usercentrics

Datenschutz in Apps - ein gesetzesfreier Raum?

DSGVO-Verstöße bei Apps in der EU

Eine Marktanalyse von Usercentrics

Inhalt

Die wichtigsten Erkenntnisse 3

Der aktuelle App-Markt 4

Der App-Markt der Zukunft 5

Das sollten App-Anbieter jetzt tun 6

Externe Ressourcen 7

Appendix 8

DSGVO-Nichteinhaltung: App-Kategorien im Vergleich 9

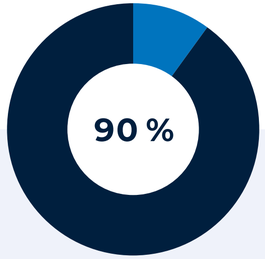
Methodik 10

Über Usercentrics 11

usercentrics

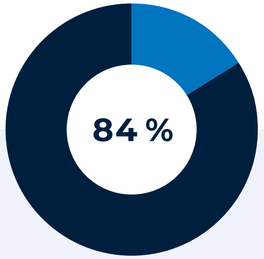
Die wichtigsten Erkenntnisse

Unsere Analyse zeigt: Viele Apps innerhalb der EU verstoßen gegen die geltenden Datenschutzvorschriften. Nutzer werden ohne ihre Einwilligung getrackt und ihre personenbezogenen Daten an Dritte weitergegeben – ein eindeutiger Verstoß gegen die Vorgaben der Datenschutz-Grundverordnung (DSGVO) und der ePrivacy-Richtlinie.



90 % der 250 von Usercentrics analysierten Apps sind nicht DSGVO-konform: Sie tracken Nutzer ohne deren Einwilligung.

In der Kategorie Glücksspiel-Apps wurde die DSGVO zu 100 % nicht eingehalten – der höchste Wert in allen analysierten Kategorien.



Die Kategorie Lebensmittel-Apps kommt mit 84 % auf den niedrigsten Wert.

Die meisten Tracking-Technologien in Apps sind darauf ausgelegt, personenbezogene Daten wie IP-Adressen, Online Identifiers und Standortdaten von Nutzern zu verarbeiten.

Usercentrics hat für diesen Bericht mit Hilfe von Apptopia, einem der führenden Anbieter von Competitive Intelligence für Apps, 250 Apps untersucht. Die Analyse wurde im Oktober 2022 durchgeführt. Mehr dazu erfahren Sie im Anhang.

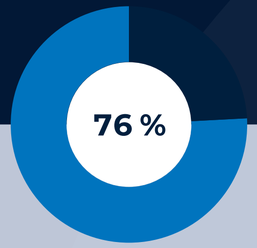
usercentrics

Der aktuelle App-Markt

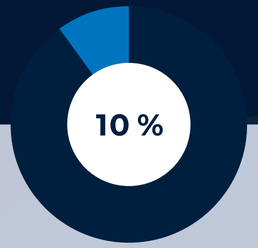
Vier Jahre nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) gleicht der App-Markt in der EU in Bezug auf Datenschutz nach wie vor dem Wilden Westen. Kein Wunder, denken die meisten Menschen, wenn Sie den Begriff DSGVO hören, doch zunächst einmal an Cookie-Banner auf Webseiten. Dass dieselben Regeln für die Einholung der Nutzereinwilligung auch für Apps gelten, ist allerdings den wenigsten bewusst.

Im September 2022 analysierte Usercentrics den App-Markt der EU. Das Ergebnis: **90 % der untersuchten Apps halten weder die DSGVO noch die ePrivacy-Richtlinie ein, denn sie nutzen Tracking-Technologien, die personenbezogene Daten von Nutzern erheben, ohne vorab deren Einwilligung einzuholen.**

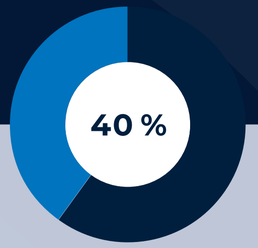
Aktuelle Studien zeichnen ein ähnliches Bild:



Eine Studie von Appvisory zeigt, dass **von einer Million Apps 76 % nicht** die Anforderungen der DSGVO erfüllen, personenbezogene Daten nur mit Einwilligung des Nutzers zu erfassen.

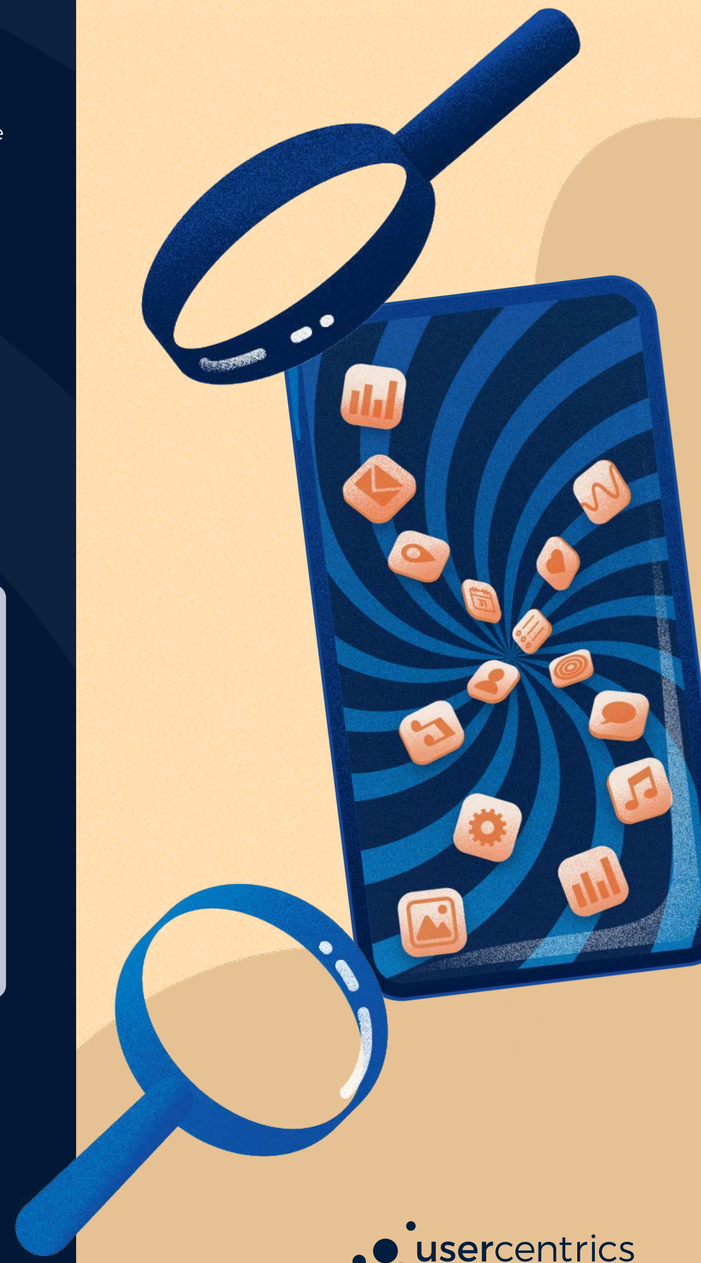


Eine Oxford-Studie ergab, dass **von zwei Millionen Apps nur 10 % DSGVO-konform waren.** Die gleiche Studie zeigte auch auf, dass Apps personenbezogene Daten im Durchschnitt an zehn Drittunternehmen weitergeben.



Eine Studie von Deloitte und Google stellte fest, dass **40 % von 4.150 Nutzern** innerhalb eines Jahres nach der Studie **Apps aufgrund von Datenschutzbedenken gelöscht haben.** Dies zeigt eindeutig, was passiert, wenn App-Anbieter ohne die Einwilligung der Nutzer agieren und die DSGVO nicht einhalten.

Kurz gesagt: Die Vorschriften der DSGVO werden bei vielen Apps innerhalb der EU nicht eingehalten. App-Anbieter riskieren so Bußgelder und verspielen das Vertrauen ihrer Nutzer.



usercentrics

Der App-Markt der Zukunft

Mittlerweile ist klar, dass die Einwilligung der Nutzer einzuholen und Datenschutzkonformität zu gewährleisten weit mehr als nur gesetzliche Vorschriften sind.

Eine kürzlich von Ipsos und Google durchgeführte Studie, an der über 20.000 EU-Verbraucher teilnahmen, zeigt eindeutig, **dass es durchaus Vorteile mit sich bringt, die Einwilligung der Nutzer einzuholen und Datenschutz in den Mittelpunkt zu stellen:**

Insbesondere:

- Eine positive Datenschutzerfahrung erhöht den Anteil der Markenpräferenz um 43 %.
- Die Auswirkungen einer negativen Datenschutzerfahrung hingegen sind fast so schwerwiegend wie die eines Datenschutzverstoßes.
- Monetäre Anreize für die Offenlegung von Daten (z. B. das Angebot von Rabatten für die Erteilung einer Einwilligung) wirken sich nicht immer positiv aus und können sogar zu einem Vertrauensverlust führen.
- Wenn Menschen Vertrauen in eine Marke haben, sind sie doppelt so häufig bereit, ihre personenbezogenen Daten offenzulegen.
- Verbrauchern das Gefühl zu geben, dass sie ihre Daten kontrollieren können, ist der effektivste Weg, Vertrauen zu gewinnen und die Markenpräferenz zu stärken.

Dass - trotz der unbestreitbaren Vorteile von Datenschutzkonformität - viele in der EU verfügbare Apps nicht DSGVO-konform arbeiten, zeigt: **Der EU-Markt für Apps befindet sich immer noch in einer Umbruchphase.**

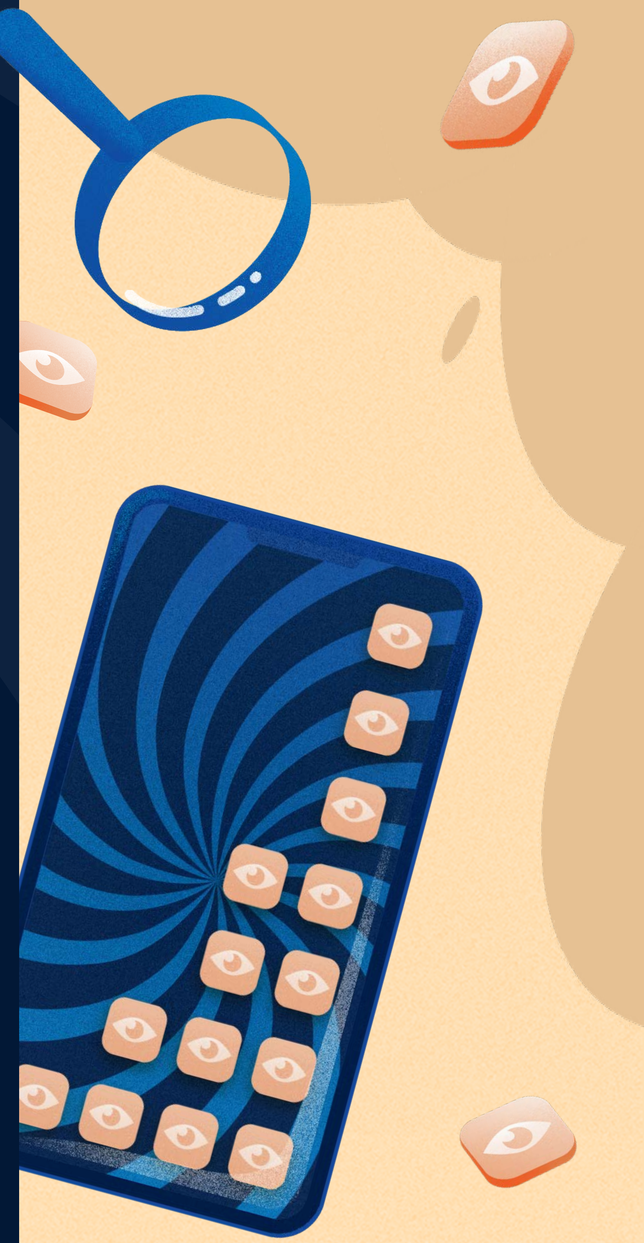
Doch die Durchsetzung der DSGVO nimmt zunehmend Fahrt auf und viele Websitebetreiber wechseln zu einem nachhaltigeren und nutzerzentrierten Ansatz, um Wachstum und Umsatz zu steigern, und stellen dabei die Einwilligung der Endnutzer in den Mittelpunkt.

Auch Apps müssen die Anforderungen der DSGVO und der ePrivacy-Richtlinie erfüllen. Nutzer müssen also auch bei Apps ihre Einwilligung erteilen, bevor Dritte ihre Daten mit Tracking-Technologien erfassen dürfen.

Anders als viele App-Anbieter glauben, ist dies kein Nachteil. Im Gegenteil, immer mehr aktuelle Studien zeigen, **dass sich dadurch durchaus auch Vorteile ergeben.**

Nutzern die Möglichkeit zur Einwilligung zu geben, stellt nicht nur die Grundlage für einen vertrauensvollen digitalen Austausch dar, sondern eröffnet auch Monetarisierungsoptionen und ermöglicht dadurch mehr Umsatz.

Es ist also letztlich eine Win-Win-Situation für Nutzer und App-Anbieter.



usercentrics

Das sollten App-Anbieter jetzt tun

Nutzereinwilligungen DSGVO- und ePrivacy-Richtlinien-konform einzuholen, sollte für App-Anbieter **Priorität haben** - und zwar nicht nur um Bußgelder zu vermeiden, sondern insbesondere auch um das Vertrauen der Nutzer zu gewinnen und den Ruf der eigenen Marke nicht zu schädigen.

Diese Checkliste kann Ihnen helfen, die Anforderungen der DSGVO in Ihrer App zu erfüllen*:

- **Prüfen Sie die Technologien, die Ihre App verwendet.** Identifizieren Sie hierfür alle in Ihren Apps installierten Software Development Kits (SDKs) und dokumentieren Sie, welche Technologie von Drittanbietern zum Einsatz kommt und auf welche Daten diese zugreift.
- **Erklären Sie den Hintergrund und Zweck von Tracking-Technologien (und fügen Sie diese Informationen in Ihre umfassende Datenschutzrichtlinie ein).** Informieren Sie Nutzer z. B. darüber, welche Daten wie und warum erfasst werden.
- **Teilen Sie Ihren Nutzern mit, dass Sie Tracking-Technologien verwenden** (z. B. in SDKs enthaltene Tracking-Technologien). Blenden Sie hierfür ein Consent-Banner ein – und zwar bevor ein SDK Daten erfasst.
- **Holen Sie eine gültige Einwilligung gemäß DSGVO ein.** Dies bedeutet, dass die Einwilligung ausdrücklich und freiwillig erteilt wird, Endnutzern alle Informationen granular vorliegen, die Einwilligung jederzeit einfach widerrufen werden kann und dass die Einwilligung dokumentiert wird.
- **Ermöglichen Sie Nutzern den Zugriff auf Ihren Dienst, auch wenn sie nicht mit der Erfassung ihrer Daten durch Tracking-Technologien einverstanden sind.** Wenn ein Nutzer die Datenverarbeitung ablehnt, sollte er die App weiterhin nutzen können, wobei nur wichtige Tracking-Technologien, die für die Funktion der App erforderlich sind, aktiviert bleiben.
- **Erfassen und verarbeiten Sie Daten nur, wenn eine gültige Einwilligung vorliegt.** Achten Sie in diesem Zusammenhang darauf, dass SDKs erst geladen werden, wenn der Endnutzer seine Einwilligung erteilt hat.
- **Dokumentieren und speichern Sie die Nutzereinwilligungen,** z. B. für ein Audit durch Aufsichtsbehörden.
- **Die Einwilligung muss jederzeit so einfach widerrufen werden können, wie sie erteilt werden kann.**
- **Achten Sie darauf, dass nach einer widerrufenen Einwilligung keine weiteren Daten erfasst oder weitergeleitet werden.**

Die Einhaltung der DSGVO und der ePrivacy-Richtlinie kann zeitaufwendig und schwierig in der technischen Umsetzung sein. Aus diesem Grund sind **Consent Management Platforms (CMPs)** schnell zu einem beliebten Tool geworden, um Unternehmen dabei zu unterstützen, Datenschutzkonformität zu gewährleisten.

Moderne Plug-and-Play-SDKs ermöglichen die schnelle Integration der CMP in Apps – eine einfache und automatische Lösung für die Einhaltung der DSGVO und ePrivacy-Richtlinie.

Falls eine Consent Management Platform (CMP) bereits in Ihre App implementiert wurde, stellen Sie anhand der Checkliste (links) sicher, dass sie den Anforderungen der DSGVO genügt.

Einer der größten Vorteile einer CMP ist, dass die nötigen Maßnahmen zur Einhaltung automatisiert werden: **Dies macht Datenschutzkonformität kinderleicht,** sodass Sie sich auf Ihr Kerngeschäft konzentrieren können.

Mit Hilfe einer CMP lassen sich die komplizierten und komplexen Vorschriften der DSGVO einfacher umsetzen. Zudem ist sichergestellt, dass Ihre App dank modernster Technologie zur Einwilligungseinholung stets den sich ändernden Vorschriften entspricht.

Vor allem aber bauen Sie Vertrauen zu Ihren Nutzern auf und leisten einen Beitrag dazu, unser digitales Ökosystem nachhaltiger für alle zu gestalten.

Sie haben Fragen zur Einhaltung der Datenschutzbestimmungen in Ihrer App? Unsere Experten helfen Ihnen gerne weiter.
Kontaktieren Sie uns unter apps@usercentrics.com

usercentrics

*Diese Angaben stellen keine Rechtsberatung dar. Wenn Sie rechtliche Fragen haben, sollten Sie sich mit der zuständigen Datenschutzbehörde oder einem Rechtsanwalt abstimmen. Die Umsetzung einer datenschutzkonformen CMP liegt letztlich im Ermessen des jeweiligen Datenschutzbeauftragten oder der Rechtsabteilung.

Externe Ressourcen

Apptopia

Studie von Appvisory

Studie der Universität Oxford

Studie von Ipsos und Google

Studie von Deloitte und Google

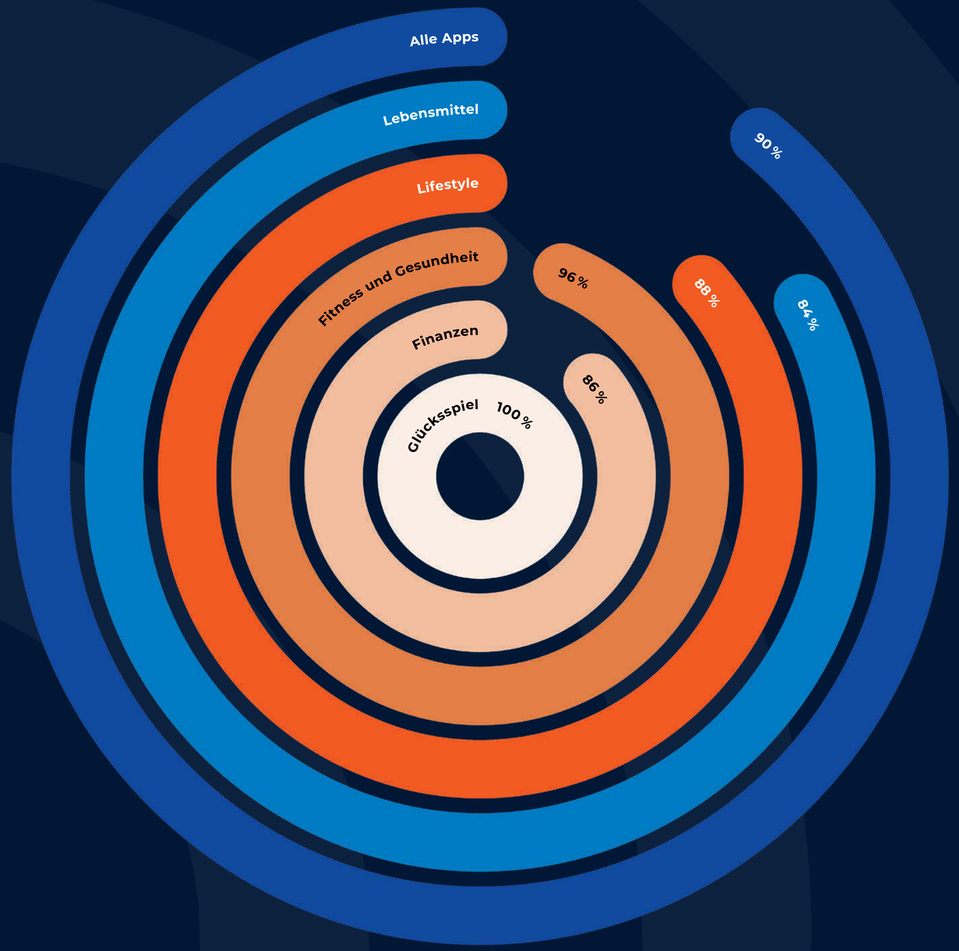
usercentrics

Appendix

usercentrics

DSGVO-Nichteinhaltung: App-Kategorien im Vergleich

Kategorie	Durchschnittlicher Grad der Nichteinhaltung für jede Kategorie (in %)
Alle Apps	90
Lebensmittel	84
Lifestyle	88
Fitness und Gesundheit	96
Finanzen	86
Glücksspiel	100



usercentrics

Methodik

Zur Durchführung der Studie nutzte Usercentrics das Tool „SDK Intelligence Insights“ von Apptopia, einem der führenden Anbieter von Competitive Intelligence für Apps.

Es wurden 250 Apps aus fünf beliebten Kategorien ausgewählt (Lebensmittel, Lifestyle, Fitness und Gesundheit, Finanzen und Glücksspiel), in denen Tracking-Technologien integriert sind, die personenbezogene Daten von Nutzern über in den SDKs enthaltene Tracking-Technologien erfassen.

Für jede Kategorie wurden insgesamt 50 Apps ausgewählt, die jeweils:

- Tracking-Technologien von Dritten zu Analytics-, Attributions-, Monetarisierungs- oder Marketingzwecken installiert haben
- von Nutzern in der EU genutzt werden
- von mindestens 50.000 Nutzern pro Tag aktiv genutzt werden

Die Kriterien wurden gemäß den Anforderungen der DSGVO und der ePrivacy-Richtlinie ausgewählt, sowie der Art und Weise, wie sie von Datenschutzbehörden in der gesamten EU interpretiert und umgesetzt wurden.

Jede App wurde auf Geräte innerhalb der EU heruntergeladen, um zu prüfen, ob eine Consent Management Platform (CMP) installiert wurde, mit der wir – als Nutzer – die integrierten Tracking-Technologien ablehnen und unsere personenbezogenen Daten schützen können.

Wenn ein Consent-Banner in der App installiert war, wurde geprüft, ob es den gesetzlichen Standards entspricht, d. h., ob das Banner die Buttons „Akzeptieren“ und „Ablehnen“ enthielt, alle in der App verwendeten Tracking-Technologien aufgelistet werden und ob der Zweck der Datenerfassung dem Nutzer beschrieben wurde.

usercentrics

Über Usercentrics

Usercentrics ist einer der weltweiten Marktführer im Bereich Consent Management Platforms (CMP). Wir unterstützen Unternehmen dabei, Nutzereinwilligungen für ihre Webseiten und Apps einzuholen, und diese so zu verwalten und zu dokumentieren, dass sie globale Datenschutzvorschriften einhalten können. Gleichzeitig ermöglichen wir mit unseren Lösungen hohe Opt-In-Raten und den Aufbau vertrauensvoller Kundenbeziehungen.

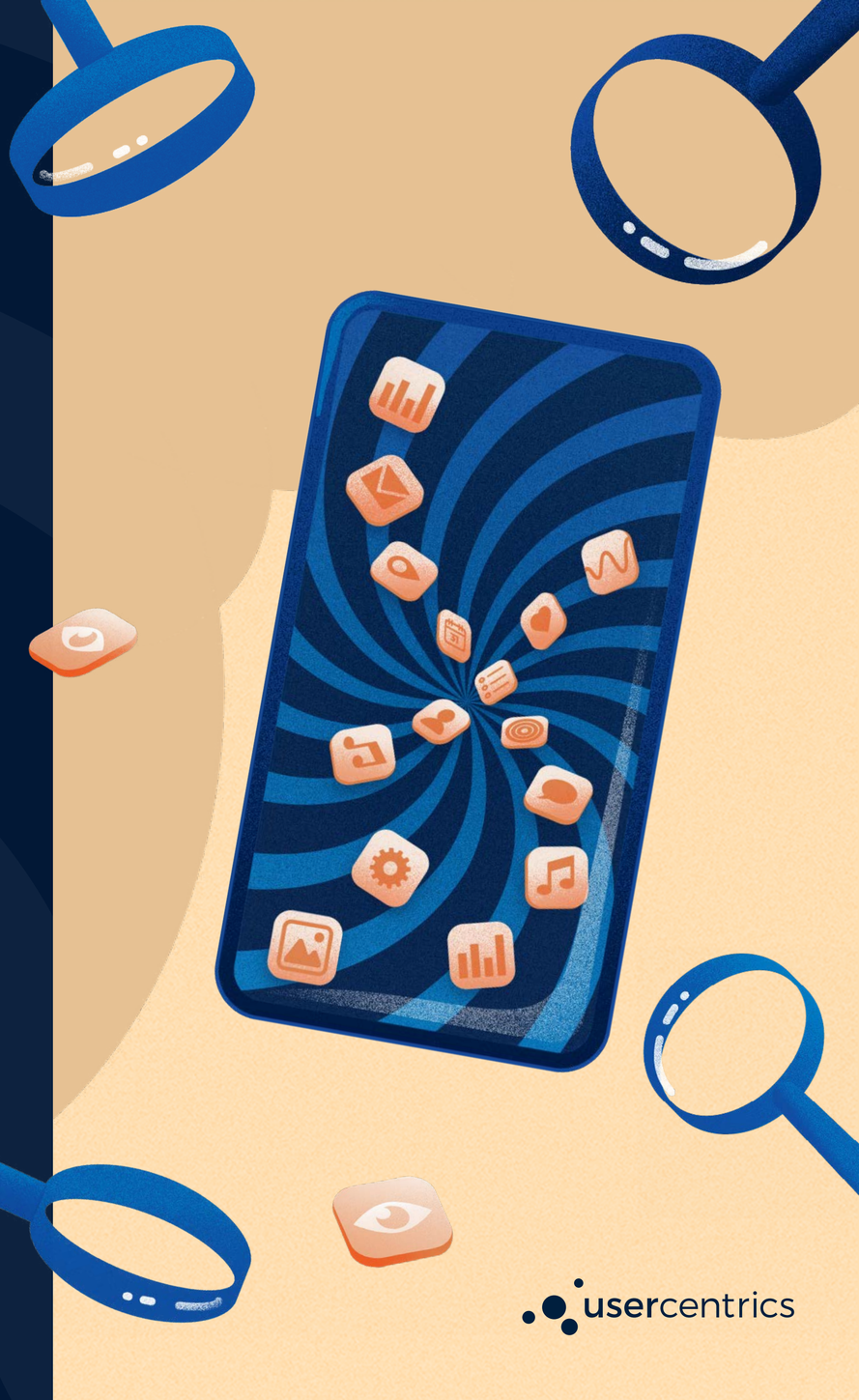
Wir sind davon überzeugt, dass ein gesundes Gleichgewicht zwischen Datenschutz und datengetriebenem Geschäft möglich ist und bieten Lösungen für jede Unternehmensgröße. Cookiebot CMP ist unsere Plug-and-Play-SaaS-Option, ebenso bieten wir eine App CMP zur Verarbeitung von Nutzereinwilligungen an. Großunternehmen mit individuellen Anforderungen vertrauen beim Consent Management auf die Usercentrics CMP. Dabei werden Einwilligungen mit Daten von der Erfassung bis zur Verarbeitung zusammengebracht.

Usercentrics ist in mehr als 180 Ländern aktiv, hat ein Netzwerk von über 2.000 Vertriebspartnern und verarbeitet täglich mehr als 100 Millionen Nutzereinwilligungen.

Die Vorteile der Verwendung der App CMP (SDK) von Usercentrics in Ihrer App:

- **Benutzerfreundlichkeit** – ein Plug-and-Play-SDK, das die Einhaltung komplexer Datenschutzvorschriften automatisiert
- **Hohe Anpassbarkeit** – kann an jede Domain und jedes Design nahtlos angepasst werden, um das Kundenvertrauen zu stärken und die Opt-In-Rate zu optimieren
- **Modernste Technologie** – erstklassige Technologie, die umfassend geprüft und optimiert wurde, um sicherzustellen, dass die App-Performance nicht leidet
- **A/B-Testing** – Schaffen Sie ein vertrauenswürdiges App-Erlebnis für Ihre Nutzer und testen Sie mit A/B-Testing-Tools das Messaging, das am besten funktioniert
- **Analytics** – Überwachen Sie die Performance des SDK mit Granular Analytics, mit der Möglichkeit, Daten vollständig zu exportieren

Kontaktieren Sie uns und finden Sie heraus, wie Sie Risiken durch eine Nichteinhaltung der DSGVO und ePrivacy-Richtlinie, wie Bußgelder, reduzieren und das Vertrauen der Nutzer Ihrer App stärken können.



Besuchen Sie usercentrics.com und erfahren Sie mehr.

usercentrics