FELDM

Dr. phil. Ramona Greiner

Dark Patterns im Consent Management – und warum Sie darauf verzichten sollten

Tl;dr

- Dark Patterns sind manipulative Designelemente. Im Consent Management werden diese immer häufiger eingesetzt, um möglichst hohe Opt-In-Raten zu erzielen.
- Die häufigsten Dark Patterns im Consent Management zielen auf Irreführung ab oder machen einen Opt-Out unnötig langwierig und kompliziert.
- Eine Trennlinie zwischen zulässigem Nudging und unzulässigen Dark Patterns ist nicht immer klar zu ziehen. Meistens unterscheiden sich die beiden im Grad der Manipulation, dem Druck, mit dem eine bestimmte Handlung bei den Nutzer:innen angeregt wird, und der Intention bzw. dem Ergebnis.
- Es gibt noch(!) kein explizites "Dark Pattern-Gesetz", aber einige Regelungen, die bereits Anwendung finden können.
- Der Einsatz von Dark Patterns beim Consent Management verringert auch die Barrierefreiheit Ihrer Website.
- Consent Management sollte als eine vertrauensbildende Maßnahme in der Kundenbeziehung verstanden werden. Dark Patterns hingegen schaffen Intransparenz und Misstrauen.

Verkaufspsychologie 2.0: Was sind Dark Patterns?

Der Begriff „Dark Patterns" geht zurück auf einen Artikel des UX-Designers und Webentwicklers Harry Brignull aus dem Jahr 2010. Hierin beschrieb er Benutzeroberflächen, die mit großer Sorgfalt und einem fundierten Verständnis der menschlichen Psychologie darauf ausgelegt sind, Nutzer:innen dazu zu bringen, bestimmte Handlungen auszuführen, die deren eigentlichen Interessen entgegenlaufen.[1]

Dass Konsument:innen beeinflusst werden, ist natürlich nicht neu und in der analogen Welt genauso zu finden; man denke nur an die "Quengelware" in der Nähe von Supermarktkassen, die die wartenden Kinder anstiftet, die Eltern so lange zu nerven, bis der Schokoriegel doch noch im Wagen landet. Auch das Arrangieren von höherpreisigen Produkten auf Augenhöhe im Regal und das "Verstecken" der günstigeren Alternativen in Bodennähe sind letztlich manipulative Techniken.
Ist es also ganz normale Verkaufspsychologie, wenn Consent-Banner so gestaltet werden, dass Nutzer:innen der Datenerhebung und -verarbeitung fast nur zustimmen können? Leider nein. Die DSGVO gibt ganz klare Vorgaben an die Hand, wie die Einwilligung zu erfolgen hat, nämlich vor allem freiwillig und informiert. In dem Moment, in dem Nutzer:innen aufgrund von manipulativen Dark Patterns zustimmen, haben wir ein datenschutzrechtliches Problem und es zeichnet sich ab, dass das Thema künftig noch mehr Aufmerksamkeit und Regulierung bekommt: Zahlreiche Initiativen befassen sich derzeit mit Dark Patterns. Sie wollen dem Thema dadurch zu mehr Sichtbarkeit sowie den Nutzer:innen zu mehr Awareness und Privacy Literacy verhelfen. Ein Beispiel ist das interdisziplinäre Dark Pattern Detection Project, an dem mehrere Universitäten beteiligt sind. Ebenso gab es bereits 2019 einen Gesetzesentwurf in den USA, der Dark Patterns sowie A/B-Tests verbieten sollte und gemeinsam von Demokraten und Republikanern eingebracht, jedoch nie verabschiedet wurde – im

[1] Vgl. Brignull, H. (2010). 90 Percent of Everything.Dark Patterns: dirty tricks designers use to make people do stuff.

Gegensatz zum 2019 verabschiedeten California Consumer Privacy Act (CCPA), welcher bestimmte Formen von Dark Patterns bereits untersagt. Ein Verbot von Dark Patterns im WebDesign wird von verschiedenen Stellen, z.B. der EU-Kommission in ihrer New Consumer Agenda gefordert und wird vermutlich auch Eingang in kommende Gesetze wie den Digital Services Act der EU finden – nicht zuletzt Deutschland setzt sich dafür ein.

(Er-)Kenne deinen Feind: Dark Patterns im Consent Management

Damit Sie Dark Patterns bei der Gestaltung Ihres Cookie-Banners vermeiden können, müssen Sie wissen, welche es gibt und wo Ihre Alarmglocken schrillen sollten. Im Consent Management sind es vor allem die Folgenden, die häufig eingesetzt werden.

Deliberate Misdirection (= Bewusste Irreführung)

Das Misdirection-Dark Pattern lenkt durch auffällige grafische Elemente vom Inhalt ab und ist wohl das klassischste Dark Pattern, wenn es um die Gestaltung von Buttons geht. Der Einsatz dieses Dark Patterns im UX-Design hat den Zweck, die Aufmerksamkeit der Nutzer:innen von einem Inhalt auf einen anderen zu lenken. Wenn Nutzer:innen eine Entscheidung zwischen zwei Optionen wählen sollen, ist meist die Option grafisch besonders hervorgehoben, die dem Interesse des Website-Betreibers entspricht. Dabei wird sowohl mit schlichter Signalwirkung und Auffälligkeit, aber auch mit Farbpsychologie gearbeitet. Wo hier ein Nudging aufhört und ein Dark Pattern beginnt, muss im Einzelfall entschieden werden, wie im nächsten Kapitel noch genauer erläutert wird.

Wenn bei zwei gleichwertigen Buttons der eine kräftig grün ist und der andere etwas heller, würde man sicher von Nudging sprechen. Wenn der zweite Button jedoch so stark ausgegraut ist, dass man ihn kaum noch erkennen kann, ist es vermutlich bereits ein Dark Pattern. Ebenso ist es als Dark Pattern zu werten, wenn die zweite, für den Website-Betreiber ungünstige Option, gar nicht als Button auftaucht, sondern nur im Fließtext zu finden ist.

Abb. 1.: Beispiele für Deliberate Misdirection im Bereich Consent.

Im linken Beispiel (vgl. Abb. 1) sieht man deutlich, dass der Nutzer:innenwille durch die Gestaltung manipuliert wird: "Grün" wird mit "Nummer Sicher" assoziiert und der starke Kontrast lenkt die Aufmerksamkeit sofort auf diesen Button. Im rechten Beispiel sehen wir nicht nur die deutliche Hervorhebung, sondern werden auch durch den Text getäuscht. Wer auf einen Link klickt, im Willen, sich von einem Service abzumelden oder eine Einwilligung zu widerrufen, geht davon aus, dass die vorausgewählte bzw. hervorgehobene Option dem auch entspricht. Die grafisch naheliegende Option ist hier jedoch der Abbruch des Widerrufs. Das wird aber nur deutlich, wenn man genau liest, denn das "Abbrechen" im hervorgehobenen Button erweckt kurz den Eindruck, als würde man damit die Einwilligung "abbrechen". Tatsächlich würde man aber den Widerruf abbrechen und den wirklichen Widerruf nur per Klick auf den Textlink unterhalb des Buttons vollziehen können.

Forced Enrollment/Action/Consent (= Erzwungene Einwilligung)

Forced Enrollment zwingt Sie zur Akzeptanz von bestimmten Bedingungen, um einen Dienst nutzen zu können, obwohl Ihre Zustimmung für die Erbringung des Dienstes eigentlich nicht erforderlich wäre.
Hier befinden wir uns im Bereich des Consent Managements nicht nur in einer moralisch fragwürdigen Situation, sondern auch rechtlich. Die Freiwilligkeit bzw. die Wahlfreiheit ist Kern der datenschutzrechtlichen Einwilligung. Sie verlangt, dass den Betroffenen die Wahl gelassen wird: Möchten Sie die Datenverarbeitung oder nicht? Dabei sollten Ihnen im Falle der Ablehnung keine Nachteile entstehen. Grundlage dafür ist das datenschutz- sowie das wettbewerbsrechtliche Kopplungsverbot. Das heißt, die Erbringung einer Leistung darf nicht an die Bereitstellung von Daten oder die Einwilligung zur Nutzung von Daten zu Zwecken, die für die Leistungserbringung nicht erforderlich sind, gekoppelt werden.

Im Bereich Medien gibt es hier eine Sonderregelung, die es Onlineangeboten von Nachrichtenmedien ermöglicht, den Zugang zu den journalistischen Inhalten zu verhindern, bis eine Option ausgewählt ist: Ein Abonnement, also ein finanzielles Entgelt, oder man stimmt der Datennutzung zu und "zahlt" mit seinen Daten, die den Qualitätsmedien wiederum die Existenz sichern können. Diese Vorgehensweise ist derzeit Gegenstand mehrerer Beschwerden der Datenschutzorganisation noyb bei verschiedenen deutschen Aufsichtsbehörden.

Bei Websites, die sich nicht zum Medienbereich zählen lassen, wird es kritisch. Dürfen Sie Ihren Kund:innen die Angebote auf Ihrer Website vorenthalten, wenn erstere einer Datenverarbeitung nicht zustimmen? Die relevante Regelung hierzu findet sich in Art. 7 Abs. 4 DSGVO, die jedoch nicht explizit einer Nutzungsverweigerung widerspricht – insofern es sich nicht um die Erfüllung eines Vertrages handelt. Ob Sie als Website-Betreiber hier eine Art Hausrecht haben oder nicht, wird von verschiedenen Jurist:innen unterschiedlich beurteilt. Hier müssen Sie mit Ihrer Rechtsabteilung eine Entscheidung treffen. Wenn Sie jedoch ein vertrauensvolles Verhältnis zu Ihren Website-Besucher:innen haben wollen und diesen überhaupt die Chance geben wollen, etwa in Ihrem Online-Shop einzukaufen, sollten Sie von diesem Dark Pattern dringlichst absehen.

Confirmshaming (= Einwilligung durch Bloßstellen)

Beim Confirmshaming findet die Manipulation erneut auf textlicher Ebene statt. Die Option, die der Manipulierende vermeiden möchte, ist so formuliert, dass die Benutzer:innen sich nicht mit der Aussage auf dem Button identifizieren wollen und daher die andere Option wählen. Dieser Typ von Dark Patterns löst bei den Nutzer:innen bewusst ein schlechtes Gefühl aus, sollten sie nicht im Sinne des Anbieters handeln. Ein klassisches Beispiel aus dem eCommerce-Bereich ist die Newsletter-Anmeldung, die einen 20%-Rabatt gewähren kann, bei welcher der Ablehnen-Button oder die Ablehnen-Tick-Box jedoch mit „Nein danke, ich möchte nicht sparen. Ich habe genug Geld." beschriftet ist.

Im Consent Management begegnen uns Confirmshaming-Buttons immer häufiger. Die Bandbreite des Shamings reicht dabei von schwach bis sehr deutlich.

Beispiele:

- "Nein, ich möchte keine personalisierten Angebote."
- "Nein, ich will anonym bleiben."
- "Nein, ich will keine besseren Angebote bekommen."
- "Nein, ich möchte Ihnen nicht bei der Optimierung Ihrer Website helfen."
- "Nein, ich habe etwas zu verbergen."
- "Nein, meine Daten gehen Sie gar nix an!"
- "Nein, Premium-Service ist nichts für mich. Ich will nur das Standardangebot."

Sie sehen, dass es schwerfällt, sich mit den meisten der Aussagen zu identifizieren, weshalb der Klick zu "Ja, ich will den besten Service" plötzlich viel attraktiver wirkt und Sie damit der Datenerhebung und -verarbeitung zustimmen.

Roach Motel (= "Kakerlaken-Falle")

Das Roach Motel macht es den Nutzer:innen möglichst einfach, in eine für den Anbieter günstige Situation zu kommen und erschwert es, diese wieder zu verlassen. Wir kennen das von Mobilfunkverträgen oder Zeitungsabonnements, die mit einem Klick geschlossen werden können, das Beenden aber nur über mühsame, oft postalische Wege oder Anrufe zu vollziehen ist.
Das Datenschutzrecht sieht vor, dass gegebener Consent schnell und so einfach wie er erteilt wurde wieder zurückgenommen werden können muss. Doch das gestaltet sich in der Realität häufig anders: Wenn man einmal auf "Akzeptieren" geklickt hat, ist es meist schwer, den Weg zu den Einstellungen wiederzufinden. Häufig muss man ans untere Ende der Seite scrollen, die Datenschutzhinweise aufrufen und hoffen, dass man dort direkt die Einstellungen anpassen kann. Mitunter ist der Link zu den Einstellungen aber auch im Fließtext der Datenschutzerklärung versteckt und muss mühsam innerhalb der riesigen Texttapete gefunden werden – hier würden wir bereits von einem Roach Motel sprechen.

Click Fatigue (= Klick-Ermüdung)

Dieses Dark Pattern funktioniert, weil wir grundsätzlich eher klick-faul sind und, vor allem wenn wir eine bestimmte Seite aufrufen wollen, auch ungeduldig. Daher werden die Klickwege zu verschiedenen Optionen unterschiedlich lang gestaltet, damit Nutzer:innen eher die schnelle und einfache Variante wählen als die, die sie durch mehrere Untermenüs navigiert.
Wir wissen alle, dass wir Cookies schnell und einfach akzeptieren können – meist nur durch einen einzigen Klick. Die Alternative heißt oft "Einstellungen" und man wird auf eine weitere Ebene geleitet, die vor Texten, Untermenüs und weiterführenden Links sowie zahlreichen Toggle-Optionen nur so strotzt.
Eine Beschränkung auf die erforderlichen Cookies kann daher meist nur durch mehrere Klicks erreicht werden, was gerade die in der DSGVO geforderte Freiwilligkeit und aufgrund der Unübersichtlichkeit auch die Informiertheit in Frage stellt und daher auch zu rechtlichen Konsequenzen führen kann.

Preselection (= Vorauswahl)

Das Preselection-Dark Pattern nimmt eine freiwillige (wenn auch abänderbare) Vorauswahl zwischen verschiedenen Möglichkeiten vorweg und agiert dabei so gut wie immer im Sinne des Website-

Betreibers und nicht im Sinne des zu schützenden Individuums. Aus dem Online-Shopping kennt man das Pattern, wenn beispielsweise eine wiederkehrende Lieferung vorausgewählt ist, was beim vermeintlich einmaligen Bestellvorgang übersehen werden kann. Doch auch im Consent Management war dieses Dark Pattern zunächst weit verbreitet. Besonders das Planet49-Urteil des EuGH bzw. die Cookie-II-Entscheidung des BGH hat dem einen deutlichen Riegel vorgeschoben und in diesem Fall auch Rechtssicherheit gebracht. Das BGH-Urteil setzt die Vorgaben des EuGH um und endet mit dem eindeutigen Satz: "Der Gerichtshof der Europäischen Union hat auf Vorlage durch den Senat auch mit Blick auf Art. 4 Nr. 11 der Verordnung (EU) 2016/679 entschieden, dass ein vom Nutzer abzuwählendes, voreingestelltes Ankreuzkästchen keine wirksame Einwilligung darstellt." Damit ist ein Vorankreuzen keine Einwilligung und wenn sie als solche genutzt wird, drohen rechtliche Konsequenzen.

Hidden Information (= Versteckte Informationen)

Dieses Dark Pattern macht relevante Informationen nur schwer zugänglich, indem es entweder Click Fatigue nutzt und die Informationen in komplexen Untermenüs unterbringt oder sie ganz versteckt. Letzteres geschieht über sehr kleinen oder ausgegrauten Text, winzige Fußnoten oder sogar über Benutzerelemente, die überhaupt erst sichtbar werden, wenn man mit der Maus zufällig über einen unauffälligen Bereich hovert (vgl. Abb. 2 und Abb. 3). Auch hier droht die Abmahnung, da von einer nach DSGVO-Anforderungen wirklich informierten und freiwilligen Einwilligung nicht gesprochen werden kann. Die entscheidenden Informationen müssen einfach zugänglich sein.

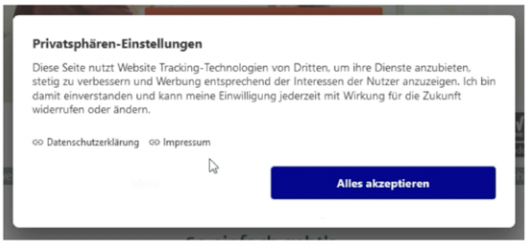

Abb. 2.: Kein Button zum Ablehnen oder für weitere Einstellungen sichtbar.

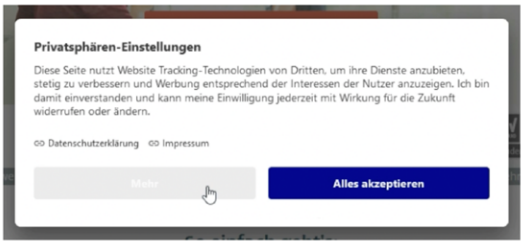

Abb. 3.: Erst wenn der Mauszeiger in den relevanten Bereich kommt, erscheint ein Button mit der Bezeichnung "Mehr".

Nagging (= Nörgelei)

Auf unsere Ungeduld beim Besuch einer Website zielt auch das Nagging-Dark Pattern ab. Meist wird es als Pop-Up eingesetzt, das immer wieder auftaucht, auch nachdem die Nutzer:innen eine Entscheidung getroffen haben – insofern diese nicht dem Wunsch des Website-Betreibers entspricht. Bei der Smartphone-Nutzung werden wir alle regelmäßig gefragt, ob wir nicht doch gerne Push Notifications zulassen oder die Ortungsdienste aktivieren möchten. Beim Consent Management wird das Cookie-Banner immer und immer wieder angezeigt, bis die Nutzer:innen letztlich entnervt auf das "Genörgel" reagieren und zustimmen.
Doch hier ist Vorsicht geboten. Nicht nur, weil der Einsatz von Dark Patterns bald rechtlich unterbunden werden könnte, sondern auch weil Sie als Website-Betreiber Ihre Kund:innen und vor allem deren Vertrauen in Ihre Marke verlieren können – entweder weil die Nutzer:innen schlichtweg genervt sind oder weil sie den Manipulationsversuch durchschauen und an der Aufrichtigkeit der Marke zweifeln.

ABER: Es ist erforderlich, erneuten Consent einzuholen, wenn sich bei den eingesetzten Technologien etwas verändert hat, beispielsweise ein Serverstandort oder ein Anwendungszweck der erhobenen Daten. Eine Mehrfachausspielung bei einem wiederholten Besuch der Website muss also nicht zwangsläufig ein Dark Pattern darstellen. Dieses wäre es erst, wenn das Banner bei ein und demselben Besuch der Seite mehrfach auftaucht.

Für Speicherdauern und die wiederholte Ausspielung des Banners gilt grundsätzlich:

- Opt-Out-Speicherdauern von 24 Stunden bis sieben Tagen haben sich als üblich gezeigt. Längere Opt-Out-Speicherdauern sind rechtlich nicht erforderlich und aus Marketing-Sicht nicht ratsam, können aber natürlich als Instrument der Vertrauensbildung gesehen werden und auf die Markenidentität einzahlen, vor allem wenn es aktiv kommuniziert wird.
- Ausnahme CCPA: Wenn kalifornische Nutzer:innen von ihrem Recht auf Opt-Out Gebrauch machen, müssen die Unternehmen dem Wunsch zwölf Monate lang nachkommen, bevor sie die Nutzer:innen erneut zum Opt-In auffordern dürfen.
- Die Opt-In-Speicherdauern sind oft länger gewählt, damit die gegebene Einwilligung möglichst lange Bestand hat. Hier ist eine Speicherdauer von sechs Monaten bis zu einem Jahr inzwischen Best Practice und eine Dauer, die man in der Datenschutzerklärung so auch guten Gewissens angeben kann. Kürzere Speicherdauern und regelmäßiges Nachfragen erhöhen natürlich die Transparenz, können aber zur Folge haben, dass damit bereits gegebener Consent widerrufen wird und die Nutzer:innen von den Bannern genervt sind.
- Falls Technologien verwendet werden, die die Einhaltung des IAB TCF 2.0- Standards erfordern, sind die Speicherdauern grundsätzlich auf 13 Monate begrenzt (vgl. IAB 2020, S. 10). Damit ist es auch insgesamt empfehlenswert, alle Opt-in-Speicherdauern auf unter 13 Monate festzulegen und diese Vorgabe des IAB als Richtmaß zu verwenden.

Meatball notifications (= Fleischbällchen-Benachrichtigungen)

Wir kennen Meatball-Notifications vor allem aus den Sozialen Medien und von unseren Mailprogrammen. Dabei handelt es sich um die meist roten Kreise, die oben rechts an einer App oder einem Programm-Icon erscheinen, wenn es eine neue Nachricht gibt: Eine neue Mail, ein neuer Like auf Instagram oder eine Reaktion auf einen Tweet. Sie signalisieren Ihnen, dass Sie die App oder das entsprechende Menü nun öffnen sollten, weil es eine Neuigkeit gibt.
Dadurch werden wir darauf trainiert, neugierig zu werden, wenn wir diese Meatball-Notifications sehen: Unser Gehirn schüttet Dopamin aus und wenn wir erst einmal darauf anspringen, ist Tür und Tor offen, uns dorthin zu locken, wo die App-Betreiber uns haben wollen.
Im Bereich Consent Management erscheinen diese kleinen roten Meatballs inzwischen immer häufiger – meist an einem verkleinerten Consent-Pop-Up am unteren Bildrand. Um die Benachrichtigung wegzubekommen oder aus Neugier, klickt man dann auf das Pop-Up oder die Schaltfläche, in der Annahme, dass etwas Spannendes passiert ist, weil wir es so ja gewohnt sind. Aber das ist nicht der Fall. Stattdessen teilt die Benachrichtigung nur mit, dass Sie immer noch nicht allen Marketing-Cookies zugestimmt haben und dass Personalisierung doch eigentlich eine feine Sache wäre, wenn Sie nur kurz der Datenerhebung und -verarbeitung zustimmen könnten. Die Wahrscheinlichkeit, dass man dann eine andere Auswahl trifft als zuvor, steigt trotzdem, da dies einem „Klick-Handlungsimpuls" entspricht, den wir antrainiert haben. Hier ist aus einer clever gestalteten Benachrichtigung schnell ein manipulatives Dark Pattern geworden.

Ein schmaler Grat: Nudging und Dark Patterns

Das sogenannte „Nudging", von „to nudge" (= sanft schubsen), ist ursprünglich ein Begriff der Verhaltensökonomik, geprägt vom Wirtschaftswissenschaftler Richard Thaler und dem Rechtswissenschaftler Cass Sunstein. Zusammen verfassten sie im Jahr 2008 das bis heute gültige Standardwerk[2] zu diesem Thema. Inzwischen hat sich der Begriff von der Verhaltensökonomik losgelöst und ist zu einem Buzzword der Marketingkommunikation geworden.

Der im Consent Management manchmal mitschwingende Vorwurf der Manipulation und Täuschung scheint übertrieben, wenn man die von Anfang an gängige Praxis bei der Gestaltung von Consent-Bannern betrachtet, die überwiegend darin besteht, den „Ablehnen"-Button heller zu gestalten oder auszugrauen und den „Akzeptieren"-Button hervorzuheben.[3]
Anders verhält es sich jedoch bei Dark Patterns. Die Unterscheidung zwischen Nudging und Dark Patterns liegt vor allem im Grad der Manipulation, dem Druck, mit dem eine bestimmte Handlung bei den Nutzer:innen angeregt wird, und der Intention bzw. dem Ergebnis. Der Übergang zwischen zulässigem (positivem) Nudging und unzulässigem Nudging, dem Dark Pattern, ist fließend. Es muss eine Beurteilung des individuellen Falles vorgenommen werden.

Grundsätzlich gilt aber, dass erlaubtes Nudging darauf angelegt ist, den Nutzer:innen zu Entscheidungen zu verhelfen, die ihren vermuteten eigenen mittel- oder langfristigen Präferenzen entsprechen oder zumindest gesamtgesellschaftliche Ziele fördern. Ein Beispiel aus der analogen Welt hierfür wäre das "Innovative People-Flow-Management", das eine Optimierung des Ein- und Aussteigeverhaltens der Menschen im Stuttgarter ÖPNV zum Ziel hat.

Dark Patterns wiederum setzen sich über die Ziele der Subjekte hinweg oder ignorieren sie zumindest. Sie beeinflussen beispielsweise beim Consent Management die Entscheidungen allein gemäß der Interessen der Website-Betreiber – vielfach wird daher auch vom Dark Nudging gesprochen.[4]

Während von Dark Patterns vehement abzuraten ist, ist ein leichtes Nudging aus einer praxisorientierten Sicht durchaus möglich und noch rechtskonform. Laut einer Studie von 2019 nutzten 57,4 % aller Cookie-Banner das Interface-Design, um die Nutzer:innen hin zum Consent zu beeinflussen.[5] Obwohl es Gegenstimmen gibt, wie zum Beispiel die irische Datenschutzbehörde, gibt es rechtlich derzeit noch keinen greifbaren Grund, auf angemessenes Nudging, also das Anregen einer bestimmten Entscheidung, bei der Gestaltung der Cookie-Banner zu verzichten. Ob Nudging beim Einholen von Consent irgendwann komplett verboten wird, ist nicht absehbar. In Frankreich und Dänemark verfährt man bereits heute nach der Devise, dass der Akzeptieren- und der Ablehnen-Button gleich gestaltet sein sollten. Eine ähnliche Auffassung, wenn auch nicht detaillierter ausgeführt, vertritt die bayerische Aufsichtsbehörde. Barbara Thiel, Landesbeauftragte für den Datenschutz des Landes Niedersachsen, zieht die Abgrenzung des Erlaubten und Nicht-Erlaubten folgendermaßen: "Hat ein User durch [...] Nudging-Maßnahmen keine echte Entscheidungsfreiheit mehr zwischen Einwilligung und Ablehnung, ist die Grenze des Erlaubten überschritten."[6]

In keinem Fall dürfen Ihre Nudging-Elemente im Banner also in den Bereich der Täuschung oder deutlichen Manipulation fallen. Das kann nämlich nicht nur rechtliche Konsequenzen haben, sondern sorgt auch für ein negatives Image für Ihr Unternehmen und Ihre Marke, wenn sich Ihre Kund:innen hinters Licht geführt fühlen.

---

[2] Thaler, R. H., & Sunstein C. R. (2019). Nudge. Wie man kluge Entscheidungen anstößt. Berlin: Ullstein.
[3] Vgl. Gradow, L. & Greiner, R. (2021). Quick Guide Consent Management. Wiesbaden: Springer Gabler, S. 144f.
[4] Vgl. Martini et al. (2020). Dark Patterns – Phänomenologie und Antworten der Rechtsordnung. ZfDR 2021. S. 47–74, S. 51.
[5] Vgl. Utz et al. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field, S. 976
[6] Barbara Thiel, zit. nach: Prüfung zu Cookies und Drittdiensten auf niedersächsischen Webseiten. https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/prufung-zu-cookies-und-drittdiensten-auf-nieder-sachsischen-webseiten-194909.html. Aufgerufen am 10. Januar 2022. Vgl. auch: Handreichung „Datenschutzkonforme Einwilligungen auf Webseiten – Anforderungen an Consent-Layer." LfD Niedersachsen.

Recht und Unordnung: Die Gesetzeslage

Bisher gibt es keine explizite Regelung zu Dark Patterns, weder in Deutschland noch auf EU-Ebene. Es gibt jedoch datenschutzrechtliche, verbraucherschutzrechtliche, vertragsrechtliche sowie lauterkeitsrechtliche Regelungen, die sich auch auf Dark Patterns beziehen lassen. Vor allem im Datenschutz- und Verbraucherschutzrecht können durch behördliche und gerichtliche Rechtsgestaltung die Grenzen zwischen dem noch Erlaubten und dem rechtswidrig Manipulativen recht scharf gezogen werden. Sowohl die Behörden als auch die Gerichte ziehen bereits Flanken und Grenzen ein. Das vermutlich größte Problem des Rechts ist, dass es von einem rational nach seinen Interessen handelnden Individuum ausgeht und daher der Schwerpunkt der Regelungen auf das Bereitstellen von klaren, verständlichen und vollständigen Informationen für die Nutzer:innen gelegt wird. So ist es in der Regel erforderlich, dass die Bereitstellung von Informationen gewisse Kriterien erfüllt.

Zum Beispiel:

- leicht erkennbare, unmittelbar erreichbare und ständig verfügbare Information (bspw. § 5 Abs. 1 TMG)
- „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar" (NetzDG)
- „in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form" (Art. 8 Abs. 3 ePrivacy-VO)
- „leicht wahrnehmbar, unmittelbar erreichbar und ständig verfügbar" (§§ 85, 93 Abs. 1 Medienstaatsvertrag im Hinblick auf nutzerfreundliche Designgestaltung. Eine Definition der Benutzeroberfläche findet sich dabei in § 2 Nr. 15. In § 84 Abs. 3, 2 wird die Oberflächengestaltung geregelt und eine unbillige Behinderung bei der Auffindbarkeit von einzelnen Angeboten verboten.)

Darüber hinaus gibt es eine ganze Reihe von Regelungen, die die persönliche Autonomie gegen Dark Patterns zu schützen versuchen:

Im Bereich des Datenschutzrechts ist es einerseits die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit Art. 7 Abs. 4 DSGVO. Dabei ist vor allem das Merkmal der Freiwilligkeit relevant, an dem es fehlt, wenn die Einwilligung „durch starke Täuschung oder Drohung mit erheblichen negativen Wirkungen erreicht" wird, denn in diesem Fall wird die Einwilligung nicht von der „Autonomie des Einwilligenden getragen"[7]. Daraus leiten sich das Verbot von „Preselection-Patterns" im Planet49-Urteil des EuGH bzw. im Cookie II-Urteil des BGH ab sowie das Verbot der vertikalen und horizontalen Kopplung. Das zweite relevante Merkmal ist die Informiertheit an der es insbesondere dann fehlt, wenn die Informationen durch optische Gestaltung, Formulierung oder überkomplexe Strukturen verwirrend dargestellt sind.

Neben der Einwilligung ist die zweite und immer stärker an Bedeutung gewinnende Regelung im Zusammenhang mit Dark Patterns (und der Gestaltung des Consent Managements) Art. 25 Abs. 1 DSGVO – Privacy-by-Design: Zur Technikgestaltung gehört, nach der sich immer stärker durchsetzenden Auffassung von Behörden, Gerichten und Wissenschaft, auch das Design der Anwendungsoberfläche, sodass Design-Muster einen Teil der Technikgestaltung darstellen und gegen die Vorgaben von Art. 25 Abs. 1 verstoßen, wenn beispielsweise Design-Muster von Consent-Bannern Nutzer:innen dazu verleiten, größere Mengen an Daten preiszugeben als für den beabsichtigten Zweck erforderlich. Entscheidend ist, dass die Anwendung bzw. die bewusste Vermeidung von Dark Patterns auch geprüft werden kann: Aufsichtsbehörden können im Rahmen ihrer Untersuchungsbefugnisse, nach Art. 58 Abs. 1 lit. a DSGVO, zum Beispiel von Verantwortlichen Auskunft darüber verlangen, ob sie Dark Patterns testen, einsetzen oder gar personalisieren.

[7] Martini et al. (2020). Dark Patterns – Phänomenologie und Antworten der Rechtsordnung. ZfDR 2021. S. 47–74. S. 55.

Die Abgrenzung zwischen zulässiger Oberflächengestaltung und unzulässigen Dark Patterns erfolgt nach den Vorgaben der Gesetzgebung, welche vereinzelt durch die Aufsichtsbehörden und letztlich die Rechtsprechung konkretisiert werden.

Beispiele dafür sind:

- UK-Aufsicht: ICO zu Age Appropriate Design
- FR-Aufsicht: CNIL zu Gestaltung von Cookie-Informationen
- DE-Aufsicht: LfD Niedersachsen - Handreichung zu datenschutzkonformen Einwilligungen auf Webseiten
- USA: CPRA (Sec. 14 lit h)
- EU: Der Digital Services Act (DSA): Er regelt den Umgang mit „illegalen Inhalten" sowie mit Meinungsfreiheit und Falschinformationen auf digitalen Plattformen, adressiert aber auch die manipulative Verhaltenssteuerung in Erwägungsgrund 32, 63, 68 sowie in Art. 26 Abs. 1 lit c.

In Deutschland finden darüber hinaus auch weitere Regelungen Anwendung, die sowohl direkt als auch indirekt geeignet sind, Dark Patterns zu regulieren und ggf. auch zu sanktionieren:

Im **Lauterkeitsrecht,** also im **Gesetz gegen den unlauteren Wettbewerb** (UWG), finden sich beispielsweise folgende Regelungen:

- § 4a verbietet „aggressive geschäftliche Handlungen", vor allem Belästigung, Nötigung und unzulässige Beeinflussung, die die Entscheidungsfreiheit beeinträchtigen
- § 7 verbietet unzumutbare Belästigung, vor allem im Zusammenhang mit Werbung
- § 5 und §5a erfassen das „Erschleichen" und „Irreführen"
- § 3 Abs. 2 ist die Generalklausel, deren zentraler Punkt die „wesentliche Beeinflussung des wirtschaftlichen Verhaltens des Verbrauchers" und der Verstoß gegen die unternehmerische Sorgfalt ist. Sie bietet einen weiten Ausgestaltungsspielraum für Gerichte.
- Die Schwarze Liste des Anhangs zu § 3 Abs. 3 adressiert in Nr. 6 "Bait and Switch" (= Lockvogelangebote), in Nr. 7 verbietet sie unwahre, d.h. objektiv unrichtige Angaben über begrenzte Verfügbarkeit von Waren oder Dienstleistungen. Misdirection-Patterns werden in Nr. 8 (Sprachenwechsel) behandelt, Nr. 21 befasst sich mit kostenpflichtigen Gratisleistungen und Nr. 22 mit der Täuschung über abgegebene Bestellungen.

Im **Vertragsrecht** sind es Regelungen in § 312 BGB:

- So regelt § 312 a Abs. 3 das Preselection-Verbot im elektronischen Geschäftsverkehr.
- Nach § 312 j Abs. 1 Satz 2 müssen Informationen klar, deutlich und verständlich bereitgestellt werden, wobei auch das Design der Bereitstellung relevant ist, vgl. BGH im Flugbuchungen-Urteil vom 20.03.2018.

Wir können abschließend also festhalten, dass das Thema der Dark Patterns im Consent Management verschiedene Rechtsbereiche tangiert, die es im Einzelfall zu berücksichtigen gilt. Allerdings gibt es durchaus bereits Handhabe gegen Verstöße beim manipulativen Design von Consent-Bannern: Die für das Consent Management wohl interessanteste gerichtliche Entscheidung hat das Landgericht Rostock (Az.: 3 O 762/1) am 15.09.2020 erlassen. Zu Beginn des Verfahrens waren im Consent-Banner von advocado.de die Einwilligungen zum Setzen von Präferenzen-, Statistik- und Marketing-Cookies voreingestellt. Im Laufe des Verfahrens wurde das Banner angepasst: Unten links ein stark ausgegrauter Button mit dem Text "Nur notwendige Cookies verwenden", rechts daneben ein leuchtend grüner Button mit dem Text "Cookies zulassen" und nochmals rechts daneben ein bloßer Text "Details zeigen" mit einem "Dropdown-Pfeil". Diese Art von Bannern begegnen uns ständig und erscheinen soweit nicht außergewöhnlich, allerdings beschreibt das Urteil, warum diese Art der Gestaltung nicht zulässig ist:

„Eine wirksame Einwilligung ist damit auch mit dem nunmehr verwendeten Cookie-Banner nicht möglich. Denn auch bei diesem sind sämtliche Cookies vorausgewählt und werden durch Betätigung des grün unterlegten „Cookie zulassen"-Buttons „aktiviert".
[…]
„zwar hat der Verbraucher die Möglichkeit, sich Details anzeigen zu lassen und einzelne Cookies abzuwählen. Tatsächlich wird der Verbraucher jedoch regelmäßig den Aufwand eines solchen Vorgehens scheuen und deshalb den Button ohne vorherige Information über die Details betätigen. Damit weiß der Verbraucher aber gerade nicht, welche Tragweite seine Erklärung hat. Der Umstand, dass der Nutzer bei dem nun verwendeten Cookie-Banner auch die Möglichkeit hat, über den Bereich „Nur notwendige Cookies verwenden" seine Einwilligung auf technisch notwendige Cookies zu beschränken, ändert an der Beurteilung nichts. Insoweit ist festzuhalten, dass dieser Button gar nicht als anklickbare Schaltfläche zu erkennen ist. Zudem tritt er auch neben dem grün unterlegten und damit als vorbelegt erscheinenden „Cookie zulassen"-Button in den Hintergrund. Diese Möglichkeit wird von einer Vielzahl der Verbraucher deshalb regelmäßig gar nicht als gleichwertige Einwilligungsmöglichkeit wahrgenommen werden. Daran ändert auch der Einleitungstext nichts, da dieser bereits nicht darüber aufklärt, welche Cookies wie vorbelegt sind und damit durch welchen Button, welche Cookies „aktiviert" werden." (VZBV)

FELDM

Fazit und Ausblick: Vertrauen und Barrierefreiheit als Wettbewerbsvorteil

Wie eingangs bereits angedeutet, gibt es verschiedene Bestrebungen, gegen den Einsatz von Dark Patterns im Internet vorzugehen. Ganz konkret fordern die EU-Staaten, dass im derzeit diskutierten Digital Services Act die sogenannten „Dark Patterns" beim Verkauf von Waren und Dienstleistungen im Netz verboten werden sollen (Stand November 2021). Damit sollten Sie Ihr bestehendes Cookie-Banner bereits jetzt auf den Einsatz von manipulativen Design-Mustern prüfen und diese künftig vermeiden.

Besucher:innen Ihrer Seite sind eher gewillt, Ihnen die Datenerhebung zu erlauben, wenn sie Ihrer Marke vertrauen – und damit ist nicht nur der Cookie Consent gemeint, sondern auch das damit immer enger zusammenhängende Permission Marketing, das einen direkten Einfluss auf Ihre Umsätze haben dürfte. Sie müssen also das Vertrauen Ihrer Nutzer:innen gewinnen. Dabei geht es nicht nur um eine offene und transparente Kommunikation, um einzelne Bestandteile des Wordings und der optischen Erscheinung Ihres Cookie-Banners oder Preference-Centers, sondern auch um ein größeres und umfassenderes Vertrauen in Ihre Marke.

Barrierefreiheit ist dabei ein zurecht immer wichtiger werdender Aspekt. Die auftretende Manipulation und Komplexität der Consent-Banner durch Dark Patterns multipliziert sich, wenn diese nicht visuell erfahren werden können, sondern für Menschen mit Sehbehinderung von Screenreadern vorgelesen werden. Das Navigieren durch Untermenüs, in denen die Informationen zu Technologien und Verarbeitungszwecken akustisch nur nach und nach erfasst werden können, durchdrungen von weiteren Links, Hinweisen und Toggeln zum Einstellen der persönlichen Präferenzen, ist für viele blinde Menschen ein schier unüberwindbarer Dschungel. Dass die Texte oft unnötig kompliziert sind und häufig auch auf deutschen Websites in Englisch verfasst, potenziert das Problem nochmals und beschränkt die Verständnisschwierigkeiten, die daraus resultieren, nicht mehr nur auf sehbehinderte Menschen.

Auch Barrierefreiheit und ein allgemeines Bemühen darum, dass die Websites für alle Menschen zugänglich und die Einwilligungen zu Datenverarbeitungen informiert und freiwillig getroffen werden können, zahlen auf Ihre Glaubwürdigkeit und auf das Vertrauen in Ihre Marke ein. Langfristig wird sich Ihr Engagement hier auszahlen, da Sie rechtmäßig erhobene Daten nachhaltig und wertsteigernd nutzen können.

Transparenz und Aufrichtigkeit währen länger als der Quick Win durch manipulative Dark Patterns.

Noch Fragen oder Anmerkungen?

FELD M ist Ihr verlässlicher Partner, der die aktuellen rechtlichen Diskussionen verfolgt, pragmatische Best Practices kennt und selbst innovative technische Lösungen für Ihren individuellen Anwendungsfall entwickelt, damit Sie einen echten und rechtlich sicheren Vorteil gegenüber Ihren Wettbewerbern haben. Kontaktieren Sie mich gerne unter ramona.greiner@feld-m.de.