WHITEPAPER

CONSENT MANAGEMENT TOOLS IM ÜBERBLICK

netresearch

SPE4CRM
Smart Privacy Engines for CRM

INHALT

01 EINFÜHRUNG

Das vorliegende Whitepaper gibt einen Überblick über Consent Management Tools am Markt sowie eine Einschätzung über mögliche Anknüpfungspunkte für ergänzende Lösungen.

Seit den gesetzlichen Regelungen zum Schutz personenbezogener Daten (DSGVO, CCPA oder die kommende E-Privacy-Verordnung), sind Betreiber damit konfrontiert, ihren Nutzern die Verwendung ihrer Daten aufzuzeigen und vor allem deren Einwilligung (Consent) dazu vorab einzuholen. Falls keine Einwilligung erteilt wurde, sind Betreiber dazu verpflichtet, die Verwendung der Daten zu unterlassen.

Das bringt zwei wesentliche Herausforderungen mit sich:

- Die Betreiber müssen technisch und organisatorisch dafür sorgen, dass die gesetzlichen Bestimmungen eingehalten werden.
- Ersteres muss so benutzerfreundlich wie möglich geschehen.

Die eben genannten Herausforderungen implizieren eine Reihe an Anforderungen, denen entsprechende Consent-Management-Lösungen begegnen müssen. Im folgenden Kapitel sollen diese erläutert werden.

Was ist Consent Management?

Der Begriff **Consent Management**, auch Einwilligungsmanagement, umfasst dabei technische und organisatorische Ansätze, um die Einwilligung von Website- oder App-Benutzern zur Datenverarbeitung durch den Betreiber bzw. vom Betreiber beauftragte Drittparteien zu erfassen, zu analysieren und umzusetzen.

02 ANFORDERUNGEN

BENUTZERFREUNDLICHKEIT

In der Regel haben Betreiber von Online-Angeboten ein wirtschaftliches Interesse, die Einwilligung zur Datenverarbeitung für die Anwender so benutzerfreundlich und wenig störend wie möglich zu gestalten. Vor allem in stark umkämpften Märkten, wie zum Beispiel im E-Commerce-Sektor, spielt die Benutzerfreundlichkeit des Online-Shops eine wesentliche Rolle. Ist sie problematisch, bedeutet dies in der Regel den unmittelbaren Verlust von Interessenten. Dabei ist die sogenannte Absprungrate ein kritischer Faktor für die Wirtschaftlichkeit der Online-Shops. Da die Betreiber meist einigen – auch finanziellen – Aufwand betreiben müssen, um Besucher für ihre Online-Shops zu gewinnen, ist die Benutzerfreundlichkeit für Betreiber häufig geschäftskritisch.

Was ist eine Absprungrate ?

Eine **Absprungrate** bezeichnet je nach Maßgabe das Verhältnis der Besucher, die ein Produkt kaufen oder in den Warenkorb legen zu denen, die vorher die Seite verlassen.

Nun liegt die Benutzerfreundlichkeit eines Angebots vorwiegend im Auge des Benutzers. Dementsprechend schwer ist es im Vorfeld allgemeingültige Aussagen hierfür zu treffen. Dennoch gibt es eine Reihe von Maßgaben, die in verschiedenen Studien und Arbeiten zum Thema Benutzerfreundlichkeit ermittelt wurden. Eine generelle Möglichkeit, die Benutzerfreundlichkeit zu erhöhen, ist der Einsatz von Design-Mustern. Diese beschreiben gestalterische Lösungen verbreiteter Probleme, wie z.B. die Benachrichtigung von Benutzern, Bestätigung von Aktionen, und können als Best Practices angenommen werden. Aktuell beginnen sich solche Muster auch für das Consent Management zu etablieren, was nicht nur sinnvoll und hilfreich für die Anbieter, sondern vor dem Hintergrund der gesetzlichen Pflicht auf jeder Website, auch dringend notwendig ist.

> Consent Management Lösungen sollten sich an diesen Konventionen zumindest orientieren bzw. diese nur brechen, wenn dadurch eine substantielle Verbesserung der Benutzerfreundlichkeit erreicht wird.

RECHTLICHE KONFORMITÄT

Es ist zwingend notwendig, dass die CM-Lösungen die jeweilig geltenden gesetzlichen Bestimmungen erfüllen. Hierbei kann es je nach Standort des Nutzers andere Gesetze und Verordnungen (z.B. DSGVO) bzw. Auslegungen davon geben, denen die CM-Lösung begegnen muss.

> Die DSGVO ist ein Verordnung der Europäischen Union, welche die Verarbeitung von personenbezogenen Daten von „Betroffenen durch „Verantwortliche", z.B. Unternehmen, regelt.

Für ein, nach DSGVO, rechtlich konformes Consentmanagement müssen unter Anderem folgende Punkte beachtet werden:

- Der Consent und sein Umfang müssen nachweisbar sein.
- Der Betroffene muss seinen Consent jederzeit widerrufen können.
- Datenverarbeitung darf nicht ohne Consent stattfinden, es sei denn, sie ist für den Betrieb zwingend notwendig, z.B. zur Speicherung des Warenkorbs.
- Der Consent muss explizit und aktiv erfolgen.
    - Consent Optionen dürfen nicht Voraus markiert sein, es sei denn, sie sind für den Betrieb der Seite unabdingbar.
    - Impliziter Consent „Durch die weitere Nutzung der Seite" ist nicht zulässig.
- Der Zweck jeder Datenverarbeitung muss für den Nutzer verständlich einsehbar sein.

TECHNISCHE KONFORMITÄT

Über die gestalterischen Konventionen hinaus haben sich bzw. wurden in der jüngeren Vergangenheit auch Standards zur Verarbeitung und Weitergabe von Consents entwickelt. Diese sind insbesondere dann wichtig, wenn Consents über die aktuell besuchte Website hinaus von Bedeutung sind. Vor allem im digitalen Anzeigenmarkt ist das der Fall. Das Interactive Advertising Bureau Europe (IAB), ein Branchenverband der digital Werbetreibenden, hat mit dem Transparency und Consent Framework (TCF) einen relevanten Standard für die Branche festgelegt.

Consent Management Lösungen sollten diesen Standard dringend unterstützen, da er von den meisten Analyse-, Retargeting- und Werbenetzwerken unterstützt wird.

Die Kommunikation von Consents an diese Netzwerke über den TCF-Standard hat sich konsolidiert und wird voraussichtlich noch stärker gefördert werden. Darüber hinaus bietet das TCF eine standardisierte Vorgehensweise zur Erreichung der Rechtssicherheit in Bezug auf die Verarbeitung und Weitergabe personenbezogener Daten.

Die Internationale Organisation für Standardisierung (ISO) hat zudem den Standard ISO 27701 für Privacy Information Management Systems herausgegeben. Dessen Einhaltung sollte den Anwendern der jeweiligen Consent Management Lösung (CM-Lösung) zusätzliche Rechtssicherheit verschaffen.

INTEGRATION

Bei der Integration von Consent Management Lösungen in die bestehende IT-Landschaft, u.a. von E-Commerce-Unternehmen können sowohl client- als auch serverseitige Dimensionen betrachtet werden. Clientseitig gibt es da zum einen die Integration in die Website bzw. in mehrere Websites – im Folgenden als Widget(s) bezeichnet. **Die Herausforderung liegt darin, die Funktion der Website durch die Einbindung weder optisch noch technisch zu beeinträchtigen.** Die Bandbreite an Frontend-Technologien sowie die teilweise geforderte lang zurückreichende Browser-Kompatibilität, welche mögliche Lösungsansätze, wie Web-Components zumindest erschwert, verlangt den CM-Anbietern hierbei besondere Expertise ab.

Gestalterisch können abhängig von der sonstigen Gestaltung der Website zudem unterschiedliche Anforderungen an die Widgets bestehen. Je nach Detailgrad, kann das beispielsweise die Platzierung auf der Website, das Verhalten (z.B. Banner bzw. Pop-Over, Modal-Fenster oder Fly-Out), die Farbgebung, Button- bzw. Eingabefeld-, Schrift-, Animations- und Rahmenstile betreffen. Diese Anforderungen müssen bei Responsive Websites auch für die jeweiligen Break Points erfüllt werden. Den genannten Anforderungen mit einem möglichst geringen Integrations- bzw. Anpassungsaufwand zu begegnen, erfordert von der CM-Lösung aufwendige Konfigurationsmöglichkeiten bzw. Konfiguratoren.

Alternativ könnte die Oberfläche der Widgets auch programmatisch durch den integrierenden Web-Entwickler angepasst werden. Hierbei muss der CM-Anbieter jedoch dafür Sorge tragen, dass durch solche programmatischen Anweisungen nicht die Funktionalität der Widgets selbst beeinträchtigt wird – was in diesem Fall potentiell möglich ist.

Was sind Responsive Websites und Break Points?

Responsive bezeichnet die unterschiedliche Darstellung der gleichen Website für verschiedene Auflösungen, Pixeldichten und Seitenverhältnisse. Hierbei wird neben prozentualen Gestaltungsanweisungen mit sogenannten Break Points gearbeitet. Dies sind Dimensionsabfragen, ab bzw. bis zu denen bestimmte Anweisungen gelten sollen.

Eine weitere Dimension der clientseitigen Integration betrifft die tatsächliche Anwendung der vom Nutzer getroffenen Einstellungen direkt auf der Website. In der simpelsten Form bedeutet dies die Entfernung nicht zugelassener Cookies und die Vermeidung des erneuten Setzens. Hierbei ist allerdings zu beachten, dass nicht nur Cookies unter die einschlägigen Richtlinien fallen, sondern alle Möglichkeiten benutzerseitig Daten zu speichern, die zur Wiedererkennung verwendet werden können (Web Storage API, IndexedDB API, Service Worker API und andere teils noch nicht voll unterstützte Funktionen wie Cache API oder WebAssembly API). Effektiver und sicherer ist daher gänzlich die Einbindung der Skripte, die diese Daten speichern, durch die CM-Lösung zu vermeiden.

Darüber hinaus sollten CM-Lösungen mit gängigen Online-Marketing-Tools, wie z.B. zur Besucheranalyse, für A/B-Testing, Retargeting, Website-Chat-Bots, zusammenarbeiten können. Für einfache Opt-In-Verfahren sollte dies mit der oben erwähnten Sperrung der entsprechenden Skripte keine große Hürde darstellen. Schwieriger stellt sich hingegen die pflichtgemäße Auszeichnung der entsprechenden Tools und deren Datenverarbeitungsaktivitäten im Consent-Dialog und in der Datenschutzerklärung sowie die Durchführung von Opt-Outs dar. Hierfür ist entscheidend, dass die CM-Lösung die jeweiligen Tools kennt, entsprechend auszeichnen und Opt-Outs vornehmen kann. Ein Spezialfall dieser Tools sind sogenannte Tag-Manager, wie beispielsweise Google Tag Manager oder Matomo Tag Manager, die ihrerseits verschiedene solcher Tools bündeln und von zentraler Stelle aus verwalten können (d.h. ohne Eingriffe in die Website bei Änderungen an den verwendeten Tools). Da diese Tag-Manager mögliche weitere Tools kapseln, die dadurch nicht mehr direkt für die CM-Lösung erkennbar sind, muss die CM-Lösung in der Lage sein mit solchen interagieren zu können.

Zusätzlich zu diesen clientseitigen Dimensionen sind serverseitige Maßnahmen insbesondere dann zu treffen, wenn Cookies bei der Auslieferung der Website und nicht erst bei der Auslieferung von Skripten gesetzt werden. Hierfür sind möglichst nahtlose Integrationen in gängige Content-Management- und Shop-Systeme in Form von Plugins sehr sinnvoll. Die CM-Lösungen sollten bestrebt sein, solche zur Verfügung zu stellen.

> Bei Eigenentwicklungen hingegen sollten die CM-Lösungen gut dokumentierte Mechanismen bereitstellen, über die serverseitig auf die Ergebnisse und Ereignisse des Consent Managements reagiert werden kann.

Letztendlich stellen weitere technische Ausprägungen jeweils weitere Anforderungen an die CM-Lösung – ob zum Beispiel die Website eine AMP-Variante bereitstellt, ob sie als Progressive Web App arbeitet oder ob es Mobile Apps gibt, die zu integrieren sind.

DOKUMENTATION

Eine gute CM-Lösung muss zunächst die eingesetzten Tools bzw. gesetzten Cookies auf der Website selbstständig erkennen können. Bei Kenntnis dokumentiert die CM-Lösung diese idealerweise auch für den Consent-Dialog sowie die Datenschutzerklärung und lässt solche Dokumentationen ergänzend durch den Website-Betreiber erlauben. Dieses Feature ist wichtig, um zustimmungspflichtige Aktivitäten vorab zu erkennen bzw. dem Betreiber aufzuzeigen und damit späteren unvorhergesehenen Darstellungen im Consent-Dialog oder gar einer unerkannten Aktivität vorzubeugen.

Im besten Fall kann die CM-Lösung auch auf Veränderungen der verwendeten Cookies reagieren und diese dem Betreiber und den Besuchern aufzeigen sowie wiederum in die Datenschutzerklärung einfließen lassen. Des Weiteren muss die CM-Lösung die getroffenen oder verweigerten Zustimmungen der Benutzer serverseitig festhalten, was auch für spätere Änderungen gilt.

> Die Consent Management Lösung muss die getroffenen oder verweigerten Zustimmungen der Nutzer serverseitig festhalten, was auch für spätere Änderungen gilt.

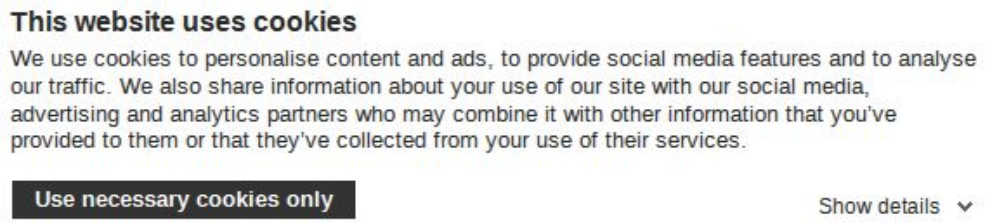
03 KOMMERZIELLE LÖSUNGEN

Cookiebot

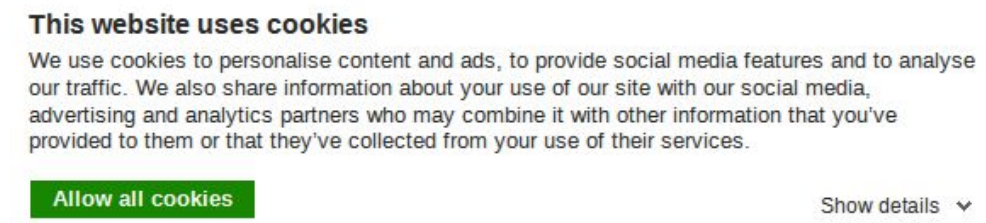
Cookiebot ist ein Angebot der dänischen Firma Cybot und bietet eine spezialisierte Plattform für die Verwaltung von Cookie-Einwilligungen in verschiedenen Kostenvarianten an. Das Preismodell ist nicht an Funktionen, sondern an die Anzahl der Unterseiten der jeweiligen Domain gebunden. Die Varianten reichen für eine Domain von einem freien Angebot (bis zu 100 Unterseiten) bis 37 EUR pro Monat (unbegrenzte Unterseiten). Es stellt eine monatliche automatisierte Analyse der Website auf die Verwendung von Cookies (Cookie Scan) zur Verfügung. Auf deren Basis werden der Consent-Dialog und eine Cookie-Übersicht für die Datenschutzerklärung generiert. Diese werden mittels JavaScript-Snippets auf der Website eingebunden, welche auf der Cookiebot-Plattform konfiguriert werden. Die gefundenen Cookies werden mit einem zentralen Register bekannter Cookies (Cookie Repository) abgeglichen und bei Bekanntheit automatisch klassifiziert – unbekannte Cookies können selbstständig beschrieben und einem Verwendungszweck zugewiesen werden.

Der Consent Dialog kann in folgenden Punkten angepasst werden:

- Darstellungsweise (Position des Dialogs – oben, unten, als Overlay, u.a.)
- Anzuzeigende Buttons und Cookie-Klassen
- Methode
  - Ausdrückliche Einwilligung – Nutzer müssen ausdrücklich eine Auswahl treffen.
  - Implizite Einwilligung – Die Einwilligung wird angenommen, wenn Nutzer den Dialog ignorieren.
- Typ – die Art und Weise der Einwilligungsmöglichkeiten
  - „Nur ablehnen“ – nur Opt-Out-Möglichkeit aus der impliziten Einwilligung

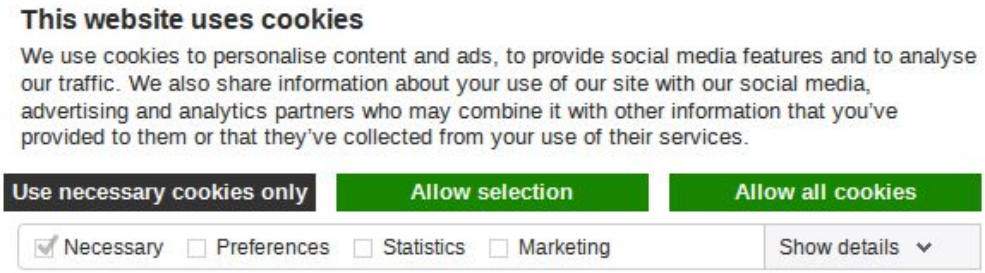


  - „Nur akzeptieren“ – der Nutzer muss allen Cookies zustimmen, um die Website verwenden zu können. Hiervon ist abzuraten, wenn die Seite mehr als nur technisch notwendige Cookies verwendet.

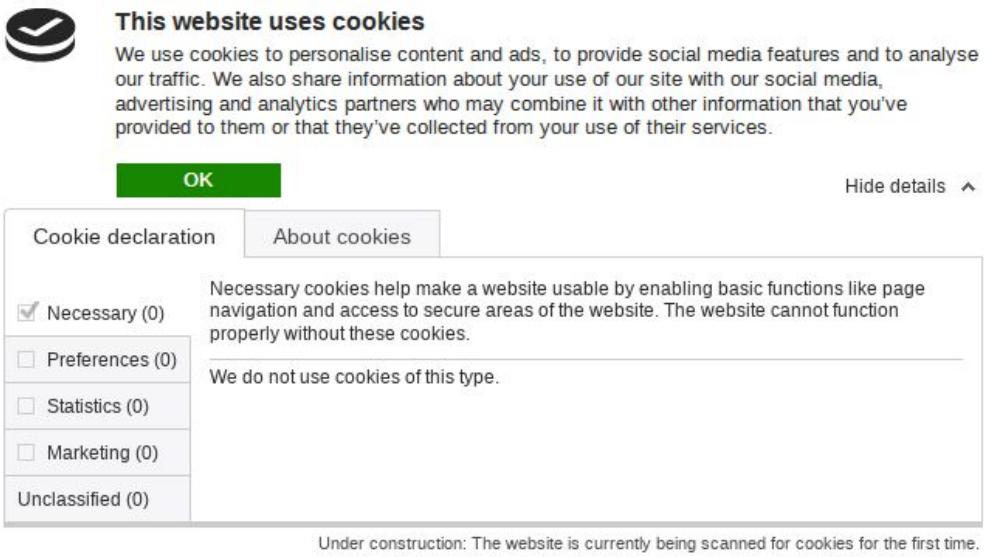


- „Akzeptieren/Ablehnen“ – Opt-In und Opt-Out stehen zur Verfügung

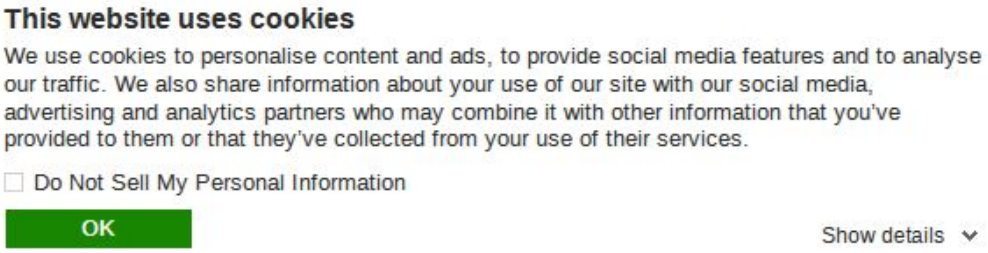
- „Mehrere Ebenen“ – Opt-In und Opt-Out nach Verwendungszwecken möglich



- „Inline mit mehreren Ebenen“ – wie „Mehrere Ebenen“, aber Opt-In/Out in Cookie-Liste



- „Nicht verkaufen“ – wie „Nur akzeptieren“, aber mit Auswahl, dass die personenbezogenen Daten nicht verkauft werden dürfen (Vorgabe des California Consumer Privacy Act)



In den bezahlten Varianten kann darüber hinaus…

- …die Einwilligung für mehrere Domains gleichzeitig aktiviert,
- ein Farbthema aus einer vorgegebenen Liste gewählt und
- das Gebiet, für das Einwilligungen eingeholt werden sollen, eingegrenzt werden.

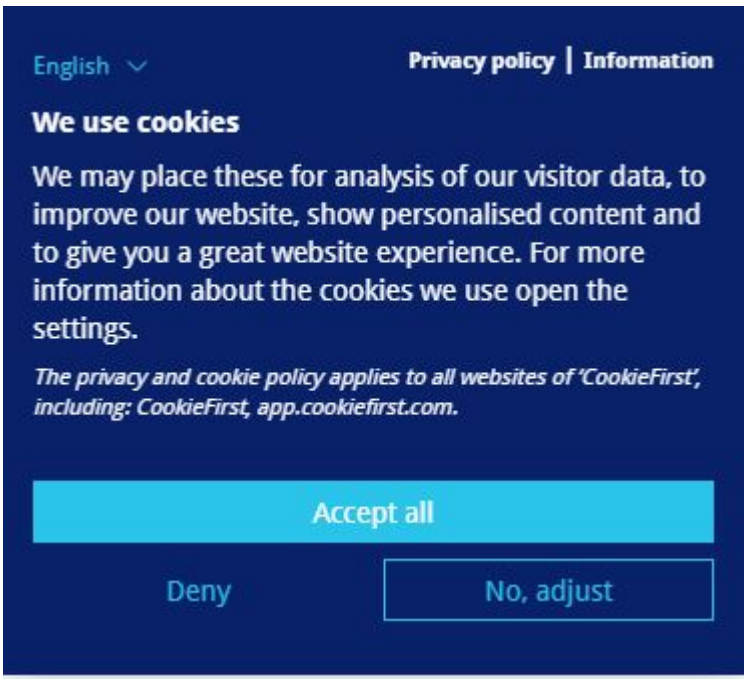
Das Cookie-Verzeichnis kann nur in den bezahlten Varianten durch Auswahl vorgegebener Vorlagen angepasst werden.

Cookiebot verfügt über einen sogenannten Autoblocking-Modus, in welchem das Cookiebot-Skript relevante Skripte anderer Tools (wie z.B. Google Analytics, Social Media Widgets, Videos von Videoplattformen, u.a.) automatisch blockiert, das bedeutet konkret deren Einbindung verhindert. Insbesondere für weniger technisch versierte Website-Betreiber handelt es sich um eine einfache Möglichkeit Rechtskonformität zu erreichen. In diesem Zusammenhang ist allerdings mit Kompatibilitätsproblemen zu rechnen und die Wirksamkeit der Blockierung sollte eingehend getestet werden. Für die erweiterte Anwendung der Consent-Einstellungen bietet Cookiebot ein JavaScript-Software Development Kit (SDK) – eine spezialisierte Software-Bibliothek als Programmierschnittstelle zu einem Dienst.

Cookiebot stellt eine schnelle und unkomplizierte Möglichkeit für das Consent Management und die Erreichung der Konformität zumindest für einen Rechtsraum dar, wobei jedoch unbedingt darauf geachtet werden sollte, dass eine geeignete Darstellungsform gewählt wird. Für die Auslieferung einer Website in unterschiedliche Rechtsräume scheint die Lösung hingegen nur bedingt geeignet, da die Konfiguration des Consent Dialogs an Domains bzw. Domain-Gruppen gebunden ist. Das bedeutet, dass länderspezifische Konfigurationen zwingend länderspezifische Domains erfordern. Dies kann für einige Shop-Betreiber Aufwand mit sich bringen. Vor allem stellt sich aber die Frage, inwiefern Konformität je Rechtsraum gegeben ist, wenn diese von Cookiebot nicht automatisch umgesetzt wird.

Eine weitere Komplikation ist, dass Cookiebot zumindest in der kostenlosen Variante nur einen monatlichen Scan der Website erlaubt. Das kann dazu führen, dass neue Anwendungen nur verzögert gefunden und in die Cookie-Listen aufgenommen werden und die Consent-Lösung in der Zwischenzeit nicht rechtskonform ist.

CookieFirst ist ein Angebot des niederländischen Unternehmens Digital Data Solutions und verfolgt den gleichen Geschäftszweck mit prinzipiell ähnlichem Funktionsumfang wie Cookiebot. Es grenzt sich gegenüber Cookiebot bewusst durch mehr bzw. komfortablere Funktionalitäten ab. Hierzu zählt beispielsweise, dass ausdrücklich auf nicht DSGVO-konforme Einwilligungsabfragen verzichtet wird.



Zudem lässt sich die Einbindung von Drittanbieter-Tools abhängig von der Zustimmung der Nutzer einfacher steuern. Im Gegensatz zu Cookiebot, bei welchem die Einbindung dieser Skripte zusätzliche Programmierung erfordert, bietet CookieFirst einen Tag Manager, über den die Skripte (z.B. Google Analytics, u.a.), abhängig von der Zustimmung des Nutzers, hinterlegt und Verarbeitungskategorien zugewiesen werden können. Diese Art der zustimmungsabhängigen Einbindung bedarf nur eines einmaligen Eingriffs in die Seite. Weitere Skripte oder Anpassungen können dann ohne Programmierung über die CookieFirst-Anwendung vorgenommen werden. Das ist zum einen für die Administratoren einfacher und zum anderen stellt es auch eine effektive Art der Steuerung dar, weil Fehlerquellen minimiert werden.

Neben weiteren kleineren Verbesserungen, wie anpassbaren Bezeichnungen und Texten für die Cookie-Kategorien sowie weitergehenden Anpassungsmöglichkeiten für die Darstellung, unterscheidet sich aber auch das Preismodell: Es ist grundsätzlich günstiger (kostenfrei bis 19 EUR pro Monat) und nicht an die Anzahl der Unterseiten gebunden. Die im Abschnitt Cookiebot dargestellte Problematik bezüglich länderspezifischer Domains wird auch durch CookieFirst nicht adressiert.

Was ist ein Tag Manager?

Ein **Tag Manager** bezeichnet ein Service, der verschiedene Drittanbieter-Skripte kapselt, sodass diese nicht einzeln in die Seite integriert werden müssen, sondern nur durch das **Tag Manager** Skript eingebunden werden. Ein bekanntes Beispiel ist der **Google Tag Manager**.

Usercentrics ist eine in Deutschland entwickelte Consent Management Plattform für den Enterprise-Bereich. Damit geht sie im Funktionsumfang über den von Cookiebot und CookieFirst hinaus. Hervorzuheben ist hierbei ein deutlicherer Fokus auf Rechtssicherheit, Konformität, Transparenz und Benutzerfreundlichkeit, die sich zum Beispiel in der Darstellung des Consent-Dialogs sowie dem Umfang der Cookie-Informationen zeigen:

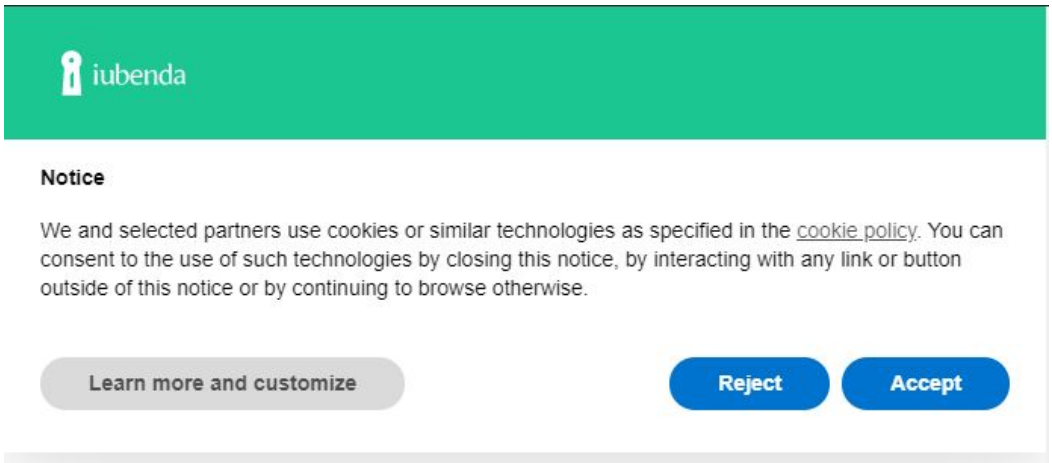
Diese Enterprise- und Publisher-Ausrichtung unterstreicht fortgeschrittene Funktionalitäten, wie den…

- …TagLogger, der zur Laufzeit Skripteinbindungen auf der Website überwacht und protokolliert,
- der Privacy Smart Locker, der Skripte und Tags nicht freigegebener Anbieter bzw. Anwendungen auf der Website unterdrücken kann,
- Multidomainunterstützung,
- ein SDK für Mobile Apps,
- eine umfangreiche API,
- konstante Aktualisierung mit neuen Rechtsvorgaben,
- Konformität mit dem IAB TCF Standard (siehe Abschnitt Konformität)
- und anderes mehr.

Viele dieser Funktionalitäten sind erst in den höheren Preismodellen verfügbar, welche wiederum auf der Anzahl von Sessions pro Monat basieren. Eine kostenfreie Version steht nicht zur Verfügung.
Preise beginnen bei 8 EUR für eine Domain mit 20000 Sessions pro Monat und steigen mit höheren Session Zahlen.

iubenda

Iubenda ist ein Angebot eines gleichnamigen italienischen Unternehmens und geht über eine Consent Management Plattform hinaus. Zum Beispiel bietet es zusätzlich Generatoren für Datenschutz- und Cookie-Richtlinien sowie AGB an. Außerdem stellt iubenda eine Plattform für ein unternehmensinternes Datenschutzmanagement mit weiteren Funktionalitäten, wie beispielsweise Verarbeitungsverzeichnissen, zur Verfügung. Über die Funktionen, die die vorangegangenen Angebote beinhalten, bietet iubenda neben einer umfassenden konstanten rechtlichen Begleitung ihrer Kunden zudem Konformität mit dem California Consumer Privacy Act (CCPA).



Im Rahmen des Consent Managements ist auch eine Kontrolle über die Einbindung externer consent-abhängiger Skripte möglich. Iubenda bietet Module für eine Reihe an Webservern, die solche Skripte bereits vor der Auslieferung der Seite von deren HTML-Code entfernen und damit Bandbreite und mögliche Komplikationen mit browserseitigem Sperren reduzieren.
Das Preismodell beginnt bei etwa 9 EUR für kleine Seiten und bietet eine Reihe wählbarer Optionen, abhängig davon, wie viele Zugriffe stattfinden und welche Konformität angestrebt wird.

OneTrust

OneTrust ist ein US-amerikanisches und englisches Unternehmen, welches neben einer Consent Management Plattform eine ganze Reihe von Datenschutz-, Konformitäts- und Risikomanagement-Lösungen anbietet. Die laut eigener Aussage mit über 100.000 Websites meistverwendete Cookie Consent Lösung, bietet wie die vorangegangenen Lösungen einen…

- … automatischen Scan der Website auf Basis von Cookies, Skripten, Tracking-Pixels, u.a.,
- die automatische Kategorisierung von Cookies auf Basis interner Datenbanken,
- anpassbare Cookie-Banner,
- Auto-Blocking von Skripten,
- Tag Manager Integrationen,
- dynamisch erzeugte Cookie-Richtlinien,
- und vor allem Konformität mit – im Vergleich – den meisten Richtlinien und Standards (DSGVO [Dtl.], E-Privacy, CCPA [USA], ICO [UK], CNIL (Frk.] und Industrie-Frameworks vom IAB und DAA [Digital Advertising Alliance])
- standortabhängige Consent Abfragen

Ergänzt wird das Angebot mit einer Lösung für Consent Management und Analyse in Mobile Apps sowie dem Preference Center Management. Bei letzterem handelt es sich um eine Lösung für die Verwaltung von Verarbeitungseinwilligungen über verschiedene Kanäle, wie Apps, Websites, Direktkontakten oder E-Mails. Diese ermöglicht zudem die Synchronisation von Verarbeitungsentscheidungen mit anderen Systemen, wie CRM, Marketing Automation Systemen, Tag Managern, CMS, u.a.

Während die Cookie Consent Lösung preislich im Umfeld der zuvor erläuterten Lösungen liegt, stellt das eben beschriebene Preference Center Management mit 270 EUR pro Monat eine kostenintensive Option dar. OneTrust selbst bietet keine kostenfreie Variante an, jedoch dessen Tochterunternehmen CookiePro.

CookiePro
by OneTrust

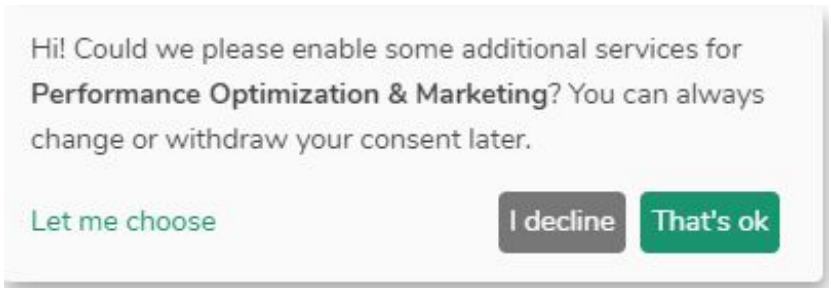
TrustArc

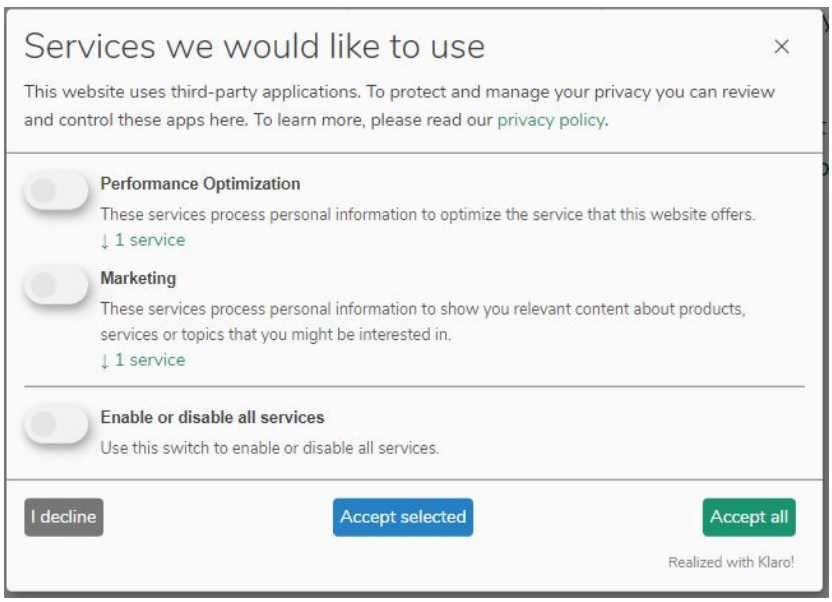
TrustArc ist ein US-amerikanisches Unternehmen – bis 2017 TRUSTe -, welches ähnlich wie OneTrust ein breites Spektrum von Produkten und Dienstleistungen im Bereich Privacy Compliance anbietet. Ein Teil dieses Angebots ist der Cookie Consent Manager, der ähnlich den vorangegangenen Tools eine vollumfängliche Consent Management Lösung darstellt. Neben der kostenpflichtigen, ist auch eine kostenfreie Variante verfügbar.

04 OPEN SOURCE

Klaro

Klaro! Ist eine denkbar einfache Umsetzung des Consent Managements. Es wird über ein Skript in die Seite eingebunden und mit einer Liste an Apps konfiguriert. Die Einbindungs-Tags der Apps müssen durch den Betreiber dahingehend geändert werden, dass sie nicht direkt als JavaScript ausgeführt werden. Die Nutzer-Einwilligungen werden von Klaro! dann so umgesetzt, dass die Einbindungs-Tags freigegebener Apps so umgeschrieben werden, dass sie vom Browser interpretiert und die Cookies aller anderen Apps entfernt werden.





05 FAZIT

Die hier vorgestellten Lösungen werden alle mehr oder weniger deutlich den in Kapitel 2 dargestellten Anforderungen gerecht. Sie bilden nur einen Bruchteil aller am Markt existierenden Anbieter ab, repräsentieren allerdings die am meisten verbreiteten Ansätze. Ob und welche dieser Lösungen letztlich auf einer Website eingesetzt werden sollten, hängt stark von den technischen Gegebenheiten sowie dem verfügbaren finanziellen und personellem Budget ab.

Grundlegend ist der Einsatz einer kommerziellen Lösung, vor allem unter dem Aspekt der fortlaufenden Rechtssicherheit empfehlenswert. Denn nur aktiv betreute Lösungen können den derzeit schnellen Änderungen rechtlicher Anforderungen gerecht werden. Für die Beurteilung des Anbieters dürfte hierbei vorrangig dessen Vertrauenswürdigkeit und wirtschaftliche Sicherheit ausschlaggebend sein. Diese dürfte bei den Consent Management und Privacy Compliance Plattformen eher gegeben sein, da diese in der Regel über Cookie Consent hinausgehende Marktsegmente bedienen und entsprechend wirtschaftlich unabhängig sind. Die Wahl eines Anbieters mit weiterführenden Compliance Angeboten, wie Datenschutz-, Risiko-, Vorfall- und Anfragenmanagement ist dann zu empfehlen, wenn eine über die Website hinausgehenden gesamtheitliche technische und organisatorische Unterstützung benötigt wird.

Open-Source-Lösungen bieten hingegen für technisch versierte Betreiber die Möglichkeit kostengünstig und mit größtmöglicher Freiheit rechtliche Konformität zu erreichen sowie bei entsprechendem Aufwand, die Rahmenbedingungen aktiv zu verfolgen und ggf. entsprechend zu reagieren.

06 ANHANG

QUELLENVERZEICHNIS

- Cookiebot, https://www.cookiebot.com
- CookieFirst, https://cookiefirst.com
- CookiePro by OneTrust, https://www.cookiepro.com
- Google Tag Manager, https://tagmanager.google.com
- Interactive Advertising Bureau (IAB) – TCF Transparency Consent Framework, https://iabeurope.eu/transparency-consent-framework
- ISO – ISO/IEC 27701:2019, https://www.iso.org/standard/71670.html
- iubenda, https://www.iubenda.com/en/cookie-solution
- Klaro!, https://heyklaro.com/
- Matomo Tag Manager, https://matomo.org/docs/tag-manager
- MDN web docs Mozilla – Web Storage API, https://developer.mozilla.org/en-US/docs/Web/API/Web_Storage_API
- MDN web docs Mozilla – IndexedDB API, https://developer.mozilla.org/en-US/docs/Web/API/IndexedDB_API

- MDN web docs Mozilla – Service Worker API, https://developer.mozilla.org/en-US/docs/Web/API/Service_Worker_API
- MDN web docs Mozilla – Cache, https://developer.mozilla.org/en-US/docs/Web/API/Cache
- OneTrust, https://www.onetrust.com
- OneTrust – Most Widely Used, https://www.onetrust.com/products/cookie-compliance
- Studien der Nielsen Norman Group, insbesondere zum E-Commerce, https://www.nngroup.com/reports/ecommerce-user-experience
- TrustArc, https://trustarc.com
- TrustArc – Cookie Consent Manager, https://trustarc.com/cookie-consent-manager
- unternehmer.de – Accelerated Mobile Pages (AMP), https://unternehmer.de/lexikon/it-lexikon/accelerated-mobile-pages-amp
- usercentrics CMP, https://usercentrics.com/de/
- WebAssembly, https://webassembly.org

SPE4CRM
Smart Privacy Engines for CRM

ÜBER SPE4CRM

Das Forschungsprojekt SPE4CRM hat sich zum Ziel gesetzt ein intelligentes Datenschutzmanagement unter Anwendung einer Smarten Privacy Engine (SPE) in CRM-Prozessen zu schaffen. Zu der Zielgruppe zählen klein- und mittelständische Unternehmen (KMU). Vor dem Hintergrund der DSGVO orientiert sich SPE4CRM dabei an den aktuellen und zukünftigen Anforderungen bei der Verarbeitung personenbezogener Daten im Unternehmen sowie beim Austausch zwischen Unternehmen. Dadurch schafft SPE4CRM Transparenz über vorhandene und verarbeitete Daten im Unternehmen.

Website: http://spe4crm.de/

netresearch

ÜBER NETRESEARCH

Die Netresearch DTT GmbH (NR) ist Part des Projektkonsortiums und liefert umfangreiche Dienstleistungen im Bereich E-Commerce. Im Rahmen der E-Commerce Beratung unterstützt das Unternehmen seine Kunden beim Aufbau einer wettbewerbsfähigen Strategie, der Auswahl geeigneter Tools und passender Partner sowie in der Umsetzung entsprechender Projekte. Das Leistungsportfolio umfasst dabei die Felder strategische, technologische und Online-Marketing Beratung sowie Softwareentwicklung, Systemintegration und Support bzw. Wartung.

Website: https://www.netresearch.de/

IMPRESSUM

Herausgeber
Netresearch DTT GmbH
Nonnenstraße 11c
04229 Leipzig
Tel.: 0341/478420
E-Mail: info@netresearch.de
Website: https://www.netresearch.de

Mitwirkende
Social CRM Research Center e.V.
Dittrichring 15
04109 Leipzig
Tel.: 0341/99359620
E-Mail: info@scrc-leipzig.de
Website: https://www.scrc-leipzig.de

Stand
November 2021

Haftungsausschluss
Die Netresearch DTT GmbH versucht mit größtmöglicher Sorgfalt, in dem vorliegenden Whitepaper richtige, vollständige und aktualisierte Informationen zur Verfügung zu stellen. Fehler können jedoch nicht völlig ausgeschlossen werden. Die Netresearch DTT GmbH übernimmt daher keinerlei Haftung oder Garantie für die Richtigkeit, Vollständigkeit, Qualität und/oder Aktualität der veröffentlichten Informationen, es sei denn, die Fehler wurden vorsätzlich oder grob fahrlässig begangen. Dies betrifft sowohl materielle als auch immaterielle Schäden Dritter, die durch die Nutzung des Informationsangebots verursacht werden.