CHEATSHEET

DATENSCHUTZ im digitalen Marketing

STRATEGIE
MARKETING
COACHING
KI

SHARE2B:GREEN
STRATEGY | MARKETING | COACHING
AI

EINLEITUNG

Datenschutz im digitalen Marketing ist wichtiger denn je. Indem du die Datenschutzbestimmungen einhältst, vermeidest du nicht nur Bußgelder und rechtliche Probleme, sondern baust auch Vertrauen bei deinen Kund:innen auf und schützt dein Unternehmen. Dieses Cheatsheet gibt dir einen Überblick über die wichtigsten Punkte, die du beachten solltest, um datenschutzkonformes Marketing zu gewährleisten.

Haftungsausschluss

Denke daran, dass dieses Cheatsheet nur die wichtigsten Aspekte abdeckt und in keiner Form eine Rechtsberatung darstellt. Wenn du unsicher bist, ziehe unbedingt eine/n Expert:in für Datenschutz hinzu. So stellst du sicher, dass die individuellen Anforderungen deines Unternehmens genau geprüft und alle Datenschutzrichtlinien und -maßnahmen rechtlich abgesichert sind.

STRATEGIE

Ziel: Integration von Datenschutz in alle Marketingprozesse.
Daten-Sicherheitsrichtlinie erstellen: Definiere alle Datenarten und Sensitivitätslevel.
Datenflüsse dokumentieren: Identifiziere, wie und wo Daten gespeichert und genutzt werden.
Zugriffskontrollen: Implementiere Maßnahmen wie Verschlüsselung und Zugriffsüberwachung.
Verantwortlichkeiten zuweisen: Bestimme die zuständigen Personen für die Datensicherheit.
Schulungen für Mitarbeiter: Regelmäßige Schulungen zu Datenschutz und Sicherheit.
Checkliste:
[ ] Sensible Daten identifiziert und klassifiziert.
[ ] Datenflüsse und -speicherung dokumentiert.
[ ] Zugriffs- und Sicherheitsmaßnahmen definiert.
[ ] Verantwortliche benannt und geschult.
[ ] Regelmäßige Überprüfungen und Updates der Sicherheitsrichtlinie – Intervall festgelegt.

ERFASSUNG

Ziel: Sicherstellen, dass alle Daten legal und ethisch gesammelt werden.
Daten-Touchpoints auditieren: Überprüfe alle Stellen, an denen Daten gesammelt werden.
Einwilligung einholen: Explizite Zustimmung der Nutzer an allen Erfassungspunkten sicherstellen.
Keine „Dark Patterns" verwenden: Täuschende Praktiken vermeiden. (weitere Infos siehe unten)
Datenschutzrichtlinie aktualisieren: Website-Privacy-Policy/Cookie Banners auf den neuesten Stand bringen.
Checkliste:
[ ] Alle Datenerfassungspunkte identifiziert und geprüft.
[ ] Einwilligungen der Nutzer eingeholt.
[ ] Datenschutzrichtlinie/Cookie Banner auf der Website aktualisiert.
[ ] Keine Listen von Drittanbietern ohne Zustimmung nutzen.
[ ] Datenschutzrichtlinien von Drittanbietern validiert.

TRACKING

Ziel: Effektives Tracking unter Einhaltung von Datenschutzbestimmungen.
Opt-out-Möglichkeiten bieten: Nutzer:innen erlauben, das Tracking einfach und schnell abzulehnen.
Nur notwendige Daten sammeln: Minimierung der Datenerfassung und -speicherung.
Erstanbieter-Tracking verwenden: Statt Drittanbieter-Tracking-Pixel nutzen. (weitere Infos siehe unten)
Checkliste:
[ ] Deutlich sichtbare und einfache Opt-out-Optionen für Nutzer:innen eingerichtet.
[ ] Datensammlung auf notwendige Informationen beschränkt.
[ ] Erstanbieter-Tracking implementiert.

ANALYSE

Ziel: Datenschutzkonforme Analyse und Attribution.
Datensammlung minimieren: Vermeide direkte Identifikatoren.
Optionale Datenarten: Kontextdaten anstelle von personenbezogenen Daten verwenden.
Datenaggregation: Daten auf Gruppen- oder Segmentebene aggregieren.
Checkliste:
[ ] Direkt identifizierende Daten minimiert.
[ ] Kontextuelle Daten zur Modellierung genutzt.
[ ] Daten nur auf notwendiger Basis zugänglich gemacht.
[ ] Daten auf Gruppen- oder Segmentebene aggregiert.

ERGÄNZUNG

"Dark Patterns" sind täuschende Designpraktiken, die darauf abzielen, Nutzer:innen dazu zu bringen, Entscheidungen zu treffen, die sie normalerweise nicht treffen würden. Ein häufiges Beispiel für einen Dark Pattern ist das sogenannte "Nudging" bei Cookie-Bannern. Dabei wird die Option, alle Cookies zu akzeptieren, deutlich hervorgehoben und leicht zugänglich gemacht (z.B. durch einen großen, auffälligen Button), während die Option, nur notwendige Cookies zu akzeptieren oder die Cookie-Einstellungen anzupassen, versteckt oder schwieriger zu finden ist (z.B. durch kleinere Schrift oder versteckte Menüs). Dies verstößt gegen den Grundsatz der informierten Einwilligung, da die Nutzer:innen nicht klar und transparent über die Art und den Umfang der Datenerfassung informiert werden.

Erstanbieter-Tracking bezieht sich auf die Datenerfassung durch die Website, die der Nutzer direkt besucht. Im Gegensatz dazu erfolgt Drittanbieter-Tracking durch externe Unternehmen, die Tracking-Pixel oder Cookies auf der Website platzieren, um Nutzerdaten für ihre eigenen Zwecke zu sammeln. Erstanbieter-Tracking gilt als sicherer und datenschutzfreundlicher, da die gesammelten Daten nur von der besuchten Website verwendet werden und nicht an Dritte weitergegeben werden. Damit baust du Vertrauen zu deinen Besucher:innen auf.