API

OPEN ACCESS

Publiziert im Juli 2024
DOI: 10.15460/apimagazin.2024.5.2.208

Zeitschriftenartikel

Begutachtet

Begutachtet:

Dr. iur. Lutz Gollan
Landesbetrieb Verkehr
Hamburg
Deutschland

Erhalten: *16. Juni 2024*
Akzeptiert: *22. Juni 2024*
Publiziert: *11. Juli 2024*

Empfohlene Zitierung:

LEWJOHANN, Nele und LUIG, Charlotte, 2024: Dark Patterns und Privacy by Design. In: *API Magazin* **5**(2) [Online] Verfügbar unter: DOI 10.15460/apimagazin.2024.5.2.208

Dark Patterns und Privacy by Design

Nele Lewejohann[1]* und Charlotte Luig[1]*

[1] Hochschule für Angewandte Wissenschaften Hamburg, Deutschland
Studentinnen im 6. Semester des Studiengangs Bibliotheks- und Informationsmanagement

* Korrespondenz: redaktion-api@haw-hamburg.de

Zusammenfassung

Diese Arbeit befasst sich mit den Konzepten von Dark Patterns und Privacy by Design im Kontext des Datenschutzes. Dark Patterns sind manipulative Designmuster in digitalen Benutzeroberflächen, die Nutzer*innen zu unerwünschten Handlungen verleiten sollen. Verschiedene Formen dieser Muster werden erläutert und ihre Auswirkungen auf die Nutzererfahrung dargestellt. Privacy by Design hingegen betont die Integration von Datenschutzmaßnahmen von Anfang an in den Entwicklungsprozess digitaler Produkte. Der geschichtliche Hintergrund und die gesetzliche Verankerung in der DSGVO werden beleuchtet, ebenso wie die Herausforderungen bei der Umsetzung.

Schlagwörter: Dark Patterns, Privacy by Design, Datenschutz. DSGVO

Dark Patterns and Privacy by Design

Abstract

This paper addresses the concepts of Dark Patterns and Privacy by Design in the context of data protection. Dark Patterns are manipulative design patterns in digital user interfaces intended to lead users to actions now wanted by them. Various forms of these patterns are explained and their impact on the user experience is demonstrated. In contrast, Privacy by Design emphasizes the integration of data protection measures from the outset in the development process of digital products. The historical background and legal anchoring in the GDPR are examined, as well as the challenges in implementation.

Keywords: Dark Patterns, Privacy By Design, Data Protection, GDPR

DOI: 10.15460/apimagazin.2024.5.2.208

1 Einleitung

In einer zunehmend digitalisierten Welt gewinnt der Schutz personenbezogener Daten an Bedeutung. Datenschutz ist nicht nur eine rechtliche Verpflichtung für Unternehmen und Organisationen auf Grundlage der Datenschutz-Grundverordnung (DSGVO) der EU[1], sondern auch ein Grundrecht und ein grundlegendes Anliegen für die Privatsphäre und die Rechte der Verbraucher*innen. In diesem Kontext spielen Dark Patterns und Privacy by Design eine entscheidende Rolle, wenn es darum geht, ethische und transparente Standards im Umgang mit persönlichen Informationen sicherzustellen.

Diese Arbeit soll sich mit den Konzepten von Dark Patterns und Privacy by Design auseinandersetzen. Es wird herausgestellt, wie diese Konzepte in der Praxis angewendet werden und welche Auswirkungen sie auf die Nutzererfahrung haben. Darüber hinaus legen wir dar, wie Dark Patterns und Privacy by Design in Zusammenhang stehen und welche Rollen sie im Kontext des Datenschutzes spielen.

2 Dark Patterns

In diesem Kapitel wird zunächst der Begriff der Dark Patterns erläutert. Anschließend werden verschiedene Formen und Beispiele dargestellt, um das Phänomen besser zu veranschaulichen.

2.1 Begriffsbestimmung

Dark Patterns sind Designmuster, die in digitalen Benutzeroberflächen verwendet werden, um Nutzer*innen dazu zu bewegen, bestimmte Handlungen auszuführen, die möglicherweise ihren Interessen entgegenstehen, während diejenigen, die sie entwerfen, von einem Ungleichgewicht in der Gestaltungsmacht profitieren (Gertz und Martini o. D.). Der Begriff Dark Pattern wurde erstmals im Jahr 2010 von Harry Brignull eingeführt und hat sich seitdem durchgesetzt, wobei deutlich wird, dass es sich um „design patterns“ der „dark side of design“ handelt (Brignull 2010). Synonym werden u.a. auch die Begriffe „Deceptive Patterns“ (Brignull et al. 2023) oder „Manipulative Designs“ (Lehr et al. 2022) verwendet.

Bei einem User-Interface ist es unmöglich, eine gänzlich neutrale Entscheidungsarchitektur zu designen, da die Entwickler*innen immer eine eigene und persönliche Perspektive miteinbringen. Neben versehentlichem Beeinflussen gibt es aber die Dark Patterns, bei denen eine gezielte Beeinflussung zu Gunsten der Anbieter*innen vorgenommen wird (Gerber et al. 2023, S. 174). Man spricht von einem Dark Pattern, wenn der Nutzen der Anbieter*innen mehr im Fokus steht als das Ziel des

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/64/EG (Datenschutz-Grundverordnung) vom 27.04.2016, ABl. L 119, zuletzt geändert am 04.03.2021 [ELI: http://data.europe.eu/eli/reg/2016/679/oj].

DOI: 10.15460/apimagazin.2024.5.2.208

Users (Verbraucherzentrale NRW 2023). Diese Techniken werden oft eingesetzt, um Nutzer*innen dazu zu bringen, persönliche Informationen preiszugeben, unbeabsichtigt kostenpflichtige Dienste zu abonnieren oder bestimmte Aktionen auszuführen, die möglicherweise nicht in ihrem besten Interesse liegen. Sie treten fast ausschließlich in digitaler Umgebung auf und bisher gibt es keine näher definierten Ziel- oder Betroffenengruppen. Die provozierten Verhaltensweisen sind sehr unterschiedlicher Natur, vom Cookies-Akzeptieren bis hin zum Abschluss eines Kaufvertrags (Gertz und Martini o. D.). Da es keine eindeutige Definition des Begriffes gibt, ist es oft schwierig abzugrenzen, ab wann eine eingesetzte Technik einem Dark Pattern entspricht. Allgemein gilt: Die Nutzer*innen sollen in vielen Situationen von einer bestimmten Handlung überzeugt werden, und es stellt sich die Frage, wie viel davon hartnäckige Werbung ist und ab wann es zum Dark Pattern wird.

2.2 Formen und Beispiele

Es gibt unterschiedliche Kategorisierungsansätze, hier wird der Ansatz des interdisziplinären Verbundprojekts „Dark Pattern Detection Project“[2] verwendet, da dieser sehr differenziert ist. Dabei werden fünf verschiedene Wirkungsweisen herausgestellt, deren Grenzen allerdings nicht trennscharf sind (Gertz und Martini o. D.). Diese werden im Folgenden mit den zugehörigen Formen und einigen Beispielen erläutert.

2.2.1 Druck

Bei der *Dark-Patterns*-Gruppe „Druck“ werden Nutzer*innen dazu gedrängt, eine Handlung (schnell) vorzunehmen oder zu unterlassen, indem Druck aufgebaut wird (Gertz und Martini o. D.).

Confirmshaming

Beim *Confirmshaming* wird durch unterschiedliche Methoden versucht, Schuldgefühle auszulösen. Zum Beispiel nutzt die Sprachlern-App Duolingo eine Eule, die die Nutzer*innen durch traurige Emotionen beeinflusst, die tägliche Lektion zu absolvieren oder das Abonnement nicht zu kündigen, da sich bei den Nutzer*innen sonst ein schlechtes Gewissen bildet (Woellner 2022).

Scarcity

Das *Scarcity-Pattern* erweckt den Eindruck, dass ein Produkt oder eine Dienstleistung nur noch in begrenzter Menge verfügbar ist, obwohl dies möglicherweise nicht der Fall ist. Dies kann durch die Darstellung einer begrenzten Anzahl von verfügbaren Produkten visualisiert werden, um den Druck auf die Nutzer*innen zu erhöhen, schnell zu handeln (Gertz und Martini o. D.).

2 Siehe dazu: https://dapde.de/de/.

 DOI: 10.15460/apimagazin.2024.5.2.208

Countdowns

Ähnlich wie beim *Scarcity-Pattern* werden die Nutzer*innen auch hier unter Zeitdruck gesetzt, allerdings nicht durch eine begrenzte Anzahl, sondern durch einen Countdown, der suggeriert, dass ein Produkt o. ä. nur noch für eine begrenzte Zeit verfügbar ist. Ob dies tatsächlich der Fall ist, ist häufig nicht nachprüfbar (Gertz und Martini o. D.).

Nagging

Beim *Nagging* wird durch wiederholte und sehr penetrante Aufforderungen darauf abgezielt, dass die Nutzer*innen sich letztendlich aus Bequemlichkeit dazu entschließen, der Aufforderung nachzukommen, um das lästige Wegklicken zu vermeiden (Gertz und Martini o. D.). Ein Beispiel für *Nagging* ist Instagram. Die App hat das Pop-up zum Einschalten von Benachrichtigungen eine Zeit lang sehr häufig und lediglich mit den Auswahlmöglichkeiten „OK“ und „Not Now“ angezeigt, sodass keine endgültige Ablehnung möglich war (Gray et al. 2018, S. 5; Brignull et al. 2023).

Social Proof

Das *Social Proof-Dark Pattern* nutzt soziale Bewährtheit, indem positive Produktbewertungen oder Aktivitätsmeldungen anderer Nutzer*innen bzw. Käufer*innen direkt angezeigt werden. Dies kann durch echte oder gefälschte Bewertungen erfolgen, um die Kaufentscheidung der Nutzer*innen zu beeinflussen (Gertz und Martini o. D.).

2.2.2 Operativer Zwang

Bei diesen Dark Patterns werden die Nutzer*innen nicht mehr nur unter Druck gesetzt, eine bestimmte Handlung vorzunehmen, sondern dazu gezwungen, sofern sie ihrer ursprünglichen Intention nachgehen wollen (Gertz und Martini o. D.).

Forced Enrollment

Bei *Forced Enrollment* kann ein Dienst nur genutzt werden, wenn zuvor weitere Bedingungen akzeptiert werden, z. B. eine Anmeldung vorgenommen wird (Gertz und Martini o. D.).

Forced Continuity

Wenn eine Gratisversion o.ä. ausläuft und ohne Benachrichtigung eine kostenpflichtige Variante fortgeführt wird, die ggf. auch noch schwer zu kündigen ist, spricht man von Forced Continuity (Gray et al. 2018, S. 4).

Forced Review

Bei einem *Forced Review* kann ein Dienst nur genutzt werden, wenn zuvor Nutzungsbedingungen z.B. zum Datenschutz akzeptiert wurden (Gertz und Martini o. D.).

DOI: 10.15460/apimagazin.2024.5.2.208

2.2.3 Hindernisse

Diese Gruppe an *Dark Patterns* versucht, durch verschiedene Taktiken bestimmte Aktionen der Nutzer*innen zu verhindern (Gertz und Martini o. D.).

Roach Motel

Beim *Roach Motel-Pattern* kommt der Name von der Ähnlichkeit zu einer Insektenfalle: Der Einstieg ist unkompliziert, doch das Verlassen gestaltet sich äußerst schwierig. Z. B. kann die Anmeldung für eine Dienstleistung oder ein Abonnement online mit nur wenigen Klicks erfolgen, während die Kündigung nur durch viele, komplexe Umwege möglich ist (Gray et al. 2018, S. 6).

Price Comparison Prevention

Price Comparison Prevention versucht – wie im Namen angegeben – zu verhindern, dass Preise verglichen werden können, indem sich Produkt-IDs o. ä. nicht kopieren lassen oder Preise in unterschiedlichen Währungen oder für andere Einheiten angegeben werden (Gray et al. 2018, S. 6; Gertz und Martini o. D.).

Preselection

Bei diesem *Dark Pattern* ist bei einer Auswahl bereits eine Voreinstellung getroffen worden. Dies führt dazu, dass die Nutzer*innen diesem Kriterium eher zustimmen, als wenn sie es selbst auswählen müssten (Gray et al. 2018, S.7).

Hidden Information

Bei *Hidden Information* werden Informationen, die für die Nutzer*innen relevant sind, so dargestellt bzw. versteckt, dass die Nutzer*innen diese als irrelevant einstufen oder ganz übersehen (Gray et al. 2018, S.7).

Click Fatigue

Bei *Click Fatigue* wird die von den Anbieter*innen erwünschte Aktion durch einen deutlich kürzeren „Klickweg“ für die Nutzer*innen attraktiver gemacht. Dies findet sich häufig in Cookie-Einstellungen auf Webseiten wieder, bei denen die Zustimmung meist sehr einfach ist und die Ablehnung technisch nicht notwendiger Cookies häufig mehrere Klicks benötigt (Gertz und Martini o. D.).

2.2.4 Erschleichen

Bei dieser Gruppe an Dark Patterns werden den Nutzer*innen möglichst unbemerkt Zusatzleistungen aufgedrängt (Gertz und Martini o. D.).

Sneak into Basket

Das *Sneak-into-Basket-Pattern* bezieht sich wörtlich auf den Warenkorb, zu dem ein oder mehrere zusätzliche Produkte hinzugefügt werden, ohne dass diese von den Nutzer*innen ausgewählt wurden und somit versehentlich mitgekauft werden (Gray et al. 2018, S. 6).

 DOI: 10.15460/apimagazin.2024.5.2.208

Hidden Subscription

Bei der Hidden Subscription wird statt eines Produkts o. ä. ein ganzes Abonnement abgeschlossen, meist ohne dass die Nutzer*innen dies bemerken. So ist beispielsweise das Designtool Figma so gestaltet, dass ein Vertrag vereinbart wird, ohne dass es beabsichtigt war. Dies passiert, wenn Nutzer*innen die Funktion „Teilen eines Designs“ auswählen, damit ein*e Empfänger*in es bearbeiten kann. Für diese Person wird dann automatisch ein Abonnement abgeschlossen, ohne es entsprechend anzuzeigen. Die Kosten werden über die Zahlungsmethode der einladenden Kund*innen abgebucht (Brignull et al. 2023).

Hidden Cost

Es wird ein günstiger Preis suggeriert, zu dem allerdings noch einige Kosten hinzukommen, die bewusst erst am Ende des Bestellprozesses o.ä. angezeigt werden. Die Nutzer*innen sind aufgrund der bereits investierten Zeit eher bereit, diese zusätzlichen Kosten zu tragen. Diese Taktik wird häufig bei Ticketverkäufen angewandt, bei denen am Ende des Bestellprozesses zusätzlich hohe Servicegebühren hinzukommen (Brignull et al. 2023).

2.2.5 Irreführung

Irreführende Dark Patterns missbrauchen bewährte neutrale oder positive Design Patterns oder Erwartungen an die Benutzeroberfläche, um Nutzer*innen auf ungewollte Pfade zu lenken (Gertz und Martini o. D.).

Trick Question

Es werden Fragen gestellt, die durch doppelte Verneinungen oder andere missverständliche Formulierungen dazu führen, dass die Nutzer*innen unsicher sind, welche Antwort ihrer Intention entspricht, z. B. die Frage „Are you sure you want to cancel your account?“ mit den Antwortmöglichkeiten „Cancel“ oder „Continue“ (Woellner 2022).

Misdirection

Beim *Misdirection-Pattern* werden die Nutzer*innen durch eine psychologisch wirkende Farbgebung beeinflusst, z. B. auf einen bestimmten Button zu klicken (Woellner 2022).

Bait and Switch

Bait and Switch ist ein Dark Pattern, bei dem das Klicken auf eine bestimmte Schaltfläche oder ein Element in der Benutzeroberfläche zu einem anderen Ergebnis führt als erwartet. Typischerweise wird den Nutzer*innen eine Handlungsoption präsentiert, die eine bestimmte Funktion suggeriert oder eine bestimmte Erwartung weckt, jedoch führt die tatsächliche Interaktion zu einem anderen Ergebnis. Ein häufiges Beispiel ist das Klicken auf ein Element, das normalerweise eine bestimmte Aktion auslöst, wie das Schließen eines Fensters durch Klicken auf das „X“-Symbol. Im Fall

DOI: 10.15460/apimagazin.2024.5.2.208

von Bait and Switch könnte jedoch das Klicken auf das „X“-Symbol stattdessen eine unerwartete Handlung auslösen, wie beispielsweise das Starten eines unerwünschten Prozesses oder das Öffnen eines Pop-up-Fensters mit Werbung (Gertz und Martini o. D.).

3 Privacy by Design

In diesem Kapitel wird zunächst der Begriff der Privacy by Design erläutert. Anschließend werden verschiedene Prinzipien dargelegt und dargestellt, wie diese Prinzipien gesetzlich verankert sind und wo trotz gesetzlicher Grundlage weiterhin Schwächen für den Datenschutz liegen.

3.1 Begriffsbestimmung

Der Datenschutz soll das Grundrecht auf informationelle Selbstbestimmung aus Art. 8 Absatz 1 EU-Grundrechte-Charta und Art. 2 Absatz 1 und Art. 1 Absatz 1 Grundgesetz[3] vor übermäßigen Eingriffen schützen[4]. Privacy by Design ist ein Ansatz, bei dem Datenschutzmaßnahmen direkt von Beginn an bei der Entwicklung von digitalen Produkten berücksichtigt und integriert werden, sodass im späteren Gebrauch der Produkte der Datenschutz bestmöglich garantiert werden kann.

Eine Abgrenzung muss man zum Begriff Privacy by Default machen. Bei diesem Ansatz sollen die Voreinstellungen der digitalen Produkte im Hinblick auf die Privatsphäre der Nutzer*innen datenschutzkonform und nutzungsfreundlich eingestellt sein, sodass „nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden“ (Art. 25 Absatz 2 Satz 1 DSGVO). Die Nutzer*innen können bei der Nutzung dann noch eigene Einstellungen nach individuellen Wünschen treffen, z. B. bei den Cookie-Einstellungen. Die beiden Grundsätze werden häufig zusammen genannt und sind auch im selben Artikel 25 der DSGVO beschrieben.

Der geschichtliche Hintergrund für die Entwicklung von Privacy by Design lässt sich bis ins 20. Jahrhundert zurückverfolgen. Durch Listen der niederländischen Bevölkerung mit Religionszugehörigkeiten wurde es während der Besatzung den Nazis einfach gemacht, die jüdische Bevölkerung gezielt zu finden und zu verschleppen. Aus diesem Fehler heraus erkannte John Borking 1995 die Notwendigkeit, persönliche Daten auch technologisch zu schützen. Diese Idee wurde anschließend von Ann Cavoukian weiterentwickelt zum Prinzip Privacy by Design (Heesen et al. 2022, S. 173). Ann Cavoukian, die Datenschutzbeauftragte von Ontario, prägte den Namen des Grundsatzes Privacy by Design. Seit über zehn Jahren diskutiert Cavoukian die Wichtigkeit, Datenschutz von Anfang an in Entwicklungen mit einzubeziehen. Mitt-

3 Grundgesetz für die Bundesrepublik Deutschland in der Fassung vom 19.12.2022, BGBl. I, S. 2478.
4 Charta der Grundrechte der Europäischen Union vom 07.06.2016, ABl. C 202/389 [ELI: http://data.europe.eu/eli/treaty/char_2016/oj].

DOI: 10.15460/apimagazin.2024.5.2.208

lerweile ist Privacy by Design zu einem bekannten konzeptionellen Modell geworden (Cavoukian et al. 2010, S. 408). Dabei betont Cavoukian, dass hier eine Rechenschaftspflicht („accountability“) der handelnden Organisationen gemeint ist, und nicht lediglich eine einfache Verantwortung („responsibility“) der Verantwortlichen, die durch Privacy by Design umgesetzt werden soll (Cavoukian et al. 2010, S. 409).

3.2 Prinzipien

Bei der ersten Begriffsbestimmung im Jahr 2010 hat Ann Cavoukian sieben grundlegende Prinzipien herausgestellt (Cavoukian et al. 2010, S. 409f.):

1. Proactive not Reactive; Preventative not Reactive
Privacy by Design ist eine vorbeugende Maßnahme. Es wird also nicht darauf gewartet, dass ein negatives Ereignis eintritt, sondern bereits im Vorhinein präventiv gehandelt.

2. Privacy as the Default
Die Privatsphäre ist standardmäßig geschützt, d.h. auch wenn Nutzer*innen keine Aktion vornehmen, sind ihre Daten sicher.

3. Privacy Embedded into Design
Der Datenschutz wird von Beginn an in der Technikgestaltung der Anwendung eingebaut, um eine bestmögliche Funktion zu erreichen.

4. Full Functionality – Positive Sum, Not Zero-Sum
Anbieter*innen, die den Datenschutz der Nutzer*innen von Beginn an berücksichtigen, sollten keine Nachteile, sondern wie die Nutzer*innen ebenfalls Vorteile erfahren, sodass alle Beteiligten vom Datenschutz profitieren.

5. End-to-End Lifecycle Protection
Wenn *Privacy by Design* von Beginn an berücksichtigt wird, bevor die ersten Daten gespeichert werden, schützt dies die Daten während ihres Lebenszyklus von Anfang bis Ende.

6. Visibility and Transparency
Die Anbieter*innen legen großen Wert auf Sichtbarkeit und Transparenz, sodass sich die Nutzer*innen ohne Umstände über den Datenschutz informieren können.

7. Respect for User Privacy
Um *Privacy by Design* erfolgreich umsetzen zu können, müssen die Anbieter*innen den Datenschutz der Nutzer*innen respektieren und die Daten dementsprechend behandeln und verarbeiten.

 DOI: 10.15460/apimagazin.2024.5.2.208

3.3 DSGVO-Verankerung und Umsetzungsschwächen

Der Grundsatz *Privacy by Design* ist in der DSGVO der Europäischen Union verankert. Konkret wird *Privacy by Design* in Artikel 25 Absatz 1 der DSGVO erwähnt. Dieser Artikel trägt in der deutschen Fassung die Überschrift „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ und legt fest, dass sowohl bei der Gestaltung von Produkten als auch bei den Voreinstellungen in diesen Produkten der Schutz personenbezogener Daten berücksichtigt werden muss. Weitere Ausführungen zu den Grundsätzen und deren Zielen finden sich im Erwägungsgrund 78 der DSGVO. Vor allem in besonders sensiblen Bereichen, wie z. B. bei elektronischen Zahlungssystemen oder in sozialen Medien und sozialen Netzwerkdiensten, ist die gesetzliche Pflicht zur *Privacy by Design* sehr wichtig (Agentur der Europäischen Union 2019, S. 408, S. 432 und S. 436). Die Verankerung in der DSGVO ist zwar ein wichtiger „Schritt zur unionsweiten Kontrolle der Datenverarbeitung durch Technikgestaltung“ (Dix 2020, S. 261) und stellt ein Mittel zur Begrenzung von kontrollfreien Räumen und Sicherheitslücken in technischen Produkten dar (Dix 2020, S. 266), ist aber trotzdem noch keine ausreichende Lösung.

Unter *Privacy by Design* ist mehr zu verstehen als nur der Datenschutz durch Technikgestaltung. Es sollte umfassender gedacht werden. Nur in der deutschen Sprachfassung der DSGVO wird von der Technikgestaltung gesprochen, dabei sollte es keine Einschränkung auf die Technik geben, sondern der Datenschutz als integraler Bestandteil des gesamten Entwicklungsprozesses gelten und nicht nur in der Technikgestaltung (Hansen 2017, S. 9). Durch die DSGVO werden nur die Verantwortlichen in die Pflicht gezogen, nicht die (technischen) Designer*innen selbst, die für die konkrete Umsetzung zuständig sind (Dix 2020, S. 261), was unter anderem mit dazu führt, dass das Prinzip nicht konsequent durchgesetzt wird (Klumpp 2020, S. 516). Bei der Entscheidung für Produkte spielt der Datenschutz leider oft eine geringere Rolle als z. B. Preise und Optik, sodass „im Herstellerwettbewerb die optimale Lösung regelmäßig immer verliert“ (Klumpp 2020, S. 517). Auch ist der Grundsatz „(noch) zu wenig konkretisiert und ausgewogen“ (Steidle 2020, S. 281), es gibt keine genauen Vorgaben, wie das Prinzip umgesetzt werden soll und welche „Mittel“ erlaubt wären. Als einzig wirklich konkretes Beispiel wird die „Pseudonymisierung“ genannt, die aber natürlich keine allgemeingültige Lösung darstellt. Die Formulierung in Artikel 25 Absatz 1 DSGVO bietet zudem einige Schlupflöcher, da die Umsetzung an verschiedene Bedingungen geknüpft wird, z. B. an den Stand der Technik oder an Implementierungskosten. Dies könnte von den Verantwortlichen ausgenutzt werden, um eine fehlende Umsetzung zu rechtfertigen.

Im Digital Services Act der EU vom 19.10.2022[5] wird konsequenterweise den Anbieter*innen von Online-Plattformen inkl. Social Media in Artikel 25 Absatz 1 untersagt, ihre Online-Schnittstellen so konzipieren, organisieren oder betreiben, dass Nut-

5 Gesetz über digitale Dienste, VO (EU) 2022/2065, ABl. L 277/1.

DOI: 10.15460/apimagazin.2024.5.2.208

zer*innen getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden. Dies deckt sich inhaltlich weitestgehend mit den Vorgaben der schon länger bestehenden §§ 4a ff. des deutschen Gesetzes gegen den unlauteren Wettbewerb (UWG)[6], die u.a. aggressive Werbung oder Irreführung verbietet (Martini et al. 2021).

4 Fazit

Dark Patterns und Privacy by Design stehen in direktem Zusammenhang, da sie beide mit der Gestaltung von Benutzeroberflächen und dem Umgang mit personenbezogenen Daten in digitalen Produkten zu tun haben, jedoch auf unterschiedliche Weise. Dark Patterns beziehen sich auf Designentscheidungen, die darauf abzielen, Nutzer*innen irrezuführen oder zu manipulieren, um bestimmte Handlungen auszuführen. Dark Patterns stehen im Widerspruch zu den Prinzipien der Transparenz für die Nutzererfahrung. Privacy by Design hingegen ist ein Konzept, das darauf abzielt, bereits im Schritt der Entwicklung neuer (digitaler) Produkte, Datenschutz zu integrieren, statt ihn erst im Nachhinein als Ergänzung einzubauen. Da Privacy by Design auch in der DSGVO verankert ist, wird die Bedeutung der proaktiven Berücksichtigung von Datenschutzprinzipien hervorgehoben. Es zielt darauf ab, die Privatsphäre und die Kontrolle der Nutzer*innen über ihre eigenen Daten zu stärken.

Eine Herausforderung bei der Gestaltung digitaler Produkte besteht darin, Dark Patterns zu vermeiden und stattdessen Privacy-by-Design-Prinzipien zu implementieren, um sowohl die Privatsphäre der Nutzer*innen zu respektieren als auch eine ethische und vertrauenswürdige Benutzererfahrung sicherzustellen. In einer idealen Umgebung sollten Designentscheidungen darauf abzielen, die Privatsphäre zu schützen und gleichzeitig eine klare, transparente und nutzungsfreundliche Erfahrung zu bieten. Mithilfe von Privacy by Design kann so das Vertrauen der Nutzer*innen in das Produkt sowie die Zufriedenheit mit dem Produkt gestärkt werden, was wiederum den Ruf der Anbieter*innen verbessern bzw. auch die Nutzungszahlen steigern kann. In diesem Sinne ist der Einsatz von Privacy-by-Design-Prinzipien das Gegenteil zum Einsatz von Dark Patterns. Wenn diese von Beginn an berücksichtigt werden, sind Dark Patterns unwahrscheinlicher und schwieriger umzusetzen.

6 Gesetz gegen den unlauteren Wettbewerb in der Fassung vom 03.03.2010, BGBl. I, S. 254.

DOI: 10.15460/apimagazin.2024.5.2.208

Literatur

AGENTUR DER EUROPÄISCHEN UNION FÜR GRUNDRECHTE, EUROPARAT, EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER, EUROPÄISCHER GERICHTSHOF FÜR MENSCHENRECHTE, 2019. *Handbuch zum europäischen Datenschutzrecht* [online]. Ausgabe 2018. Luxemburg: Amt für Veröffentlichungen der Europäischen Union. ISBN 978-92-871-9848-8. Verfügbar unter: https://op.europa.eu/s/w3MS

BRIGNULL, Harry, 2010. *Dark Patterns* [online]. Dirty tricks designers use to make people do stuff. Brighton & London: Harry Brignull, 08.07.2010 [Zugriff am: 11.04.2024]. Verfügbar unter: https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/

BRIGNULL, Harry, LEISER, Mark, SANTOS, Cristiana und DOSHI, Kosha, 2023. *Deceptive Patterns* [online]. User interfaces designed to trick you. Eastbourne: Deceptive Patterns, 25.04.2023 [Zugriff am: 11.04.2024]. Verfügbar unter: https://www.deceptive.design/

CAVOUKIAN, Ann, TAYLOR, Scott und ABRAMS, Martin E., 2010. Privacy by Design [online]. Essential for organizational accountability and strong business practices. In: *Identity in the Information Society*, 3(2), S. 405-413. [Zugriff am 11.04.2024] Identity in the Information Society. DOI: 10.1007/s12394-010-0053-z

DIX, Alexander, 2020. Gerät die Datenverarbeitung außer Kontrolle? In: HENTSCHEL, Anja, HORNUNG, Gerrit und JANDT, Silke, Hrsg. *Mensch - Technik - Umwelt: Verantwortung für eine sozialverträgliche Zukunft.* Festschrift für Alexander Roßnagel zum 70. Geburtstag. Baden-Baden: Nomos Verlagsgesellschaft GmbH & Co. KG, S. 243-266. ISBN 9783748910770.

GERBER, Nina, STÖVER, Alina und MARKY, Karola, Hrsg., 2023. *Human Factors in Privacy Research*. Cham: Springer. ISBN 9783031286438.

GERTZ, Michael und MARTINI, Mario, o. D. *Dark Pattern Detection Project - Dapde* [online]. Speyer: Deutsches Forschungsinstitut für öffentliche Verwaltung, o. D. [Zugriff am: 10. April 2024]. Verfügbar unter: https://dapde.de/de/

GRAY, Colin M., KOU, Yubo, BATTLES, Bryan, HOGGATT, Joseph und TOOMBS, Austin L. 2018. The Dark (Patterns) Side of UX Design. In: MANDRYK, Regan, HANCOCK, Mark, PERRY, Mark und COX, Anna, Hrsg. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, S. 1-14. ISBN 9781450356206.

DOI: 10.15460/apimagazin.2024.5.2.208

HANSEN, Marit, 2017. "Datenschutz durch Gestaltung" [online]. Der Artikel 25 der Datenschutz-Grundverordnung. In: *BvD-News - Das Fachmagazin des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e. V.* [online]. 2017(2), S. 8-10. [Zugriff am: 4. Mai 2024]. BvD-News - Das Fachmagazin des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e. V. ISSN: 2194-1025. Verfügbar unter: https://www.bvdnet.de/wp-content/uploads/2017/08/BvD-News_2_2017_web.pdf

HEESEN, Jessica, AMMICHT QUINN, Regina, BAUR, Andreas, HAGENDORFF, Thilo und STAPF, Ingrid, 2022. Privatheit, Ethik und demokratische Selbstregulierung in einer digitalen Gesellschaft. In: ROSSNAGEL, Alexander und FRIEDEWALD, Michael, Hrsg. *Die Zukunft von Privatheit und Selbstbestimmung. Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt*. Wiesbaden: Springer Vieweg, S. 161-187. ISBN 9783658352639.

KLUMPP, Dieter, 2020. Digitalordnung: Privacy by Design, by Default oder per Digitalsouveränität? In: HENTSCHEL, Anja, HORNUNG, Gerrit und JANDT, Silke, Hrsg. *Mensch - Technik - Umwelt: Verantwortung für eine sozialverträgliche Zukunft*. Festschrift für Alexander Roßnagel zum 70. Geburtstag. Baden-Baden: Nomos Verlagsgesellschaft GmbH & Co. KG, S. 509-524. ISBN 9783748910770.

LEHR, Franz, DIETMANN, Heike, KRISAM, Chiara und VOLKAMER, Melanie, 2022. Manipulative Designs von Cookies [online]. Manipulative Designs von Cookies Tricks, um die Einwilligung von Website-Besucherinnen und -Besuchern zum Sammeln und Auswerten von Nutzerdaten über Cookies zu erhalten. In: *Datenschutz und Datensicherheit - DuD*, 46(5), S. 296-300. Datenschutz und Datensicherheit - DuD. ISSN: 1862-2607. Verfügbar unter: Doi: 10.5445/IR/1000146420

MARTINI, Mario, DREWS, Christian, SEELIGER, Paul und WEINZIERL, Quirin, 2021. Dark Patterns. Phänomenologie und Antworten der Rechtsordnung. In: *Zeitschrift für Digitalisierung und Recht* [online]. 2021(47), S. 49-74 München: Verlag C.H.Beck oHG [Zugriff am 22.06.2024]. Verfügbar unter: https://www.uni-speyer.de/fileadmin/Lehrstuehle/Martini/2021_Dark_patterns__zfdr_mit_Weinzierl_Seeliger_Drews_S_74ff.pdf

STEIDLE, Roland, 2020. Digitalisierung und Personenbezug. Thesen zur Weiterentwicklung des Datenschutzrechts in einer digitalen Welt. In: HENTSCHEL, Anja, HORNUNG, Gerrit und JANDT, Silke, Hrsg. *Mensch - Technik - Umwelt: Verantwortung für eine sozialverträgliche Zukunft*. Festschrift für Alexander Roßnagel zum 70. Geburtstag. Baden-Baden: Nomos Verlagsgesellschaft GmbH & Co. KG, S. 267-288. ISBN 9783748910770.

DOI: 10.15460/apimagazin.2024.5.2.208

VERBRAUCHERZENTRALE NRW, 2023. *Dark Patterns* [online]. So wollen Websites und Apps Sie manipulieren. Düsseldorf: Verbraucherzentrale NRW e.V., 04.12.2023 [Zugriff am: 10.04.2024]. Verfügbar unter: https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste/dark-patterns-so-wollen-websites-und-apps-sie-manipulieren-58082

WOELLNER, Sally, 2022. Dark Patterns. How design seeks to control us. In: *YouTube* [online]. 06.02.2022 [Zugriff am 11.04.2024]. Verfügbar unter: https://www.youtube.com/watch?v=lJUW0iZzAaQ