Market Guide for Consent and Preference Management

5 August 2024 - ID G00781583 - 30 min read

By Nader Henein, Bart Willemsen, **and 1 more**

Central to most privacy laws is the challenge of giving users clarity around — and control over — their personal data. This guide helps security and risk management leaders navigate the market for universal consent and preference management capabilities and make informed, forward-looking decisions.

Overview

Key Findings

- Modern privacy regulations are expanding in footprint and adoption.
- Consumers are increasingly seeking more clarity around — and control over — use of their personal information.
- Changes across the adtech ecosystem and uncertainty around the retirement of long-standing tracking technologies (cookies) have given rise to complex, consent-driven workflows.
- Many organizations are finding themselves constrained by their technical capabilities as market shifts drive skyrocketing demand for granular, first-party consented data.

Recommendations

To build a user-centric consent and preference stack, security and risk management leaders should:

- Identify the target level of transparency by reviewing customer analytics and documenting consumer expectations. Capabilities chosen and deployed in isolation are rarely representative of consumer needs — resulting in a loss of time and investment.
- Avoid purchasing an overly “fitted” solution by defining a clear list of requirements based on future, rather than immediate, needs.
- Offset the cost and volume of subject rights requests (SRRs) commonly associated with modern privacy regulations by advancing the maturity of the organization’s consent and preference

management (CPM) solution. Move from a reactive posture toward a self-service model.
- Build a strong business case by addressing emerging adtech requirements early in the process. Maintain a partnership with marketing leadership, as their capacity to reach clients and prospects is becoming increasingly dependent on consent.

Market Definition

This document was revised on 5 August 2024. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Consent and preference management (CPM) platforms support all aspects of collecting, consolidating, synchronizing and applying end-user choices about personal data. The intent is to extend visibility and control to data subjects, enabling them to self-determine how much of their data to expose, to whom and for what purpose. For organizations, CPM platforms provide a strong foundation for compliance-backed data usage, with detailed tracking and auditability. They contribute to a solid consent program, making data monetization easier and more profitable. CPM platforms are delivered via software.

Central to most privacy laws is the challenge of giving users clarity around — and control over — their personal data. CPM platforms address this challenge by handling collection, consolidation, synchronization and usage of end-user choices. They empower data subjects with self-determination, enabling them to control how much personal data to expose, to whom and for what purpose.

For organizations, CPM platforms provide a strong foundation for compliance-backed data usage, with detailed tracking and auditability. In more fundamental terms, CPM platforms contribute to a solid consent program, making data monetization easier and more profitable.

Vendors in this market come in two categories:

- **Generalists:** These are traditionally privacy platform vendors that provide their offering as a set of modules, one of which is a CPM module. Generalists offer clients many capabilities under one umbrella and satisfy the requirements of 60% to 70% of the market.

- **Specialists:** These vendors focus almost exclusively on CPM, with substantial depth in terms of scale and capability. Specialists address the requirements of 95% of the market, with further extensibility and customization that will cover even the most demanding requirements.

CPM platforms are delivered via software. Functionality clusters into four service classes:

- **Core services:** These represent the base capabilities within CPM that enable the consolidation and storage of preferences from multiple repositories within a single source of truth.

- **User services:** These focus on collection and self-service interactions available to the end user.

- **Integration services:** These allow organizations to configure third-party services to both feed into and read from the single source of truth programmatically (via push or pull).

- **Administration services:** These provide monitoring, configurability and logging capabilities around consent and preference settings.

Mandatory Features

The mandatory features for this market include:

- **Core services:** In concert, core services enable the organization to maintain and enforce a unified view of user choices. Examples of core services include:

  - **Multidimensional preference matrices/single source of truth** enable the representation of highly configurable and granular consent structures.

  - **Harmonization engine** enables the platform administrator to connect into multiple preference repositories, providing bidirectional synchronization of user preferences with the CPM single source of truth.

  - **Tracker consent** extends configurable management of consent preferences, even when the site or app user has never registered.

Common Features

The common features for this market include:

- **User services:** Examples include consent collection, contextual and learning consent, layered workflow, offline interface, delegated consent, simplified opt-out, self-service interface, and bot-capable interface.

- **Integration services:** Examples include partner consent services, consent triggers, identity integration, rich APIs, direct marketing augmentation and mail gateway integration.

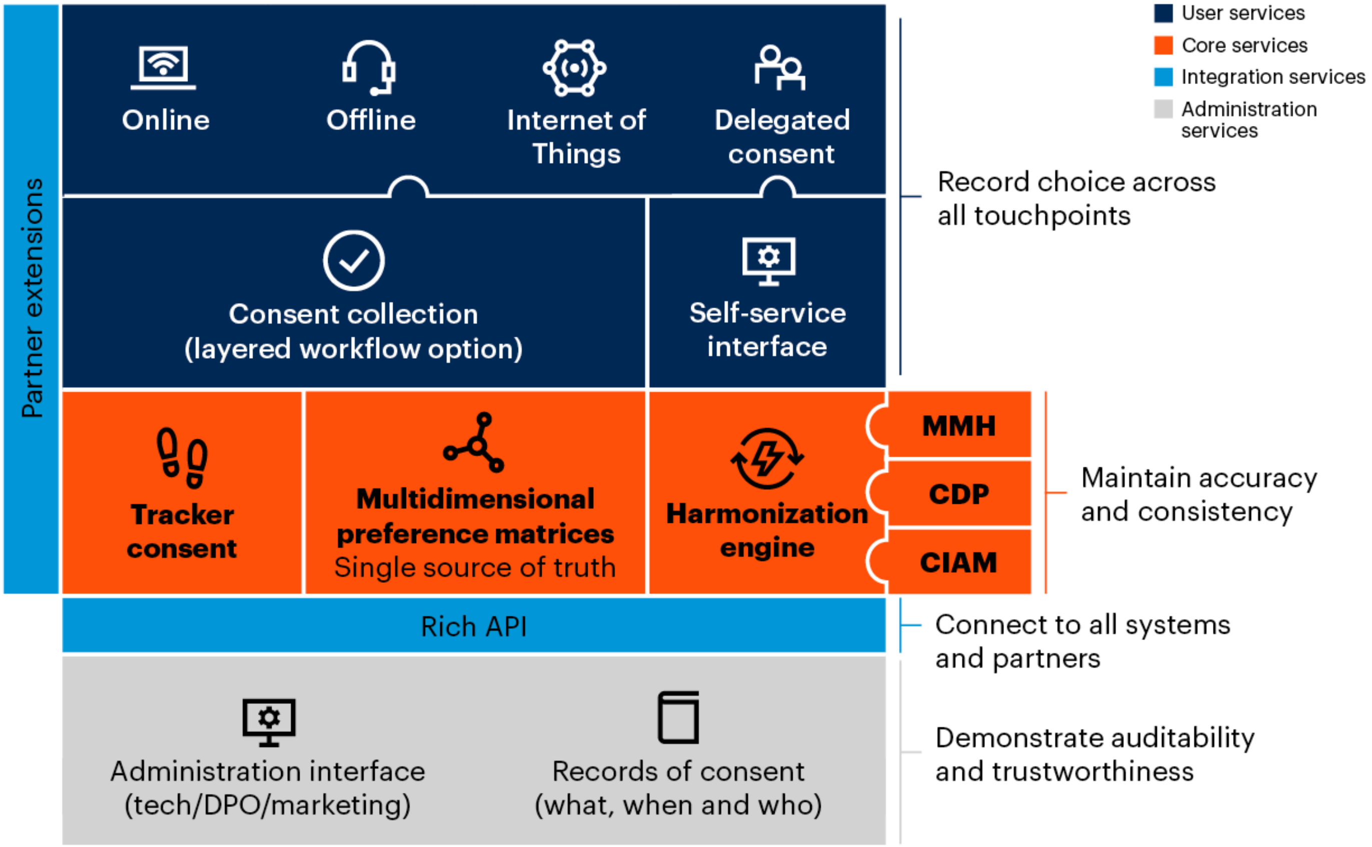
- **Administration services:** Examples include administration interface, records of consent and multitenancy.

Market Description

This market focuses exclusively on the CPM space. See Note 1 for markets that are out of scope. Figure 1 provides a high-level overview of the four service classes of CPM functionality, which are detailed further in the sections below.

Figure 1: Consent and Preference Management

Consent and Preference Management
Service ecosystem


User services
Core services
Integration services
Administration services
Partner extensions
Online
Offline
Internet of Things
Delegated consent
Consent collection (layered workflow option)
Self-service interface
Record choice across all touchpoints
Tracker consent
Multidimensional preference matrices
Single source of truth
Harmonization engine
MMH
CDP
CIAM
Maintain accuracy and consistency
Rich API
Connect to all systems and partners
Administration interface (tech/DPO/marketing)
Records of consent (what, when and who)
Demonstrate auditability and trustworthiness

Source: Gartner

CDP = customer data platform; CIAM = customer identity and access management; MMH = multichannel marketing hub; DPO = data protection officer

781583_C

Gartner

Core Services

- **Multidimensional preference matrices/single source of truth:** These allow for the representation of highly configurable and granular consent structures. As an example of marketing communication preferences, users may want to get football scores consolidated at the end of the day via email, whereas they may prefer to receive basketball updates as they happen via SMS.

- **Harmonization engine:** This enables the platform administrator to connect into multiple preference repositories, providing bidirectional synchronization of user preferences with the CPM single source of truth. The administrator should be able to configure rules to resolve collisions (such as two repositories showing conflicting preferences). The engine should have prebuilt connectors for popular providers — such as Salesforce (Marketing Cloud Account Engagement) and Adobe (Marketo Engage and Campaign) — backed by an API for custom integration.

The end result maintains a unified view of user preferences and propagates that view into other repositories. This synchronization of user preferences ensures that users have a consistent experience when dealing with various applications within one organization.

- **Tracker consent:** This refers to extending configurable management of consent preferences, even when the site or app user has never registered. The notion of “tracker consent” includes, but is not limited to, consent management for cookies, pixels, web beacons and tags. Offerings vary in terms of their capabilities. Some can manage only consent, while others can also control the actual trackers, cookies and scripts (including the prevention of preloading before a choice is made by the user).

User Services

- **Consent collection:** Configurability of endpoint-agnostic consent collection is supported through a variety of interfaces (such as web, mobile, in-person and set-top box) or purposes (such as advertising consent and communication preferences). When dealing with Internet of Things (IoT) deployments, security and risk management leaders should ensure that consent-based processing supports workflows to capture user preferences at the point of data collection.

- **Contextual and learning consent:** These capabilities allow administrators to solicit consent in the context of an activity when user data is needed, and to provide consumers with consent language and phrasing that is best-suited to them. These capabilities elicit much higher consent rates by tying the request to a user-initiated activity. For example, users configuring the color and specifications of a vehicle on a car manufacturer’s site would be asked if they want to store their preferences (in a cookie). This approach may be preferable to asking them if they consent to five categories of cookies when they first arrive on the website.

- **Layered workflow:** This provides for configurable, multistage, opt-in support features such as the double opt-in commonly used in Germany. With the double opt-in, the user grants consent on the site and later receives an email to confirm having granted consent. If the link in the email is not clicked within an allotted time, consent is rolled back.

- **Offline interface:** This allows consent administration capabilities to be conducted in person or through a service center agent. Many organizations collect and administer consent in person, on paper or over the phone, and users will expect them to continue providing the same channels to administer preferences.

- **Delegated consent:** This refers to providing workflows that support scenarios where the data subject is not able to, or is not legally authorized to, consent in person. For example, these workflows may be required when consent is collected from a parent or guardian on behalf of a minor.

- **Simplified opt-out:** This capability ensures that the user can opt out of certain processing activities with a simplified one-click process. It supports explicit requirements within privacy legislation, such as the Do Not Sell link/button specified under California's privacy laws. [1]

- **Self-service interface:** This refers to extending a preference center where users can administer their consent choices. Well-developed preference centers elevate an organization to a higher level of privacy management maturity — placing control back into the individual's hands.

- **Bot-capable interface:** This refers to allowing for an interactive, bot-driven consent collection process — as well as revalidation or, in some cases, revocation. Bots can achieve higher consent rates because they provide a more natural and interactive experience.

Integration Services

- **Partner consent services:** These capabilities support data sharing with third parties based on consent (e.g., with partners or service providers). They enable tracking and communication to those third parties of changes in consent or preferences. The Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection authority (DPA), provided guidance to organizations reinforcing the requirement for transparency and expedient user preference propagation when partners and data processors are involved. [2]

- **Consent triggers:** This refers to providing time-based or event-driven consent triggers for preference modification. An example would be revoking consent if the recipient of a marketing email does not open or click through three consecutive marketing mailers across a six-month period.

- **Identity integration:** This refers to APIs supporting identity resolution between the CPM single source of truth and an organization's customer identity and access management (CIAM) or master data management (MDM) platform. Alternatively, the API may support resolution for the new batch of alternative IDs in adtech, such as LiveRamp's RampID or The Trade Desk's Unified ID 2.0 (see Identity Resolution in the **Hype Cycle for Digital Advertising, 2023**).

- **Rich APIs:** APIs support integration with federated consent repositories and associated services such as service desk platforms. The APIs can provide custom integration capabilities, allowing marketers to capitalize on external data analytics and visualization.

- **Direct marketing augmentation:** This refers to services that utilize mail footer generation and administration — as well as pixel tracking — to gauge engagement for consent triggers.

- **Mail gateway integration:** These services passively monitor mail gateways for mass-mailer dispatch, to assess whether consent preferences (such as unsubscribe options) are consistently communicated. These services provide the administrator with a view of the number of mass mailers sent from the organization's mail gateway and the associated degree of conformity. Advanced mail gateway integration can block emails from dispatch that signal noncompliance to the sender. They can also inject preference management options directly into the email footer.

Administration Services

- **Administration interface:** This refers to configurable, role-driven dashboards with options for single sign-on (SSO) and enterprise identity integration. The interface provides a single console for all things related to CPM. It can provide different views for different role functions — such as data protection officers, IT support, service desk staff and marketing teams.

- **Records of consent:** This refers to maintaining tamper-proof consent logs to demonstrate each user's preferences over time. This module can issue and maintain consent receipts for nonrepudiation using various technologies such as blockchain. The ultimate goal is to demonstrate historic compliance and lineage.

- **Multitenancy:** This refers to providing nested capabilities to administer multiple sites, organizations or languages from one interface that has templating capabilities.

> **Off-Label Use of CPM Platforms**
>
> Under the GDPR and other comprehensive privacy regulations (such as the LGPD in Brazil or the PIPL in China), there must be a defined legal basis for processing personal information (e.g., consent).
>
> At more advanced levels of maturity, some organizations have repurposed CPM platform capabilities to act as a single source for the legal basis of processing. They employ the platform as an arbiter for the way personal data should be used, and to log when the data is processed.

Market Direction

The notion of consent management has been around for the better part of the past four decades. Today, universal consent and preference management (UCPM) has a strong foothold in the market. Sparked by the GDPR, [3] its forward momentum is supported by maturing privacy laws (such as Brazil's LGPD [4]) and emerging regulatory prerequisites for informed consent prior to the use of personal data in AI-driven projects. [5]

Developments

Two key aspects have accelerated the growth of the CPM market:

1. Continuing regulatory shifts across the privacy landscape at the regional, [6] country [4,7] and state [8,9] levels

2. Fundamental changes in the adtech ecosystem, [7] and increasing end-user demand for transparency

Consent verification started as nothing more than a simple checkbox exercise performed as part of web design best practices — more so than governance. It went no further than JavaScript form validation. Preferences were not logged because users could not proceed without blanket acceptance.

Now, regulatory requirements and consumer expectations have shifted. Organizations invest substantial resources into the full life cycle of user consent management. This process starts with endpoint-agnostic collection (including offline and in-person logging) and concludes with the validation of user preferences prior to processing. This overall approach to CPM allows individuals to easily modify choices at will — providing transparency and placing them in the driver's seat.

Although positioned differently in various regulations, the requirement to allow individuals to manage their consent is increasingly combined with preference management. Looking forward, visibility and control over the use, sharing and dominion of one's personal data will increasingly become consolidated. This consolidation will yield a unified privacy center where each individual will have broader transparency, enhanced effectiveness and a fluid privacy user experience (UX).

> **"Privacy UX" is a term that encompasses the full range of privacy-centered interactions between an individual and an organization. These interactions include privacy notices, data acquisition (through forms, cookies or otherwise), consent and preference management, and subject rights management.**

The market will start slowly moving toward a zero-touch model, where users are presented with a personalized dashboard in a privacy portal. Individuals will be able to browse their information in some detail, and understand how it is being used and by whom (inclusive of third parties). Users will then have granular control over their personal data.

This self-service approach addresses many aspects of CPM, thereby driving down costs by reducing the need for in-person interaction. The aim is to both fulfill the requirements of privacy laws and to act in the spirit of those laws. This objective involves placing control over personal data back in the hands of the individual. Organizations need to achieve this end without burdening the user while supporting the free flow of information and maintaining utility for the business.

Cautions

Avoid Dark Patterns in User Experience Design

"Dark patterns" are design choices that we often see for consent screens — built to trick or frustrate a user into opting in. They capitalize on the average user's lack of interest or understanding in order to elicit the desired response and gain access to user data. For example, cookie walls often exhibit dark patterns by providing site visitors with a simple, large, prominent opt-in button, whereas the opt-out requires a series of screens with long lists of incomprehensible choices. Throughout the whole experience, the opt-in button is prominent and ever-present — providing an easy way to “just move on.”

Security and risk management leaders should ensure that the configuration of their CPM front end:

- Prioritizes a balanced set of options
- Provides clear language to help users make an informed and explicit choice

Dark patterns are not a purely European concern. The Federal Trade Commission (FTC), which is charged with consumer protection in the U.S., has warned that it will use its regulatory powers to stop deceptive or unfair business practices associated with dark patterns. [10]

Beware That Adopting the Transparency and Consent Framework Does Not Automatically Translate Into GDPR Compliance

The Interactive Advertising Bureau (IAB), responsible for developing most of the standards within the online advertising industry, has released the Transparency & Consent Framework (TCF), currently in Version 2.2. [11] In its own words, IAB Europe states that the TCF “has the objective to help all parties in the digital advertising chain to comply with the EU’s General Data Protection Regulation …” [1] [2] This assertion, together with the IAB’s position in the industry, encouraged many CPM vendors to adapt their products for TCF.

TCF standardizes some very good privacy principles, and Google has made it a prerequisite [13] for organizations serving ads in Europe. *However, TCF does not immediately translate to GDPR compliance*. In October 2020, the matter reached privacy regulators, spurring a heated exchange between the Belgian DPA and the IAB. [14] In September 2022, the case was referred to the Court of Justice of the European Union (CJEU), which ruled in March 2024 that TCF requires substantive improvements. [15]

Market Analysis

Recently, Gartner conducted a detailed market sizing and forecasting study for data privacy. The CPM market has shown substantial growth, with an expected total end-user spend of $509 million in 2024 — a 27% increase from 2023. Moreover, we project consistent growth of more than 20% year over year for the coming five years. Detailed results are published in **Forecast: Information Security, Worldwide, 2022-2028, 2Q24 Update**.

We expect strong and steady growth to continue through a combination of investment, acquisition and consolidation. In fact, we are seeing rapid growth and substantial potential in the CPM space as:

- Regulations across the globe take root

- Seismic shifts across the adtech ecosystem move from an unconsented, cookie-based modality toward a consent-based, preference-driven future

> **Many organizations continue to hold large legacy volumes of ambiguous user consent, sitting in dozens of stand-alone repositories. These consent repositories represent considerable legal and financial risk if they remain unmanaged.**

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Vendor Selection

The intent of this Market Guide is to assist the work of security and risk management leaders focused on privacy program management. Overall, Gartner estimates that there are about 60 vendors in this market that can provide the foundational core services and at least one additional capability from each of the remaining three service categories. The 15 vendors listed here have been active in the market for at least four years, with most active for over five years (see Table 1).

The vendors are listed alphabetically alongside their respective CPM offerings. Development has been accelerated by market demand, but the potential for net new customers continues to represent a substantial opportunity, as does driving depth through further integration with existing clients.

Table 1: Representative Vendors in Consent and Preference Management

Vendor	Product Name	Headquarters	Founded
BigID	Privacy Suite	New York, U.S.	2016
Commanders Act	Trust Commander — part of Platform X	France	2010
Didomi	Consent Management Platform and Preference Management Platform	France	2017

Ketch	Consent and preference management	California, U.S.	2020
LuxTrust	Fair&Smart — Right Consents	Luxembourg	2005
OneTrust	Consent and Preferences	Georgia, U.S.	2016
Osano	Unified Consent & Preference Hub and Cookie Consent	Texas, U.S.	2018
PossibleNOW	MyPreferences	Georgia, U.S.	2000
PrivacyCheq	ConsentCheq	Pennsylvania, U.S.	2013
PRIVO	PRIVO iD and Parental Consent Platform	Virginia, U.S.	2001
Securiti	Consent Manager	California, U.S.	2018
Syrenis	Cassie	U.K.	2000
Tealium	Tealium	California, U.S.	2008
Transcend	Consent Management and Preference Store	California, U.S.	2017
Truyo	Consent & Preference Management	Arizona, U.S.	2017

Source: Gartner (August 2024)

Vendor Profiles

BigID

Established in 2016, BigID initially presented as a data-driven privacy vendor and has since expanded into data-centric security and governance on a common foundation of deep data discovery. BigID's machine learning (ML) graph-based technology correlates data knowledge with individual subjects or related data.

BigID has a series of modular apps (platform modules) across privacy, security and governance. The consent governance app can add its output to the data-handling rules automatically, and the cookie management app is designed to streamline cookie and consent management. Organizations can also build their own privacy and consent preference portals, alongside apps to streamline and automate management of data rights requests.

A focus on the individual is at the heart of BigID's data-centric approach to privacy protection. The offering is central to security and risk management leaders who want to automate a holistic privacy program.

Commanders Act

Established in 2010, Commanders Act offers Trust Commander for consent management within its customer data platform, Platform X. Trust Commander centralizes and automates the management (such as propagation) of individual consent and preferences in real time across all channels (and device types) where interactions take place. Notably, Trust Commander includes the capability to prevent activation of customer data without consent.

Similar to other vendor offerings focused on supporting adtech use cases, Trust Commander provides tag management capabilities. These help support user preferences on websites and prevent unauthorized tracking. Trust Commander can also integrate with other tag management solutions. This is relevant because tags are often managed by third parties and not the organization that owns the website.

Didomi

Established in 2017, Didomi has specialized in the CPM space exclusively since its inception. The scalable platform helps organizations use trust and compliance to generate revenue — making privacy a core part of business strategy through high site performance and customer engagement. Didomi has expanded across Europe and into North America, where evolving data protection legislation is driving demand for privacy technology.

Didomi offers a streamlined platform for managing consent and preferences, with customizable user interfaces powered by advanced enterprise technology. Didomi has maintained a strong developer focus so that its clients can build customized experiences through separate web, mobile, Accelerated Mobile Page (AMP) and Connected TV (CTV) software development kits (SDKs).

The company also offers a plug-and-play compliance module with automated web scanning, obtained through its 2022 acquisition of Agnostik, an e-privacy technology vendor. Among other capabilities, the Agnostik compliance module provides breach alerting and privacy health reporting.

Ketch

Ketch was founded in 2020. Its Data Permissioning Platform is a coordinated set of applications, infrastructure and APIs that simplify privacy operations and mobilize responsibly gathered data for AI-driven initiatives. Ketch CPM is responsive to global regulations, and customizable to customer preferences.

The Ketch offering is multichannel and cross-device, utilizing native identity infrastructure to consolidate privacy choices across devices and digital IDs. Using a permit vault, Ketch stores consent and permitted use, with instant lookback and total recall for auditability and reporting.

Importantly, Ketch also records and propagates consent and enforces permitted use instructions throughout an organization's data architecture. Consents given or withdrawn translate into immediate access that is provided or revoked within the relevant systems, including vendor systems. Ketch privacy capabilities also include SRR automation, data discovery and classification, risk assessments and intelligence, and automation of end-of-life of personal data.

LuxTrust

Established in 2005, LuxTrust (previously Fair&Smart) is a European qualified trust service provider (QTSP) registered on the EU/EEA Trusted List for the eIDAS Regulation. It took over Fair&Smart's solutions addressing the two principal aspects of privacy UX: subject rights management (Right Requests), and consent and preference management (Right Consents). The CPM solution is constructed to support key roles, with purpose-built interfaces for data protection officers (DPOs), marketing teams and IT teams in charge of platform integration.

The platform is designed to facilitate personal data sharing, with a user-centric consent collection process that can be distributed among multiple stakeholders. Created in France, the solution is exclusively European-owned, run and hosted — a key differentiator for many concerned with data residency and data sovereignty.

OneTrust

Established in 2016, OneTrust offers a suite of modules and packages for organizations to customize a solution most relevant to their needs. This suite helps organizations succeed in building trust and making an impact.

The Consent and Preferences solution includes a set of modules that enable organizations to deliver trusted experiences in the age of modern privacy. The solution allows organizations to capture consent and preferences through web forms, mobile apps, websites and APIs — centralizing the data in one location. Organizations can build self-service trust centers for consumers to view consent history, indicate communication preferences and easily manage their data.

The platform supports automated workflows and out-of-the-box integrations with marketing and data platforms. The OneTrust Consent and Preferences solution integrates seamlessly with the wide range of privacy and data governance capabilities from OneTrust. Capabilities include website scanning and automated processing of privacy rights requests.

Osano

Established in 2018, Osano provides a data privacy compliance platform that helps businesses comply with privacy regulations, such as GDPR and CCPA/CPRA, in over 50 countries.

In 2023, Osano acquired Wirewheel. It merged Wirewheel's capabilities into its existing platform to offer comprehensive CPM capabilities together with its expanding suite of privacy-focused modules.

PossibleNOW

Founded in 2000, PossibleNOW provides MyPreferences, a unified approach to managing the subject's consents and preferences across all touchpoints. Purpose-specific consent can be captured via tailored notices by region or by data category. Consent is captured on individual customer profiles and put into effect across all interactions with that customer — whether through web, app, social media, mobile or other means.

MyPreferences provides an Experience API to manage all aspects of consent and preference experiences throughout the customer journey. It also supports management of a global consent and preference repository through a webhook framework, API connectivity, and established integrations with over 200 SaaS, cloud and app adapters.

In addition, MyPreferences includes built-in audit and change logging, end-to-end configuration management, and a variety of intelligent data validation options. It supports compliance with Do Not Contact regulations, including the Telephone Consumer Protection Act (TCPA), Reassigned Numbers Database (RND), and Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act.

PrivacyCheq

Founded in 2013, PrivacyCheq provides offerings for organizations to manage privacy notices through a novel "nutrition facts" visualization that is easy for consumers to understand.

ConsentCheq is a cloud-based platform that focuses the recording and management of individual consent into a single source of truth. When consent is given or updated, the version of the privacy policy is recorded. The policy is also recorded when adaptations are made to accommodate the requirements of a particular jurisdiction. The platform is also designed to provide a self-service portal for individuals to request a history of their consent.

ConsentCheq includes a parental dashboard for parents and guardians to manage the consent given on behalf of minors under their care. The API sits at the center, orchestrating consent collection from a wide variety of touchpoints and facilitating downstream notification to third parties that need consent to act on user data.

PRIVO

PRIVO was established in 2001 in response to the introduction of the Children's Online Privacy Protection Act (COPPA). In 2004, PRIVO became an FTC-approved COPPA Safe Harbor certification provider.

PRIVO later developed a dedicated identity and consent management platform for children and minors to handle complex use cases of delegated consent across industry verticals, extending far beyond traditional consumer youth- and family-focused fields. These included fields such as edtech, healthcare, and age-restricted products and services.

The platform offers multiple complementary capabilities, such as age verification and parent-child relationship association. It also offers PRIVO iD, a single sign-on credential. Although its roots lie in the U.S., the offering is universal. Its focus is on safeguarding children's personal data collected online — a critical requirement as people shift to online learning and as the embedded brand engagement in social and gaming platforms attracts more children.

Securiti

Established in 2018, Securiti offers a suite of privacy management and data-centric controls to support a competitive privacy program. Securiti's UCPM offering is available as a stand-alone product but maintains close integration with the full-stack privacy suite and data control platform.

The UCPM offering can dynamically capture and synchronize consents recorded while offering full customization — including workflow automation spanning numerous applications (both SaaS and private). Securiti's CPM deployments (often as part of a broader privacy program) support numerous stakeholders focused on privacy and a comprehensive privacy UX.

Syrenis

Syrenis was established in 2000. Cassie, the company's UCPM platform, enables enterprises to deliver compliant communications across global legislation.

The solution is fully customizable. Consents and preferences are collected centrally — and held in a blockchain-based audit log — through multiple channels, including advanced consent banners, embedded widgets or comprehensive APIs. Advanced matching and grouping capabilities then automatically identify consent records across profiles, personas and devices. Built with an API-first architecture, the product is equally capable of handling data from legacy systems through data loader functions.

Through the Customer Service Portal and the Preference Center, individual data subjects can maintain granular control over how their data is used and shared, with changes reflected in near-real time. The platform is industry-agnostic and has been successfully implemented in a range of verticals, including healthcare, financial services, automotive and retail.

Tealium

Founded in 2008, Tealium offers the Customer Data Hub, which enables organizations to centralize all data about individuals in one vendor-neutral location. Data about each individual is collected across all potential interaction points — and offline sources where data may be stored — with the consent provided where applicable.

Organizations can then customize business rules to standardize, transform and enrich the data for each individual into cross-device profiles. This includes reconciling consent and preferences across devices. These choices are enforced throughout the customer relationship.

Tealium further provides extensions and transformations, so organizations can tokenize or remove identifiable data (such as email addresses) at the point of collection, or at server-side ingestion, to provide additional protection of personal data. Self-service portals are supported, giving individuals full control over their choices and permissions, including whether their data can be shared with third parties, and for which purposes.

Transcend

Founded in 2017, Transcend quickly emerged as a major player in the market. Its unified privacy and data governance platform helps companies of all sizes better govern their data, thereby simplifying compliance and improving business and operational resilience.

The offering comprises a full-stack consent platform with highly customizable capabilities to collect consent and automate enforcement across many interfaces. These interfaces range from websites to mobile apps and back-end systems, such as marketing platforms and customer data platforms (CDPs).

Truyo

Launched in 2017, Truyo is a collaboration between Intel and IntraEdge. It aims to deliver a comprehensive suite of privacy capabilities and an integrated AI governance platform.

The platform enables a fully automated CPM life cycle, with automated data subject access request (DSAR) response via hundreds of fully automated connectors. These capabilities are provided both through an administrative dashboard and through a touchless privacy portal for self-service. Truyo supports Global Privacy Control (GPC), Do Not Sell (DNS), and a multitude of state and international regulations with one click.

Market Recommendations

Organizations have struggled to clarify how personal data is used and to give users control over their information — while still maintaining the utility of the data for the business. Larger organizations often have multiple solutions with different consent-handling practices for a single consumer. This disparity places the organization at risk, and it projects disarray where users expect consistency.

As a security and risk management leader responsible for developing a transparent and scalable privacy practice, you should take the following steps to build a user-centric consent and preference stack:

- **Move to consolidate and centralize consent stores immediately.** This is crucial, as violations are easily recognizable by consumers and the majority of fines are levied following consumer complaints. Moreover, procrastinating and adopting a wait-and-see approach will result in a diminished capacity to market and monetize.

- **Develop a close partnership with marketing to support their capacity to reach clients and prospects.** Changes across the adtech ecosystem have shifted the focus from traditional tracking capabilities to a reliance on properly consented repositories of first-party data.

- **Assess products, allowing for growth and development.** The intent is to invest, not merely to sample. Identify where gaps exist, and prepare to deploy capabilities to strengthen areas with a higher privacy risk first.

- **Start with the core services to build a single source of truth.** Do not try to do everything at once when deploying CPM capabilities. Some overlap may exist in the short term. This is to be expected. Continuously assess consent-based data-processing activities, and take a privacy-risk-based approach. Work your way down the list from high risk to low risk, ensuring that each activity maps to clear and affirmative consent.

- **Reduce the number of SRRs by giving users back their control.** Many SRRs, especially deletion requests, are born out of user frustration with a perceived lack of control over their data. Restoring this control not only saves costs by reducing SRRs over time, but also fosters customer trust and further enhances the users' relationship with the organization. Aim for a zero-touch model, benchmarking how improved transparency lowers the volume of SRRs and, by extension, the cost to the organization.

- **Treat consent and preference management as more than a compliance target.** Emphasize a customer-centric approach, and promote respect for individual privacy as a core organizational value. This approach will, in turn, drive trust for the existing customer base and attract prospects. It will help the organization to reestablish itself, not just as the best provider of a product or service, but also as the safest place for customer data.

Evidence

[1] Chapter 20. California Consumer Privacy Act Regulations: Article 3. Business Practices for Handling Consumer Requests: 999.315 Requests to Opt-Out (PDF), State of California Department of Justice.

[2] Prospecting Towards Individuals (B to C): What Are the Rules for Transmitting Data to Partners? (French-language source), CNIL.

[3] Art. 7 GDPR: Conditions for Consent, Paragraph 3, intersoft consulting services.

[4] An Introduction to the LGPD — Brazil's Comprehensive New Privacy Law, JD Supra.

[5] Luján, Welch Introduce Bill to Require Online Platforms Receive Consumers' Consent Before Using Their Personal Data to Train AI Models, website of Ben Ray Luján, U.S. Senator for New Mexico.

[6] General Data Protection Regulation, EUR-Lex.

[7] Digital Personal Data Protection Act 2023 (PDF), Ministry of Law and Justice (Legislative Department), Government of India.

[8] Attorney General Becerra Announces Approval of Final Regulations Under the California Consumer Privacy Act, State of California Department of Justice.

[9] Proposition 24: More Data Privacy, CalMatters.

[10] Bringing Dark Patterns to Light, U.S Federal Trade Commission.

[11] What Is the Transparency & Consent Framework (TCF)? IAB Europe.

[12] IAB Europe Transparency & Consent Framework Policies, Chapter 1.1 (PDF), IAB Europe.

[13] New Consent Management Platform Requirements for Serving Ads in the EEA and UK, Google.

[14] IAB Europe's Ad Tracking Consent Framework Found to Fail GDPR Standard, TechCrunch.

[15] IAB Transparency and Consent Framework Must Be Improved, Taylor Wessing.

Note 1: Out-of-Scope Markets

Please note that vendors in the following markets are not included in this Market Guide:

- **Customer identity and access management (CIAM):** These vendors provide identity and access management for customers focused on fraud detection and authentication.

- **Web tracker consent vendors:** These vendors provide consent management only for web tracking technologies, such as cookies, tags and pixels. They do not provide a complete picture of user consents and preferences.

- **Identity resolution (IDR) vendors:** Some IDR vendors can track consent and preferences. However, their main product focus is on locating and matching customer identity records across multiple datasets derived from customer interactions with the brand at multiple touchpoints.

- **Non-stand-alone CPM platform providers:** These vendors provide consent and preference solutions only within their own platforms, such as customer data platforms (CDPs) or multichannel marketing hubs (MMHs) that provide consent capabilities.

Disclaimer: The organization (or organizations) profiled in this research is (or are) provided for illustrative purposes only, and does (or do) not constitute an exhaustive list of examples in this field nor an endorsement by Gartner of the organization or its offerings.