Patterns, verdeutlicht gleichzeitig die Aktualität der Thematik und mögliche Ansatzpunkte im Sinne des Verbraucherschutzes. Zusammenfassend handelt es sich um:

- **Taxonomien von Dark Patterns im Sinne des Verbraucherschutzes nutzen:** Die Dynamik rund um von einem Teil der Öffentlichkeit und der Wissenschaft erweiterten Taxonomien von Dark Patterns kann als eine Stärke angesehen werden, um mögliche Verstöße im Sinne von UGP-RL und DSA zu benennen und auch auf neue Phänomene des Designs von Entscheidungsarchitekturen auf Websites und Plattformen reagieren zu können.
- **Dark Patterns für die Rechtsdurchsetzung definieren:** Für die Definition von Dark Patterns für die Rechtsdurchsetzung sind die vorliegenden Taxonomien allerdings nur bedingt geeignet. Die Umsetzung des Vorschlags der Europäischen Verbraucherschutzbehörde BEUC, Dark Patterns konkret im Annex der UGP-RL aufzulisten, bräuchte jedenfalls einiges an weiterem Definitionsaufwand. Dark Patterns Praktiken müssen gut abgegrenzt werden können von legitimen Maßnahmen des Marketings. Alternativ gibt es Vorschläge, Dark Patterns als Abweichungen von Design-Standards zu definieren, auch dies könnte sich eignen.
- **Klärung der Anwendung von Rechtsmaterie:** Ein im Sinne des Schutzes des Verbrauchers bzw. der Verbraucherin dringend zu bearbeitendes Thema ist die Frage, welches Recht anzuwenden ist. Das betrifft die Verdrängung des Art 25 DSA durch UGP-RL und DSGVO (Art 25 Abs 2 DSA) und Existenzberechtigung des Art 25 DSA und ist für eine erfolgreiche Rechtsdurchsetzung unabdingbar.
- **Die Zukunft von Dark Patterns und Notwendigkeiten über das Leitbild des schutzbedürftigen Verbrauchers zu diskutieren:** Die Zukunft bringt auch technologische Veränderungen mit sich, die andeuten, dass manche Regelungen nicht in ihrem intendierten Sinne wirken könnten – wie das Verbot von verhaltensbasierter Werbung – und auch, dass der stärkeren Wirkungsweise von Dark Patterns Rechnung getragen werden muss. In Diskussion gestellt muss insofern, mit welchem Leitbild des schutzbedürftigen Verbrauchers im digitalen Zeitalter gearbeitet werden kann.
- **Dark Patterns auch abseits von Plattformen verbieten:** Angesichts dessen, dass Dark Patterns nicht nur auf Plattformen, sondern als generelleres Internet-Phänomen auftreten, ist das Verbot von Dark Patterns im DSA zu begrüßen, es wäre aber begrüßenswert über Erweiterungen nachzudenken, um diesen Praktiken auch in anderen Bereichen des digitalen Raumes begegnen zu können.

## Taxonomien der Dark Patterns im Sinne des Verbraucherschutzes nutzen

Die Definition von Dark Patterns bleibt dynamisch und wird sowohl wissenschaftlich als auch durch Internet-Communities stetig weiterentwickelt. Diese so entstehenden, umfassenden Taxonomien ermöglichen eine präzisere Benennung von Praktiken. In der durch Harry Brignull geführten Website zu Deceptive Design (vormals Dark Patterns) werden beispielhafte Probleme unter dem Titel „Hall of Shame“ gesammelt – mit Verweisen auf internationale Medienberichte.<sup>71</sup> Die Europäische Verbraucherschutzbehörde BEUC geht mit der Forderung nach der Einrichtung einer zentralen Datenbank, deren Aufbau unter der Koordination der Europäischen Kommission erfolgen sollte, in Richtung jener von Brignull organisierten Website. Die Datenbank solle nationale Entscheidungen von öffentlichen Autoritäten und zivilen Gerichten zu Dark Patterns erfassen, um Transparenz zu schaffen und die Rechtsdurchsetzung zu verbessern.

Anzumerken ist dabei, dass die mediale Aufmerksamkeit mit dem Begriff Dark Patterns gut auf problematische Praktiken der Industrie gelenkt werden kann, doch vorrangig dient das einer Illustration möglicher Verstöße – so kann über ein Dark Pattern wie „Roach Motel“ (Kakerlaken-Hotel) auf einfache Art für Verbraucher:innen erklärt werden, worin das Problem von schwer abzubrechenden Newsletter-Abonnements liegt.

Kritiker:innen merken jedoch an, dass manche Praktiken nur in bestimmten Kontexten oder nur unter bestimmten Vorzeichen der Verbrauchereinstellungen als Dark Patterns bezeichnet werden können. Ein und dasselbe Element könnte somit je nachdem, welche Absicht des Verbrauchers oder der Verbraucherin angenommen wird, anders einzuordnen sein. Ein Beispiel: Eine Empfehlung von Produkten entlang der bisherigen Kaufhistorie kann dazu führen, dass jemand mehr als intendiert in einem Onlineshop ausgibt – dasselbe Element kann aber auch von Verbraucher:innen und Verbrauchern gewünscht werden, ähnlich wie eine Beratungsleistung in einem stationären Geschäft. Ähnlich verhält es sich mit der Frage, ob ein Autoplay von Videos als Dark Patterns eingeordnet werden sollte. Diskutiert werden kann auch, ob wenn in einem Prozess ein Button prominenter gemacht wird als der andere, ein Unternehmen dies allerdings mit der mehrheitlich präferierten Option argumentiert, dies im Sinne eines Dark Patterns bewertet werden kann. Auch Dark Patterns, die darin bestehen zu zeigen, wie viele Hotelzimmer noch frei sind oder wie lange ein Rabatt noch gilt, können auch als im Interesse von Verbraucher:innen stehende Elemente interpretiert werden.<sup>72</sup>

## Dark Patterns für die Rechtsdurchsetzung definieren

Konsumentenschutzorganisationen wie BEUC (European Consumer Organisation) fordern, dass manche Dark Patterns direkt im Annex des UGP-RL verboten werden, wie z. B. der Aufbau von emotionalem Druck „Confirmshaming“.<sup>73</sup> Dafür bräuchte es

---

<sup>71</sup> (Brignull, 2024) <https://www.deceptive.design/hall-of-shame> (aufgerufen 18.06.2024)

<sup>72</sup> (OECD, 2022), S. 15

<sup>73</sup> (BEUC, 2022b)

allerdings präzisere, voneinander und von anderen legitimen Praktiken abgrenzbare Definitionen.

Ab wann ist ein Prozess oder Designelement bereits als Dark Pattern zu verbieten? Empfehlungen, die auf Kaufhistorien basieren, veranschaulichen die Ambivalenz zwischen legitimen/manipulativen oder auch von Verbraucherinnen und Verbrauchern erwünschten/unerwünschten Praktiken. Manche Vorschläge zielen darauf ab, Dark Patterns und Marketing anhand ihrer Ziele zu differenzieren: Während Marketing darauf abzielt, die Präferenzen der Verbraucher:innen zu ändern, zielen Dark Patterns auf deren Manipulation ab.<sup>74</sup> Manche schlagen vor, die Bewertung entlang der Wirkung auf Konsument:innen („Thresholds“) zu betrachten – und dafür zum Beispiel die Erwartung von Verbraucherinnen und Verbrauchern als Abgleich zu nehmen. Wenn beispielsweise die Erstellung eines Kundenkontos die Preisgabe übermäßiger Daten und die Zustimmung zu unerwünschten Mitteilungen erfordert, widerspricht dies den Erwartungen der Verbraucher:innen und stellt somit ein unverhältnismäßiges Vorgehen dar. Auch die BEUC betont, wie wichtig es wäre, Erkenntnisse der Verhaltensforschung mehr in Aktivitäten der Rechtsdurchsetzung zu integrieren. In diesem Sinne zu sehen ist auch ihre Forderung, Unternehmen zu verpflichten, jegliche Informationen über Behavioral-Experimente, die zur Optimierung des Designs einer Website durchgeführt werden, offenzulegen.<sup>75</sup>

Welches Recht ist anzuwenden? Zur Verdrängung des Art 25 DSA durch die UGP-RL und die DSGVO (Art 25 Abs 2 DSA) – die Frage der Existenzberechtigung des Art 25 DSA

Bei Dark Patterns kommt hinzu, dass die Anwendung des DSA aus Sicht mancher noch unklar ist: Wie wird sich die Anwendung des DSA gestalten, angesichts dessen, dass der DSA als *lex specifica* auf das UWG als *lex generalis* verweist? Laut Handig fehlt es hier an einer kongruenten Auslegung der geltenden Regelungen und die einzelnen Bestimmungen ergeben eher ein „pointilistisches Gesamtbild“, statt einer koordinierten Vorgehensweise. Er bezeichnet die „auf Dark Patterns bezogenen Unionsrechtsnormen [als] wenig abgestimmt“.<sup>76</sup>

Nach Artikel 25 Absatz 2 DSA gilt das in diesem Artikel geregelte Verbot der Verwendung von Dark Patterns nicht für Praktiken, die unter die UGP-RL oder die DSGVO fallen. Dies bedeutet, dass die Regelung des DSA nur dann greift, wenn die angewandte Geschäftspraktik nicht bereits durch die UGP-RL oder die DSGVO subsumiert werden kann. Insbesondere vor dem Hintergrund des weiten Anwendungsbereichs der UGP-RL stellt sich die Frage, wie effektiv und sinnvoll dieses Verbot in der Praxis sein wird. Artikel 25 Absatz 2 DSA könnte vielmehr die Rechtsdurchsetzung erschweren. Dies könnte dazu führen, dass die DSA-Behörden auch das Lauterkeitsrecht und das Datenschutzrecht prüfen müssen, ohne für diese Bereiche zuständig zu sein. Zudem könnten Gewerbetreibende in einem zivilrechtlichen Verbandsverfahren den Einwand erheben, dass ihr Verhalten nach lauterkeitsrechtlichen bzw. datenschutzrechtlichen Vorgaben zu prüfen sei und sich damit auf den Ausschluss von Artikel 25 DSA berufen. In einem Zivilverfahren ist

---

<sup>74</sup> (Luguri & Strahilevitz, 2021)

<sup>75</sup> (BEUC, 2022b, 2022a, 2023)

<sup>76</sup> (Handig, 2023) S.203

daher Vorsicht geboten. Es wird bei gewissen Designtricks angeraten sein, ein Eventualbegehren auf Unterlassung der Praktik einerseits nach dem jeweiligen nationalen Umsetzungsgesetz der UGP-RL (in Österreich das Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG) und andererseits nach Art 25 DSA zu stützen.

Zur Notwendigkeit das Leitbild des schutzbedürftigen Verbrauchers bzw. der schutzbedürftigen Verbraucherin zu diskutieren

Wie das Leitbild des schutzbedürftigen Verbrauchers im digitalen Umfeld verstanden werden kann, ist eine Problematik, die über die Studienthematik weit hinaus geht, jedoch auch beim Thema Dark Patterns und verhaltensbasierte Werbung relevant ist. Denn im digitalen Umfeld können Gewerbetreibende durch die Erhebung von personenbezogenen Daten, aber auch durch die Analyse von verhaltensbasierten oder kontextuellen Informationen, deutlich mehr Wissen über Verbraucher:innen erlangen als im stationären Handel. Überzeugungsmethoden können entsprechend perfektioniert werden, sei es, weil es ein Mehr an Daten gibt (individuell wie auch aggregiert), sei es, weil Methoden wie A/B-Tests ein hohes Grad an Anpassung erlauben, aber auch die Wirksamkeit ihrer Praktiken deutlich einfacher und zielgerichteter verbessert werden können. Unternehmen werden diese Praktiken weiter nutzen, sofern nicht durch die Durchsetzung von Verbraucherrechten oder gesellschaftliche Sanktionen diese Entwicklungen gebremst werden können.

Die Anwendung der erwähnten Techniken verschafft den Gewerbetreibenden einen erheblichen Vorteil bei der Umsetzung erfolgreicher Geschäftspraktiken online. Dark Patterns sind teilweise Resultat dieser Entwicklungen – und entsprechend ergibt sich aus Verbraucherschutzsicht das Bedürfnis, Verbraucher:innen besser und effektiver vor diesen Geschäftspraktiken zu schützen. Wie kann dies anhand eines veränderten Verbraucherleitbilds funktionieren? Die Europäische Kommission vertritt in den Leitlinien zur Auslegung und Anwendung der Richtlinie 2005/29/EG die Position, dass der Begriff der Schutzbedürftigkeit in der UGP-RL dynamisch und situationsabhängig auszulegen ist.<sup>77</sup> Diese Auseinandersetzung mit situativer, digitaler Vulnerabilität steht teils im Widerspruch zu fixen, vordefinierten Gruppen von vulnerablen Konsument:innen, die im digitalen Raum besonders schutzbedürftig sind.<sup>78</sup> Dies trifft auf Kinder und minderjährige Personen zu, aber auch auf viel diversere Gruppen, die weniger leicht definierbar aber auch identifizierbar sind.

Für einen verbraucherfreundlichen und zeitgemäßen Ansatz ist es daher notwendig, die Begriffe "Durchschnittsverbraucher" und "Schutzbedürftigkeit" zu überdenken, um die Herausforderungen des digitalen Umfelds für Verbraucher:innen genauer zu erfassen und somit die Auswirkungen von Geschäftspraktiken auf den Durchschnittsverbraucher im digitalen Umfeld besser einschätzen zu können. Diese Definition ist besonders sensibel, da auch Konsument:innen und Bürger:innen immer deckungsgleicher werden – die Teilhabe am öffentlichen Leben, online sowie offline, ist kaum ohne Konsum möglich. Bei jedem Einloggen in Soziale Medien werden

---

<sup>77</sup> Die Leitlinien der Kommission zur Auslegung und Anwendung der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt, ABl 2021 C 526/1, unter 4.2.7 zu Dark Patterns

<sup>78</sup> (BEUC, 2022b; Helberger et al., 2024)

Bürger:innen unweigerlich zu Konsument:innen, von Werbung, von zielgerichteten, personalisierten Inhalten. Werden Konsument:innen online als Bürger:innen definiert und anerkannt, dass ihre Vulnerabilität durch die ungleiche Machtverteilung zwischen Plattformen und dem Individuum notwendigerweise gegeben ist, könnten stärkere Schutzmaßnahmen vor manipulativem Design wie Dark Patterns einfacher gerechtfertigt und durchgesetzt werden.

#### Erweiterung des Verbots von Dark Patterns

Angesichts der Tatsache, dass Dark Patterns nicht nur auf spezifischen Plattformen, sondern als allgemeines Phänomen im Internet auftreten, ist das Verbot von Dark Patterns im Rahmen des Digital Services Act (DSA) ein begrüßenswerter Schritt. Es wäre jedoch ebenfalls sinnvoll, über Erweiterungen nachzudenken, um diesen Praktiken auch in anderen Bereichen der Online-Welt wirksam entgegenzuwirken. Eine Möglichkeit wäre es, diese Praktiken entweder durch eine Erweiterung der schwarzen Liste in Anhang I der UGP-RL zu regulieren bzw. zu verbieten oder eine neue Regelung zu schaffen, die es ermöglicht, Verbraucher:innen besser vor manipulativen Gestaltungspraktiken über solche Plattformen zu schützen.

Zusammenfassend kann festgehalten werden, dass der Schutz der Verbraucher:innen vor Dark Patterns eine fortwährende Herausforderung darstellt, die eine präzisere rechtliche Rahmgebung und eine stärkere Berücksichtigung verhaltenswissenschaftlicher Erkenntnisse erfordert. Nur durch ein aktualisiertes Verbraucherleitbild und verbesserte gesetzliche Maßnahmen kann den manipulativen Praktiken im digitalen Umfeld wirksam entgegengewirkt werden. Dies impliziert zudem die Erfordernis einer Neubewertung der Begriffe „Durchschnittsverbraucher“ und „Schutzbedürftigkeit“ im Kontext des digitalen Konsums, um die tatsächlichen Herausforderungen und Risiken adäquat zu reflektieren. Die Einbeziehung von Erkenntnissen aus der Verhaltensforschung sowie die Schaffung klarer rechtlicher Definitionen und Sanktionen stellen entscheidende Faktoren dar, um die Rechte und Interessen der Verbraucher:innen im digitalen Zeitalter zu schützen.

## 8 Quellen

### 8.1 Literaturverzeichnis

- Arbeiterkammer. (2024, April 15). *AK Erfolg: Abzocke bei Opodo-Reisebuchung wird Riegel vorgeschoben!* OTS.at. [https://www.ots.at/presseaussendung/OTS\\_20240415\\_OTS0020/ak-erfolg-abzocke-bei-opodo-reisebuchung-wird-riegel-vorgeschoben](https://www.ots.at/presseaussendung/OTS_20240415_OTS0020/ak-erfolg-abzocke-bei-opodo-reisebuchung-wird-riegel-vorgeschoben)
- Baroni, L. A., Puska, A. A., de Castro Salgado, L. C., & Pereira, R. (2021). Dark Patterns: Towards a Socio-technical Approach. *Proceedings of the XX Brazilian Symposium on Human Factors in Computing Systems*, 1–7. <https://doi.org/10.1145/3472301.3484336>
- Beltzung, L., Lindley, A., Rieß, E., Krickl, J., Srdjan Stevanetic, & Vignoli, M. (2021). *Hinter den Kulissen von Amazon.de—Eine Analyse der Mechanismen des Marktplatzes Amazon. Studie mit quantitativer Erhebung im Auftrag der Arbeiterkammer Wien.* <https://doi.org/10.13140/RG.2.2.22830.23367>
- BEUC. (2022a). *BEUC Comments on the EDPB Guidelines on Dark Patterns in Social Media Platform Interfaces.* Der Europäische Verbraucherverband. [https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media\\_en](https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en)
- BEUC. (2022b). *“DARK PATTERNS” AND THE EU CONSUMER LAW ACQUIS - Recommendations for better enforcement and reform.* Der Europäische Verbraucherverband. [https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013\\_dark\\_patters\\_paper.pdf](https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf)
- BEUC. (2023). *TOWARDS EUROPEAN DIGITAL FAIRNESS BEUC framing response paper for the REFIT consultation.* Der Europäische Verbraucherverband. [https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020\\_Consultation\\_paper\\_REFIT\\_consumer\\_law\\_digital\\_fairness.pdf](https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf)
- Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies*, 2016(4), 237–254. <https://doi.org/10.1515/popets-2016-0038>
- Brignull, H. (2010, Juli 8). *Dark Patterns: Dirty tricks designers use to make people do stuff.* 90 Percent Of Everything. <https://www.90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/>
- Brignull, H. (2022). Types of Deceptive Design. *Deceptive Design.* <https://www.deceptive.design/types>
- Brignull, H. (2024). *Deceptive Patterns—Hall of Shame.* Deceptive Patterns. <https://www.deceptive.design/hall-of-shame>
- Bundeskartellamt. (2019, Februar 7). *Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen.* Bundeskartellamt. [https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07\\_02\\_2019\\_Facebook.html](https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html)
- Burkell, J., Fortier, A., Wong, L., & Simpson, J. (2013). The View From Here: User-Centered Perspectives on Social Network Privacy. *FIMS Publications.* <https://ir.lib.uwo.ca/fimspub/25>
- Caragay, E., Xiong, K., Zong, J., & Jackson, D. (2024). Beyond Dark Patterns: A Concept-Based Framework for Ethical Software Design. *Proceedings of the*

- CHI Conference on Human Factors in Computing Systems*, 1–16. <https://doi.org/10.1145/3613904.3642781>
- Distler, V. (2021). *The Experience of Security in Human-Computer Interactions: Understanding Security Perceptions Through the Concept of User Experience*. [Faculty of Humanities, Education and Social Sciences: Behavioural and Cognitive Sciences]. University of Luxembourg.
- Ellwanger, C., Silva, R. P. da, & Rocha, R. A. da. (2017). Modelagem sistêmica e simulação: Estratégia de gestão no Processo de Projeto para a Experiência do Usuário (UXD). *Gestão & Produção*, 25(4), 659–670. <https://doi.org/10.1590/0104-530x3604-16>
- Europäische Kommission. (2024a, Mai). *DMA designated Gatekeepers*. [https://digital-markets-act.ec.europa.eu/gatekeepers\\_en](https://digital-markets-act.ec.europa.eu/gatekeepers_en)
- Europäische Kommission. (2024b, Mai 31). *DSA: Commission designates Temu as VLOP* [Text]. European Commission - European Commission. [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_24\\_3047](https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3047)
- Europäische Kommission. (2024c, Juni 13). *Supervision of the designated very large online platforms and search engines under DSA | Shaping Europe's digital future*. <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>
- European Data Protection Board. (2024). *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*. [https://www.edpb.europa.eu/system/files/2024-04/edpb\\_opinion\\_202408\\_consentorpay\\_en.pdf](https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf)
- European Data Protection Board, E. (2022). *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*.
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. <https://doi.org/10.1145/3173574.3174108>
- Gray, C. M., Santos, C., & Bielova, N. (2023). Towards a Preliminary Ontology of Dark Patterns Knowledge. *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–9. <https://doi.org/10.1145/3544549.3585676>
- Handig, C. (2023). Dark Patterns im Fokus. Neue Normen der EU für manipulative Gestaltungsformen digitaler Nutzerschnittstellen. *ÖBI*, 60(5/2023), 199.
- Helberger, N., Kas, B., Micklitz, H.-W., Namysłowska, M., Naudts, L., Rott, P., Sax, M., & Veale, M. (2024). *Digital Fairness for Consumers* (BEUC Report, S. 280). [https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-032\\_Digital\\_fairness\\_for\\_consumers\\_Report.pdf](https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf)
- Holle, V. von. (2019). *Eine ökonomische Revolution: Wie Verhaltensökonomie die Welt verändert*. Springer-Verlag.
- Kahneman, D. (2011). *THINKING, FAST AND SLOW*. macmillan.
- Kitkowska, A. (2023). The Hows and Whys of Dark Patterns: Categorizations and Privacy. In N. Gerber, A. Stöver, & K. Marky (Hrsg.), *Human Factors in Privacy Research* (S. 173–198). Springer International Publishing. [https://doi.org/10.1007/978-3-031-28643-8\\_9](https://doi.org/10.1007/978-3-031-28643-8_9)
- Kocyigit, E., Rossi, A., & Lenzini, G. (2023). Towards Assessing Features of Dark Patterns in Cookie Consent Processes. In F. Bieker, J. Meyer, S. Pape, I. Schiering, & A. Weich (Hrsg.), *Privacy and Identity Management* (Bd. 671, S. 165–183). Springer Nature Switzerland. [https://doi.org/10.1007/978-3-031-31971-6\\_13](https://doi.org/10.1007/978-3-031-31971-6_13)

- Kodandaram, S. R., Sunkara, M., Jayarathna, S., & Ashok, V. (2023). Detecting Deceptive Dark-Pattern Web Advertisements for Blind Screen-Reader Users. *Journal of Imaging*, 9(11), 239. <https://doi.org/10.3390/jimaging9110239>
- Kuklenko, P. (2024). *The Role of Dark Design Patterns in Online Consumer Manipulation: A Critical Study with Emphasis on Video Game Monetisation*. [Degree Thesis]. Arcada University of Applied Sciences: Online Media.
- Li, X., Zheng, H., Chen, J., Zong, Y., & Yu, L. (2024). User Interaction Interface Design and Innovation Based on Artificial Intelligence Technology. *Journal of Theory and Practice of Engineering Science*, 4(03), 1–8. [https://doi.org/10.53469/jtpes.2024.04\(03\).01](https://doi.org/10.53469/jtpes.2024.04(03).01)
- Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, 29(4), 1649–1656. <https://doi.org/10.1016/j.chb.2013.01.049>
- Liu, J., Jiang, L., Wu, Z., & Zheng, Q. (2011). Deep Web adaptive crawling based on minimum executable pattern. *Journal of Intelligent Information Systems*, 36(2), 197–215. <https://doi.org/10.1007/s10844-010-0124-5>
- Luguri, J., & Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, 13(1), 43–109. <https://doi.org/10.1093/jla/laaa006>
- Madejski, M., Johnson, M., & Bellovin, S. M. (2012). A study of privacy settings errors in an online social network. *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, 340–345. <https://doi.org/10.1109/PerComW.2012.6197507>
- Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–32. <https://doi.org/10.1145/3359183>
- Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–18. <https://doi.org/10.1145/3411764.3445610>
- Murray, D. (2023, Januar 9). *The Unknown Story of How Hotmail Grew to 12 Million Users in 1.5 Years*. The Marketing Millennials. <https://themarketingmillennials.com/articles/2023-01-09/the-unknown-story-of-how-hotmail-grew-to-12-million-users-in-1-5-years/>
- Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). *Dark Patterns Past, Present, and Future*. 18(2). <https://queue.acm.org/detail.cfm?id=3400901>
- netidee. (2018). *Preis.wert. netidee*. <https://www.netidee.at/preiswert>
- NOYB. (2024, April 9). „Pay or Okay“ erklärt: Wie dich Websites zwingen, für Datenschutz zu bezahlen. <https://noyb.eu/de/pay-or-okay-explained-why-more-and-more-websites-make-you-pay-your-privacy>
- OECD. (2022). *Dark commercial patterns | en | OECD*. <https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm>
- Princi, E., & Krämer, N. (2020). *I Spy with my Little Sensor Eye—Effect of Data-Tracking and Convenience on the Intention to Use Smart Technology*. 1–10. <https://doi.org/10.24251/HICSS.2020.171>
- Raju, S. H., Waris, S. F., Adinarayna, S., Jadala, V. C., & Rao, G. S. (2022). Smart Dark Pattern Detection: Making Aware of Misleading Patterns Through the Intended App. In S. Shakya, V. E. Balas, S. Kamolphiwong, & K.-L. Du (Hrsg.), *Sentimental Analysis and Deep Learning* (Bd. 1408, S. 933–947). Springer Singapore. [https://doi.org/10.1007/978-981-16-5157-1\\_72](https://doi.org/10.1007/978-981-16-5157-1_72)

- Sangeeta, R. (2015). A Comprehensive Study on Providing Services based on User Interest in Online Social Networks. *Engineering Technology*, 6(05).
- Shi, Z., Sun, R., Chen, J., Sun, J., & Xue, M. (2024). The Invisible Game on the Internet: A Case Study of Decoding Deceptive Patterns. *Companion Proceedings of the ACM on Web Conference 2024*, 521–524. <https://doi.org/10.1145/3589335.3651571>
- Souza, K. E. S., Seruffo, M. C. R., De Mello, H. D., Souza, D. D. S., & Vellasco, M. M. B. R. (2019). User Experience Evaluation Using Mouse Tracking and Artificial Intelligence. *IEEE Access*, 7, 96506–96515. <https://doi.org/10.1109/ACCESS.2019.2927860>
- Strange, A. (2015, Oktober 3). *LinkedIn pays big after class action lawsuit over user emails*. Mashable. <https://mashable.com/archive/linkedin-class-action>
- Tech Policy Design Lab—Deceptive Design*. (o. J.). Abgerufen 13. Mai 2024, von <https://techlab.webfoundation.org/deceptive-design/overview>
- Thaler, R. H. (2017). *Facts*. NobelPrize.org. NobelPrize.Org. <https://www.nobelprize.org/prizes/economic-sciences/2017/thaler/facts/>
- Thaler, R. H. (2018). Nudge, not sludge. *Science*, 361(6401), 431–431. <https://doi.org/10.1126/science.aau9241>
- Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin.
- Tiangpanich, P., & Nimkoompai, A. (2022). An Analysis of Differences between Dark Pattern and Anti-Pattern to Increase Efficiency Application Design. *2022 7th International Conference on Business and Industrial Research (ICBIR)*, 416–421. <https://doi.org/10.1109/ICBIR54589.2022.9786470>

## 8.2 Abbildungsverzeichnis

Abbildung 1: Die Startseite von Temu.com (Screenshot, 30.10.2023).	24
Abbildung 2: Werbeanzeige für PS4-Controller, Temu Austria (Screenshot, 16.10.2023).	25
Abbildung 3: Gleiches Werbesujet mit leicht veränderten Texten (Screenshot, 16.10.2023).	25
Abbildung 4: Rabatt zu gewinnen, Temu-App (Screenshot, 16.10.2023).	26
Abbildung 5: Countdowns auf Temu (Screenshot, 09.11.2023).	26
Abbildung 6: Countdowns und Knappheitsanzeigen auf Temu (Screenshot, 07.05.2024).	27
Abbildung 7: Meta-Werbebibliothek, Temu Austria (Screenshot, 07.05.2024).	27
Abbildung 8: Werbeanzeige Temu, „kostenloses Produkt“ (Screenshot, 07.05.2024).	28
Abbildung 9: Temu Website (Screenshot, 07.05.2024).	28
Abbildung 10: Temu Gewinnspiel, Werbeanzeige auf Instagram, (Screenshot, 18.07.2023).	29
Abbildung 11: Temu Gewinnspiel auf Instagram (Screenshot, 18.07.2023).	29
Abbildung 12: Temu Instagram Werbung (Screenshot, 18.07.2023).	29
Abbildung 13: Temu mobile Website, (Screenshot, 18.07.2023).	30
Abbildung 14: App Store Temu-App (Screenshot, 18.07.2023).	30
Abbildung 15: Startseite der Temu App nach Download (Screenshot, 18.07.2023).	30
Abbildung 16: Pop-Ups in Temu-App (Screenshot, 18.07.2023).	31
Abbildung 17: Pop-Ups in Temu-App (Screenshot, 18.07.2023).	31
Abbildung 18: Website von SHEIN.com (Screenshot, 18.10.2022).	34
Abbildung 19: Website SHEIN.com mit Pop-Up zu App (Screenshot, 11.06.2024).	35
Abbildung 20: Pop-Up „Sonderangebote nur für dich“ (Screenshot, 11.06.2024).	36
Abbildung 21: Pop-Up zur Registrierung bei SHEIN (Screenshot, 11.06.2024).	36
Abbildung 22: Pop-Up zur Registrierung bei SHEIN (Screenshot, 18.10.2022).	37
Abbildung 23: Startseite von de.SHEIN.com (Screenshot, 11.06.2024).	37
Abbildung 24: Übersicht der Blitzangebote SHEIN (Screenshot, 11.06.2024).	38

Abbildung 25: Blitzangebote von SHEIN (Screenshot, 11.06.2024).	38
Abbildung 26: Seite des SHEIN CLUB (Screenshot, 18.06.2024).	39
Abbildung 27: Seite des SHEIN Saver Clubs (Screenshot, 18.06.2024).	39
Abbildung 28: Ryanair-Tarife (Screenshot, 17.04.2024).	44
Abbildung 29: Ryan Air: Tarife-Preisdarstellung (Screenshot, 17.04.2024)	44
Abbildung 30: Ryanair Pop-Up bei Auswahl des Basic-Tarifs. (Screenshot, 17.04.2024).	45
Abbildung 31: Ryanair Gesamtpreis Ansicht. (Screenshot, 17.04.2024).	46
Abbildung 32: Ryanair Sitzplatzauswahl (Screenshot, 17.04.2024).	46
Abbildung 33: Ryanair Sitzplatzauswahl – Option 2 (Screenshot, 17.04.2024).	47
Abbildung 34: Ryanair Sitzplatz Pop-Up (Screenshot, 17.04.2024).	48
Abbildung 35: Ryanair Gepäcksauswahl (Screenshot, 17.10.2023).	49
Abbildung 36: Ryanair Gepäck bei Regular Tarif (Screenshot, 17.10.2023).	49
Abbildung 37: Ryanair Gepäck bei Plus Tarif (Screenshot, 17.04.2024).	50
Abbildung 38: Ryanair Pop-Up Versicherungen (Screenshot, 17.04.2024).	51
Abbildung 39: Ryanair Versicherungen (Screenshot, 04.09.2023).	52
Abbildung 40: Ryanair Vorauswahl Newsletter und Benachrichtigungen (Screenshot, 17.04.2024).	52
Tabelle 1 Vergleich der Tarifpakete mit frei zusammengestellten Zusatzservice-Paketen.	53
Abbildung 41: Austrian Tarife Economy (Screenshot, 18.04.2024).	56
Abbildung 42: Austrian Tarife Preise (Screenshot, 18.04.2024).	57
Abbildung 43: Austrian Business Tarife (Screenshot, 18.04.2024).	57
Abbildung 44: Austrian Economy Preise inkludierte Leistungen (Screenshot, 18.04.2024).	58
Abbildung 45: Austrian Zusatzleistungen Sitzplätze und Gepäck (Screenshot 18.04.2024).	59
Abbildung 46: WizzAir Flugauswahl (Screenshot, 18.04.2024).	60
Abbildung 47: Auswahl der Flugtarife WizzAir (Screenshot, 03.05.2024).	61
Abbildung 48: Wizz Tarifauswahl (Screenshot, 18.04.2024).	61
Abbildung 49: Wizz Sitzplatzauswahl (Screenshot, 18.04.2024).	62
Abbildung 50: Wizz Empfohlene Sitzplatzauswahl (Screenshot, 18.04.2024).	62
Abbildung 51: Wizz Anzeige WiZZ Discount Club „Mitglied werden“ (Screenshot, 18.04.2024).	63
Abbildung 52: WiZZ Discount Club – schwieriges Opt-Out (Screenshot, 18.04.2024).	64
Abbildung 53: Zusatzservices von Wizz Air (Screenshot, 03.05.2024).	64
Abbildung 54: Opodo erste Ansicht des Preises, Prime-Deal. (Screenshot, 18.04.2024).	67
Abbildung 55: Opodo nicht ermäßigter Tarif. (Screenshot, 18.04.2024).	67
Abbildung 56: Opodo Preisauflüsselung (Screenshot, 18.04.2024).	68
Abbildung 57: Opodo - Pop-Up "Weiter ohne Sitzplatz". (Screenshot, 18.04.2024).	68
Abbildung 58: Opodo, Pop-Up mit Nachfrage zu Kundenservice (Screenshot, 18.04.2024).	69
Abbildung 59: Opodo Prime Anzeige vor Kaufabschluss (Screenshot, 18.04.2024).	70
Abbildung 60: Opodo Prime Anzeige - Button-Lösung (Screenshot, 18.04.2024).	71
Abbildung 61: Zusatzleistung buchen, Option für Datumsänderung (Screenshot, 18.04.2024).	71
Abbildung 62: Anmeldung bei TikTok mit Apple ID (Screenshot, 02.04.2024).	77
Abbildung 63: Info zu Personalisierung, TikTok (Screenshot, 02.04.2024).	78
Abbildung 64: "Wähle wie Werbung angezeigt wird", TikTok (Screenshot, 02.04.2024).	78
Abbildung 65: Einstellungen zu Anzeigen auf TikTok, User-Profil Anna (Screenshot, 02.04.2024).	79
Abbildung 68 Privatsphäre Einstellungen TikTok – Privates Konto (Screenshot, 02.04.2024).	80
Abbildung 69: Schlage anderen dein Konto vor, TikTok (Screenshot, 02.04.2024).	80
Abbildung 70: Verwendung von Cookies auf Instagram (Screenshot, 02.04.2024).	83
Abbildung 71: Nutzungsbedingungen von Instagram (Screenshot, 02.04.2024).	83
Abbildung 72: Anfrage Kontakte synchronisieren Instagram (Screenshot, 02.04.2024).	84
Abbildung 73: Zugriff auf Kontakte Instagram Pop-Up (Screenshot, 02.04.2024).	84
Abbildung 74: Konto Privatsphäre-Einstellungen Instagram (Screenshot, 02.04.2024).	85
Abbildung 75: Benachrichtigungen aktivieren, Instagram (Screenshot, 02.04.2024).	85

---

<i>Abbildung 76: Einstellungen Instagram (Screenshot, 02.04.2024).</i>	86
<i>Abbildung 77: Werbepräferenzen Instagram (Screenshot, 02.04.2024).</i>	86
<i>Abbildung 78: Schematische Übersicht über die PCS-Schwerpunktsetzung der Komponenten, die zur Realisierung einer prototypischen Datenerhebung auf Basis des Appium-Frameworks.</i>	112
<i>Abbildung 79: Auszug aus dem Appium-Inspector zur Analyse der der App.</i>	113

## 9 Technischer Annex

### 9.1 Beschreibung der Tool-Entwicklung

Wie im vorliegenden Studienbericht dargelegt, werden Dark Patterns teilweise zur Ausgestaltung von Prozessen eingesetzt, weshalb zum Teil Lösungen erforderlich sind, bei denen Prozesse automatisiert durchgespielt werden. Die aus diesem Grund notwendige Automatisierungs- und Simulationstechnologie muss in der Lage sein, die Benutzerinteraktion nachzubilden.

Die präsentierte PCS-Implementierung auf Basis des Appium-Frameworks zielt darauf ab, Daten aus mobilen Apps zu extrahieren. Hierbei handelt es sich um einen Proof-of-Concept, der die Umsetzung auf Basis eines konkreten Anwendungsfalls demonstriert. Die Entwicklung eines Proof-of-Concept dient der Bewertung und Abschätzung des zugrunde liegenden Technologiestacks sowie der hierfür benötigten funktionalen und nicht-funktionalen Prozesse.

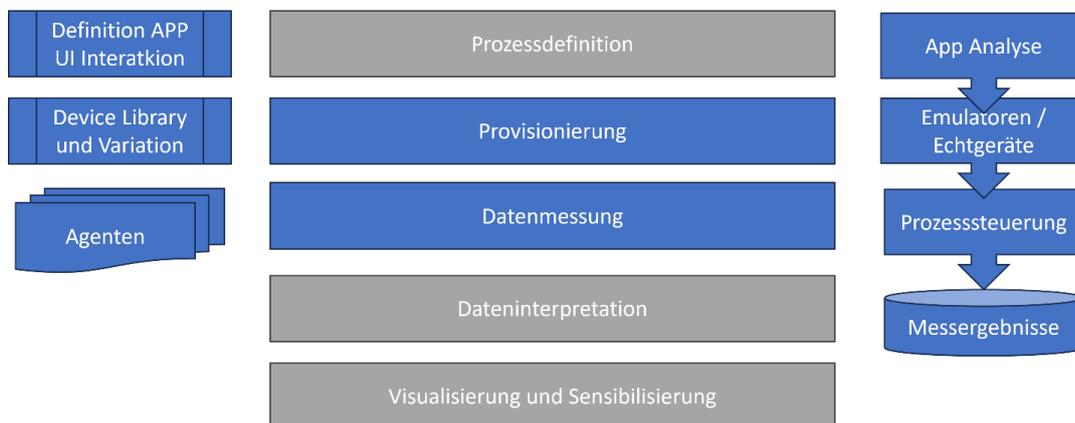


Abbildung 78: Schematische Übersicht über die PCS-Schwerpunktsetzung der Komponenten, die zur Realisierung einer prototypischen Datenerhebung auf Basis des Appium-Frameworks.

#### Prozessdefinition

Die Vorgehensweise startet idealerweise mit einer durch den Stakeholder definierten Testfallbeschreibung. Diese umfasst die Bereiche Anforderungsbeschreibung, Problemdefinition und Abgrenzung des zu beobachtenden Verhaltens in Textform sowie exemplarische Screenshots. Es ist von essenzieller Bedeutung, eine präzise Abgrenzung des Testfalls zu gewährleisten. Dies beinhaltet die exakte Beschreibung von Vor- und Nachbedingungen des zu beobachtenden Verhaltens sowie möglicher Variationen. Diese Informationen müssen in weiterer Folge in eine technische App-Analyse, Agenten-Definition, App-UI-Interaktion und Messsteuerung übersetzbar sein. Idealerweise wird die Prozessdefinition in einem gemeinsamen Workshop erarbeitet und zusätzlich eine begleitende Testfallaufzeichnung direkt in Appium durchgeführt.

Die Testfallaufzeichnung in Appium kann durch den Einsatz des Appium-Recorders erfolgen. Nach der Installation von Appium-Desktop wird der Appium-Server gestartet und eine Inspector Session initiiert. Dazu werden die „Desired Capabilities“ angegeben, eine vorhandene, geeignete Testumgebung ausgewählt und die Aufzeichnung gestartet. Die Interaktion mit der Applikation erfolgt dabei direkt auf dem

Emulator oder dem Echtgerät. Die Benutzeraktion, beispielsweise das Tippen auf Buttons, das Eingeben von Text, das Scrollverhalten und andere Benutzeraktionen, werden aufgezeichnet. Während der Interaktion mit der App zeichnet Appium die Aktionen auf und generiert automatisch das entsprechende Testskript, welches in weiterer Folge in der bevorzugten Programmiersprache (z. B. Java, Python, JavaScript) erstellt wird. Das nachträgliche Hinzufügen von Assertions oder Logik gewährleistet die vollständige Abbildung des Testfalls. Der Appium-Recorder stellt ein nützliches Werkzeug zur Aufzeichnung von Testfällen und deren Überführung in automatisierte Tests dar. Er unterstützt die Erstellung konsistenter und genauer Testskripte in Zusammenarbeit mit den Stakeholdern, wobei die Testfallbeschreibung interaktiv erstellt wird.

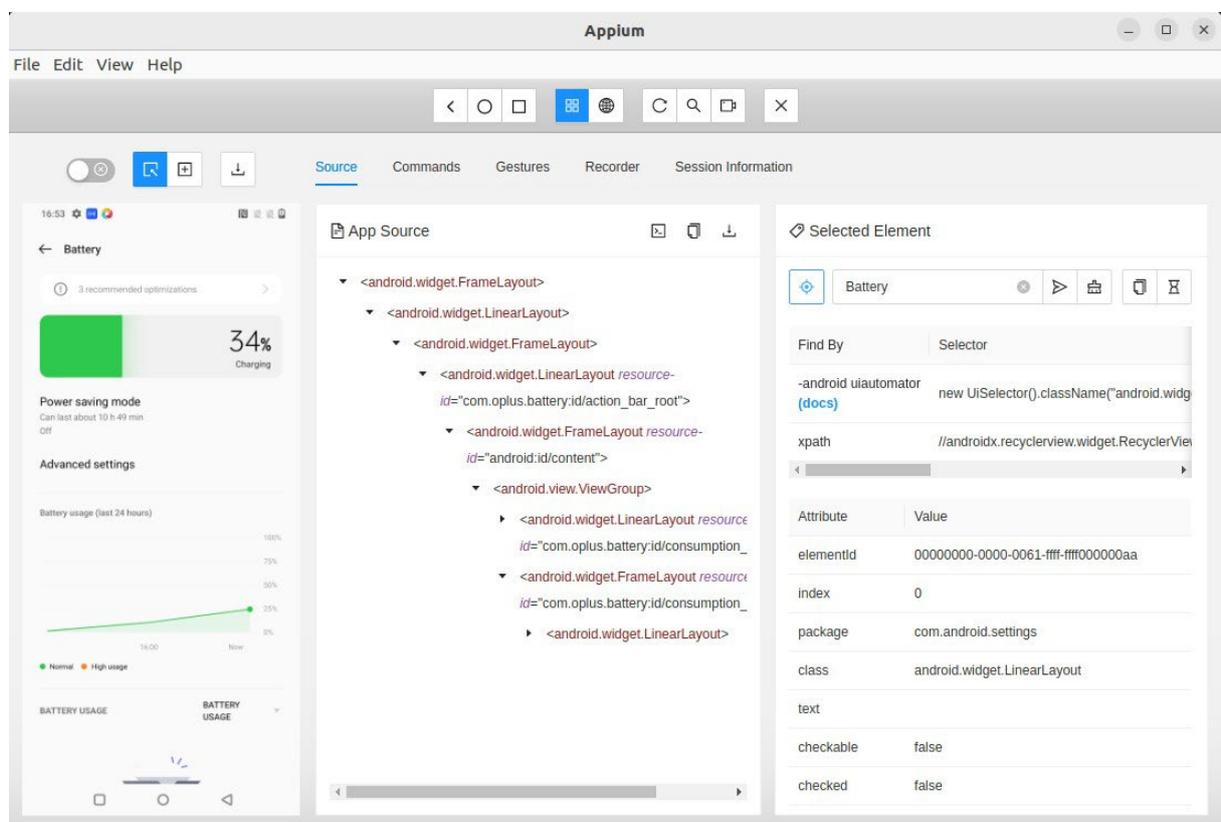


Abbildung 79: Auszug aus dem Appium-Inspector zur Analyse der Struktur & UI-Elementen der App.

Der in PCS aufgezeichnete Testfall beinhaltet das Login eines existierenden Temu-Users in die App. In weiterer Folge wurden „Assertions“ für das Vorhandensein von Countdown-Timern exemplarisch in der UI ausgewählt und unter Nutzung des Appium-Inspectors XPath-Ausdrücke definiert, welche die Definition aller sichtbaren Werte von Countdown-Timer ermöglichen. Ausgelesen wurden demnach alle Countdown-Timer auf der Produktstartseite, die unter zweimaligem Scrollen und Nachladen der Seite zu finden waren, sowie deren Werte zum Zeitpunkt der Messung, die Produkt ID und den Produkttitel.

Appium-Inspector stellt ein Werkzeug des Appium-Frameworks dar, welches zur Inspektion und Interaktion mit den Benutzeroberflächenelementen einer mobilen Anwendung zum Einsatz kommt. Es dient der Erfassung der Struktur der Applikation,

der Lokalisierung von Elementen sowie der effizienten Erstellung von Testfällen. Im Folgenden werden die Hauptfunktionen und Nutzungszwecke von Appium-Inspector dargelegt:

- **Elementinspektion und Attributanzeige:** Der Appium-Inspector erlaubt das Durchsuchen und die Inspektion der Hierarchie der Benutzeroberflächenelemente einer mobilen Anwendung. Dies umfasst alle UI-Elemente wie Buttons, Textfelder, Labels etc. Für jedes ausgewählte UI-Element zeigt der Appium-Inspector alle relevanten Attribute an, wie beispielsweise ID, Klasse, Text, Position, Größe und weitere Eigenschaften. Diese Informationen sind von entscheidender Bedeutung, um die Elemente im Testfall korrekt zu identifizieren, anzusprechen und auszulesen.
- **Automatisierte Generierungen:** Der Appium-Inspector generiert automatisch XPath-Ausdrücke und andere Lokatoren, wie beispielsweise ID, Name oder Accessibility ID, die in Testfällen verwendet werden können, um die Elemente eindeutig zu identifizieren oder alle Elemente mit bestimmten Eigenschaften zurückzuspielen.
- **Die Möglichkeit der Durchführung interaktiver Sitzungen:** Dies erlaubt eine Inspektion der Anwendung in Echtzeit. Dies impliziert, dass die App durchsucht, angeklickt und andere Aktionen ausgeführt werden können, um die Reaktion der Elemente zu beobachten.
- **Screenshot- und Quellcode-Anzeige:** Die vierte Funktion des Appium-Inspector umfasst die Erstellung und Anzeige von Screenshots der aktuellen Ansicht der Anwendung sowie die Möglichkeit, den Quellcode einer Seite zu durchsuchen.

Im gegenständlichen Einsatzgebiet, das die Übersetzung der Expert:innen Anforderungsdefinition sowie App-Analyse zur Erstellung geeigneter von Mess- und Testskripte für den Anwendungsfall erforderte, hat sich der Appium-Inspektor als wertvolles und unverzichtbares Tool erwiesen. Darüber hinaus war es im Zuge der Black-Box-Datenerhebung möglich auf Strukturänderungen in der Anwendung rasch zu reagieren, um zu eruieren, ob sich UI-Elemente tatsächlich geändert haben oder ob es sich um ein Debugging-Problem in der Testfallausführung handelt.

## Provisionierung

Appium ermöglicht das Starten und Interagieren mit sowohl Emulatoren als auch echten Geräten für automatisierte Abläufe in mobilen Anwendungen. Die Bereitstellung von Android-Emulatoren und/oder Echtgeräten stellt die Basis der Provisionierung zur Ausführung eines Appium-Testfalls dar. Zur Realisierung des PCS-Prototypen wurde das Open-Source-Framework Appium, Android Studio sowie die Google Android SDK-Tools in einer „Oracle Virtual Box“ (Ubuntu 22.04 LTS) konfiguriert. Die Android-Emulatoren (AVD) wurden mit dem AVD-Manager von Android Studio provisioniert. Der Start der Emulatoren kann über Android Studio oder direkt über die Kommandozeile (`$ emulator -avd <name_of_your_avd>`) erfolgen. Alternativ kann der Emulator auch direkt über Appium durch Angabe der „Desired Capabilities“ Konfiguration referenziert werden

Das Einrichten von Android-Echtgeräten erfordert das Aktivieren des Entwicklermodus und ein aktives USB-Debugging auf dem Zielgerät, sowie eine USB-Verbindung

(und Treiberinstallation) am Host-Computer. Über *adb devices* kann überprüft werden, ob das Gerät korrekt erkannt wird. ADB ist ein vielseitiges Werkzeug, das in Kombination mit Appium verwendet werden kann, um zusätzliche Steuerungs- und Debugging-Möglichkeiten zu bieten, dies umfasst etwa (*adb install /path/to/your/app.apk*) zum Installieren einer App oder (*adb shell am start -n <package\_name>/<activity\_name>*) zum Starten einer spezifischen Activity. Der Einsatz von ADB in Appium Skripten ist sehr nützlich, da ADB-Befehle direkt aus Appium-Testskripten ausgeführt werden können, um speziell komplexere Testszenarien zu realisieren. So wurde z. B. im PCS-Anwendungsfall die Temu APK direkt über *adb install* am Endgerät bereitgestellt, um diese in unterschiedlichen Versionen testen zu können.

Im Rahmen der Umsetzung traten folgende Schwierigkeiten auf: Android läuft in Virtualbox, allerdings lediglich als x86-Build von Android und nicht als nativer ARM-Build. Aufgrund der fehlenden Emulation eines ARM-Prozessors durch Virtualbox ist die Kompatibilität mit Android-Apps beeinträchtigt. Die Leistungsfähigkeit der in Virtual Box bereitgestellten Android-Emulatoren erwies sich als unzureichend. Der Umstand persistierte auch nach einem Upgrade auf Virtual Box 7 mit Support für Hardware-Emulation auf Intel-Prozessoren mit aktiviertem „Nested VT -x“-Support. In der Folge wurde versucht das „Android X86“-Emulator-Projekt als eigenständige VM über eine Netzwerkbrücke mit dem Android SDK Tools zu verbinden. Auch dieser Versuch musste aufgrund des mangelnden Community-Supports und des fortgeschrittenen Alters des Projekts (2022) als nicht realisierbar eingestuft werden.

Als Lösung wurde schließlich ein OnePlus 7T mit einem generischen Android-Treiber als Android-Echtgerät am Hostsystem angeschlossen und über die USB-Controller-Freigabe in Virtualbox an die ADB des virtuellen Systems bereitgestellt.

### Device Library und Variationen

Unter dieser Nomenklatur wurden zwei Begrifflichkeiten zusammengefasst, die für die Gewährleistung eines kontrollierten Experiment-Setups erforderlich sind: (1) die Verwaltung von vorhandenen provisionierten Geräten und Emulatoren sowie (2) die Auswahl und Zuordnung an Variationen und Fähigkeiten, die bei einem Messzyklus der Anwendung zum Einsatz kommen. Beispiele hierfür umfassen etwa:

- **Personas:** Die Bereitstellung von Personas (bestehend aus Username und Passwort, Appium Code-Skripten zum Login in die zu testende Applikation). Personas können darüber hinaus eine vorhandene Bestellhistorie oder personenbezogene Merkmale wie Name, Alter, etc. aufweisen, die im Kundenkonto hinterlegt und der Anwendung zur Verfügung gestellt werden.
- **Location:** Die Angabe einer Location in Appium ermöglicht es, den geografischen Standort des mobilen Geräts oder Emulators zu ändern, während die Datenerhebung ausgeführt wird. Dies ist insbesondere für das Testen von Funktionen von Vorteil, die von Standortdiensten abhängig sind, wie z. B. standortbasierte Benachrichtigungen.
- **App-Reset:** App-Reset legt fest, ob Daten wie existierende Logins zwischen Appium-Sitzungen gelöscht werden. Diese Funktionalität ist abhängig von der Konfiguration und dem verwendeten Gerät/Emulator. Appium bietet

verschiedene Konfigurationsmöglichkeiten, um den Zustand eines Geräts zu kontrollieren.

- **fullReset:** Diese Funktion sorgt dafür, dass die App deinstalliert und erneut installiert wird, und alle App-Daten gelöscht werden. Dies bedeutet, dass existierende Logins und andere Daten gelöscht werden.
- **noReset:** Diese Funktion sorgt dafür, dass die App-Daten (existierende Logins und andere Daten) zwischen den Sitzungen beibehalten werden.

Persona: A	Location: X	App Reset: fullReset
Persona: B	Location: X	App Reset: noReset
Persona: nein	Location: off	App Reset: fullReset

Eine weitere Variation in der Auswertung und Interpretation von Nudging spezifisch auf mobilen Geräten, nämlich die Analyse von Push-Benachrichtigungen (Nachrichteninhalt, Häufigkeit, etc.), wurde evaluiert. Aufgrund des fehlenden Supports des Appium Frameworks konnte diese jedoch nicht realisiert werden. Um Push-Benachrichtigungen auf einem Android-Gerät zu empfangen, müssen zunächst mehrere Voraussetzungen erfüllt werden: Aktivierung der Benachrichtigungsfunktion, Installation der Google Play-Dienste, Aktivierung der Google Play-Dienste, vorhandene Datenverbindung. Darüber hinaus muss die zu untersuchende App installiert und auf dem Gerät aktiv sein. Die Zustellung von Push-Benachrichtigungen ist in der Regel nicht möglich, wenn die App deinstalliert wurde, sich das Gerät im Ruhemodus befindet oder bestimmte Stromsparfunktionen aktiviert sind. Auf Android kann ein möglicher Workaround der fehlenden Appium-API-Unterstützung darin bestehen, die Benachrichtigungsleiste zu öffnen und Benachrichtigungen direkt zu überprüfen. Auf iOS hingegen sind zusätzliche Schritte und eventuell Drittanbieter-Bibliotheken erforderlich. Da die Analyse von Push-Nachrichten eine auf unbestimmte Zeit wartende Instanz der Testskript-Ausführung benötigt und zudem der fehlende Appium-API-Support gegeben ist, wurde von einer Umsetzung dieses Features Abstand genommen.

## Agenten

Als Standardinstanz wird ein Agent in der Konfiguration „Persona nein“, „Location off“ und „App fullReset“ als Baseline (Anonyme Messung) zur Datenmessung herangezogen. Weitere Instanzen können beliebig kombiniert und über die Device Library unter Vergabe einer eindeutigen ID hinzugefügt werden, sodass sie bei zukünftigen Ausführungen neuerlich zur Verfügung stehen. Das Deployment von Agenten umfasst die Modifikation des Testskripts zur Berücksichtigung der definierten Variationen (wie z. B. App UI Login vorab, das Setzen der Location) und stellt den hierfür benötigten Code im Testskript zur Verfügung. Agenten sind einem konkreten Emulator, bzw. einer Geräte Instanz zugewiesen, sodass die Datenmessung mit Echtgerät in unmittelbarer Abfolge, aber nie zeitgleich stattfand.

## Prozesssteuerung und Datenmessung

Die Prozesssteuerung definiert ein übersichtliches „command line interface“ in dem Agenten in regelmäßigen Intervallen zur Datenmessung eingesetzt werden. Die

extrahierten Messdaten werden in einem einheitlichen CSV-Interface übergeben. Die Middleware beinhaltet Funktionen der Ablaufsteuerung und ermöglicht es beispielsweise Prozesse zu terminieren.

Im Rahmen der prototypischen Umsetzung haben sich zwei weitere Tools als besonders nützlich erwiesen: (1) Appium-Doctor, ein Tool zur Sicherstellung einer korrekten Umgebungseinrichtung, sowie (2) der Appium Compatibility Builder, ein Tool, das Entwicklern und Testern dabei hilft, mobile Anwendungen auf verschiedenen Plattformen zu testen.

Der **Appium Compatibility Builder** bietet hierbei folgende Hauptfunktionen:

1. **Testkompatibilität:** Es hilft sicherzustellen, dass die durchgeführten Tests sowohl auf iOS- als auch auf Android-Plattformen kompatibel sind, indem es die notwendigen Anpassungen und Konfigurationen vornimmt.
2. **Konfigurationsmanagement:** Das Tool vereinfacht die Konfiguration der Testumgebung und die Verwaltung der verschiedenen Parameter, die für die Ausführung von Tests auf unterschiedlichen Geräten und Betriebssystemversionen erforderlich sind.
3. **Unterstützung der Automatisierung:** Es unterstützt die Automatisierung des Testprozesses durch die Generierung und Anpassung von Skripten, die dann von Appium ausgeführt werden können.
4. **Fehlerdiagnose:** Durch die Bereitstellung detaillierter Protokolle und Berichte hilft der Appium Compatibility Builder bei der Diagnose von Kompatibilitätsproblemen und Fehlern, die während des Testprozesses auftreten können.

Insgesamt zielt der Appium Compatibility Builder darauf ab, die Effizienz und Zuverlässigkeit des Testprozesses für mobile Anwendungen zu verbessern, indem eine einheitliche und kompatible Testumgebung geschaffen wird.

#### **Die Ergebnisse des Monitorings für den Anwendungsfall von Countdown-Timern auf Temu über einen Beobachtungszeitraum von einem Monat zeigen:**

(1) Das ursprünglich gewählte Element Selection-App-UI musste im Untersuchungszeitraum viermal angepasst werden, da die Countdown-Timer in der App fortlaufend verändert wurden und immer wieder neue Darstellungsvarianten entdeckt wurden, was ein Hauptproblem der Black-Box-Reverse-Datenerhebung darstellt. Darüber hinaus (2) zeigte die Datenanalyse, dass die präsentierten Produkte auf der Startseite stark variierten, so dass nur wenige überlappende Messdaten für den jeweiligen Countdown-Timer eines spezifischen Produktes in den Messdaten vorhanden waren. (3) Der Technologiestack erwies sich als nicht zuverlässig stabil, so dass ein manuelles Eingreifen/ Neustart mehrfach erforderlich war.

## 9.2 Vergleich der Komplexität von Appium und Selenium für Mobile Web Monitoring

Insgesamt ist der Appium-Stack aufgrund der Vielfalt und Komplexität der mobilen Plattformen und der Notwendigkeit, verschiedene Tools und Konfigurationen zu verwalten, deutlich komplexer als der Selenium-Stack, der sich auf reine Webbrowser-Interaktionen konzentriert.

- Appium: Entwickelt für die Automatisierung von mobilen Anwendungen (iOS und Android), einschließlich nativer, hybrider und mobiler Webanwendungen.
- Selenium: Entwickelt für die Automatisierung von Webanwendungen auf Desktop-Browsern.

**In Setup und Konfiguration:** Appium erfordert die Installation von *Node.js* und *npm*. Zur Bereitstellung der mobilen Plattformen werden Android SDK und AVD (Android Virtual Device) Manager (bzw. Xcode und Xcode Command Line Tools auf iOS) benötigt. Appium muss gestartet werden, um Testanforderungen zu akzeptieren, darüber hinaus müssen Emulatoren und physische Geräte konfiguriert und bereitgestellt werden. ADB ist notwendig für die Interaktion mit Android Geräten. „Desired Capabilities“ müssen für jede Testausführung spezifisch definiert werden z. B. *platformName*, *deviceName*, *app*. Selenium hingegen erfordert lediglich die Installation der Selenium-WebDriver-Bibliotheken für die gewünschte Programmiersprache. Die Treiber für den spezifischen Browser müssen heruntergeladen und konfiguriert werden.

**Bei der Testskripterstellung** müssen Appium-Testskripte speziell auf mobile Plattformen abgestimmt sein, mit Element-Lokalisierung basierend auf mobilen UI-Elementen (z. B. Accessibility-IDs oder XPath), zusätzliche Fähigkeiten werden durch Automatoren wie z.B. UiAutomator2 oder XCUITest bereitgestellt. Der UiAutomator2-Driver ist Teil des mobilen Testautomatisierungstools von Appium. Er arbeitet im Rahmen des W3C-WebDriver-Protokolls mit mehreren benutzerdefinierten Erweiterungen, um betriebssystemspezifische Szenarien abzudecken. So leitet der UiAutomator2-Driver die meisten Befehle an den UiAutomator2-Server weiter, der im Hintergrund das UiAutomator-Framework von Google verwendet. Einige Befehle werden direkt an *appium-adb* und andere Helper weitergeleitet, die auf den Tools der Android-Plattform basieren. Selenium hingegen legt den Fokus in den Testskripten auf Web-Elemente und Browser-Interaktionen (z. B. CSS-Selektoren, XPath) und bietet standardisierte Methoden zur Elementlokalisierung (z. B. *find\_element\_by\_id*)

**An Tools zum Debugging** ist der Appium-Inspector anzuführen, ein UI-Tool zur Interaktion und zum Inspizieren von UI-Elementen sowie zum Erstellen von XPath-Selektoren. ADB dient als Commandline-Tool zur Interaktion mit Android-Geräten (z. B. Installieren von Apps, Setzen von Standorten). Selenium bietet Browser Developer Tools und Selenium-DIE-Tools zum Inspizieren von Web-Elementen sowie zur einfachen UI-basierten-Testaufzeichnung an.

**Bezüglich der Wartung und Skalierbarkeit** weist Appium einen deutlich höheren Grad der Komplexität auf, die der Vielfalt an unterstützten mobilen Plattformen, Android-Betriebssystemversionen und Gerätekonfigurationen zuzuschreiben ist. Speziell der Faktor Skalierbarkeit erfordert typischerweise spezielle Setups sowie das

Zurückgreifen auf mobile Device-Farms oder Cloud-Dienste. Selenium hingegen besticht mit einer deutlich einfacheren Wartbarkeit da die Testumgebungen konsistenter und weniger variabel sind. Mit Selenium Grid können Testausführungen auf mehreren Browsern und Maschinen zugleich stattfinden.

**Begriffsdefinition** über die Appium-Komponenten und deren Zusammenspiel:

- **Client-Bibliotheken:** Testentwickler schreiben Tests in einer bevorzugten Programmiersprache und verwenden die Appium-Client-Bibliotheken, um mit dem Appium-Server zu kommunizieren.
- **Appium-Server:** Der Server empfängt die Anfragen und leitet sie an die Automatisierungs-Frameworks (z.B. UIAutomator2, XCUITest) weiter.
- **Automatisierungs-Frameworks:** Diese Frameworks interagieren direkt mit den mobilen Anwendungen und führen die Testaktionen aus.
- **Geräte und Emulatoren:** Die Tests werden auf physischen Geräten oder Emulatoren ausgeführt, die die Umgebung der Endbenutzer nachbilden.
- **Zusätzliche Tools:** Werkzeuge wie ADB und Xcode CLI Tools unterstützen bei der Interaktion und Verwaltung der Testgeräte.

### Zusammenfassung und Fazit

Der Appium-Technologie-Stack ist vielschichtig und umfasst eine Vielzahl unterschiedlicher Komponenten, die alle zusammenarbeiten müssen, um plattformübergreifende mobile Automatisierungstests zu ermöglichen. Von der Basisplattform Node.js über den zentralen Appium-Server bis hin zu spezifischen Automatisierungs-Frameworks und zusätzlichen Tools. Die Komplexität dieses Stacks erfordert ein gutes Verständnis der einzelnen Komponenten und deren Zusammenspiel, um effektive und zuverlässige Tests zu erstellen und durchzuführen.

Appium zeichnet sich durch einen deutlich höheren Initialaufwand in der Umsetzung eines Tools zum Monitoring von Informationen in mobilen Apps auf, welchem der Notwendigkeit geschuldet ist, mobile SDKs, Emulatoren/Echtgeräte und zusätzliche Tools installieren und konfigurieren zu müssen. Sofern unterschiedliche Plattformen, Geräte und Betriebssystemversionen von Relevanz sind, erhöht sich der Grad der Komplexität. Die Testausführungen müssen spezifisch auf mobile UI-Elemente und Interaktionen abgestimmt sein.

Selenium hingegen bedarf eines verglichen geringen Initialaufwand bei der Installation von WebDriver-Bibliotheken und Browser-Treibern. Webanwendungen sind in der Regel plattformübergreifend konsistenter, was die Testentwicklung und -wartung vereinfacht, darüber zeigt sich eine vereinfachte Testskripterstellung aufgrund der standardisierten Web-Elemente und Browser-Interaktionen.

Insgesamt ist der Appium-Stack, aufgrund der Vielfalt und Komplexität der mobilen Plattformen und der Notwendigkeit, verschiedene Tools und Konfigurationen zu verwalten, deutlich komplexer als der Selenium-Stack, sodass dem Monitoring von mobilen Websites zur Informationsextraktion und Bereitstellung der Datengrundlage zur Analyse und evidenzbasiertem Nachweis von Dark Patterns, insofern möglich gegenüber mobilen Apps, dem Vorzug zu geben ist. Dafür sprechen geringere Aufwände und Kosten für die benötigte Umsetzung neuer Agenten, die Integration neuer Features, die einfachere Adaption des Prozesses und des Interaktions-

monitorings bei Aufnahme neuer Plattformen sowie deutlich geringere Kosten für die langfristige Wartung und den Betrieb eines solchen Tools.

Während in PCS ein Proof-of-Concept zur strukturierten Datenerhebung in mobilen Apps unter Nutzung des Frameworks Appium entwickelt und dessen Anwendung erfolgreich auf dem Dark Patterns-Anwendungsfall der Countdown Timer in der Temu App gezeigt wurde, bieten Tools wie Selenium einen deutlich handhabbareren und schlankeren Technologiestack an, der sich zum Monitoring sowie zur Datenextraktion aus mobilen Webseiten eignet. Erfolgreich eingesetzt wurde dies z. B. im netidee-Forschungsprojekts „preis.wert“<sup>79</sup> sowie auch bei der Realisierung der größten deutschsprachigen datenbasierten Studie zum Marktplatz Amazon.de.<sup>80</sup>

---

<sup>79</sup> (netidee, 2018)

<sup>80</sup> (Beltzung et al., 2021)

## Impressum

### PCS – Platform Compliance Study

Version 1.0 – 30. September 2024, Wien, Österreich

### Österreichisches Institut für angewandte Telekommunikation (ÖIAT)

**Autor:innen:** Louise Beltzung, Julia Krickl, Irem Hölzl, Andrew Lindley

Das Projekt „Platform Compliance Studie – PCS“ wird gefördert bzw. finanziert im Rahmen des Programms KIRAS durch das Bundesministerium für Finanzen und von der Österreichischen Forschungsförderungsgesellschaft abgewickelt.



 Bundesministerium  
Finanzen



 Bundesministerium  
Arbeit, Soziales, Gesundheit  
und Konsumentenschutz

