

Ultimate Guide to
**Comprehensive Consent
and Preference
Management**



TABLE OF CONTENTS

Introduction	1
What Is Opt-Out Management?	2
What Is a Cookie?	3
What Are Pixels, Scripts, and Tags?	3
What Is a Comprehensive Consent and Preference Management System?	4
What Is the Difference Between Consent and Preference Management?	5
What Are Probabilistic IDs and Deterministic IDs?	6
When Should You Use Consent Management?	6
Why Do We Need Consent Management?	7
Consent Management and Compliance Under GDPR	8
Consent Management and Compliance Under US State Laws	8
Consent Management and Identity	9
What Is Global Privacy Control, and Why Is It Important?	9
Comprehensive Consent and Preference Management for Trust	11

Navigating Privacy Regulations and Building Consumer Trust

Now more than ever, businesses must balance digital marketing with privacy and data protection. Consent and choice management plays a crucial role in maintaining compliance with privacy regulations and fostering trust among customers and prospects.

In this comprehensive guide, we'll explore various aspects of choice management, including opt-out management, cookies, pixels, scripts, tags, and the role of consent management platforms.

We'll also examine how consent management relates to compliance under U.S. State and Federal laws, along with international regulations like the General Data Protection Regulation (GDPR) and the General Personal Data Protection Law (LGPD). And we'll cover the critical connection between consent management and consumer identity.

But first, let's start with some definitions.

What Is Opt-Out Management?

Opt-out management refers to the process of allowing customers to withdraw their consent or “opt-out” of having their personal data collected, used, or shared by a business. This is an essential component of privacy compliance, as businesses must respect their customers’ choices and provide them with the option to opt-out of data collection practices. Opt-out management ensures that businesses only process personal data for customers who have explicitly consented, thereby maintaining compliance with privacy regulations and fostering trust among customers.

Within comprehensive privacy laws in the United States, for example, there are two specific opt-outs that companies should support:



Opt-Out of Sale or Share of Personal Information

Under California Privacy Rights Act (CPRA), consumers have the right to opt-out of the sale or sharing of their personal information. Businesses must provide a clear and conspicuous link on their website or mobile app, titled “Do Not Sell or Share My Personal Information,” leading to a webpage where consumers can exercise this right. The opt-out process should be easy to navigate and should not require the creation of an account or unnecessary steps.



Opt-Out of Targeted Advertising

Within the Colorado Privacy Act (CPA), however, businesses must provide consumers with the option to opt-out of targeted advertising, as selling personal information for targeted advertising purposes may be considered a sale under the law.

What Is a Cookie?

A cookie is a small text file that a website stores on a user's device when they visit the site. Cookies are used to store information about a user's browsing activities, preferences, and other data that helps improve their experience on the website. They enable businesses to deliver personalized content, remember user preferences, and track user behavior across multiple visits. However, as cookies collect personal data, businesses must obtain user consent before setting cookies on their devices, in accordance with privacy regulations

What Are Pixels, Scripts, and Tags?

Pixels, scripts, and tags are various methods used by websites and marketing platforms to track user behavior and collect data for analytics, advertising, and personalization purposes.



A **pixel** (also known as a tracking pixel or web beacon) is a small, transparent image that is embedded in web pages or emails. When a user loads the page or opens the email, the pixel sends information back to the server, allowing businesses to track user behavior and engagement.



A **script** is a piece of code embedded in a web page that enables the execution of specific functions, such as loading external resources, collecting data, or making updates to the page's content. Scripts can be used to track user behavior, implement analytics, and deliver personalized content.

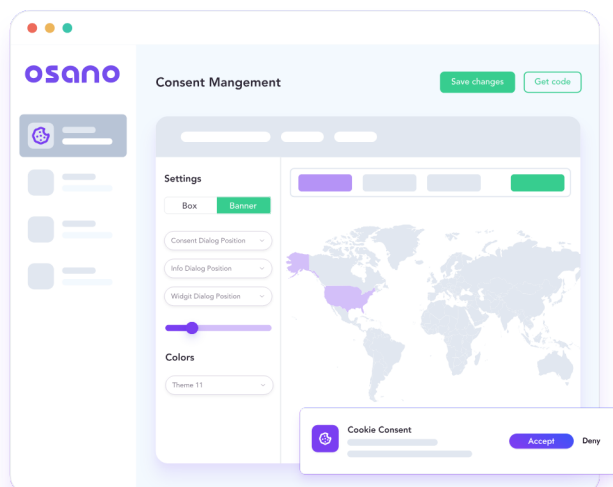


A **tag** is a snippet of code that is added to a website to enable third-party tracking, analytics, or marketing tools. Tags are often used to deploy and manage pixels, scripts, and other tracking technologies. Tag management systems can help businesses streamline the implementation and management of tags on their websites.

What Is Consent Management?

Consent management is the process of obtaining, managing, and documenting user consent for the collection, processing, and sharing of their personal data. It involves informing users about data collection practices, obtaining their explicit consent, and ensuring that businesses adhere to privacy regulations when processing personal data.

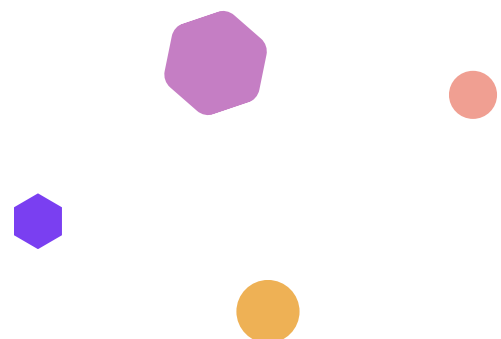
Consent management also includes logging and tracking consent collection, enabling businesses to remain compliant with global privacy regulations and maintain customer trust.



What Is a Comprehensive Consent and Preference Management System?

A Comprehensive Consent and Preference Management System (CCPM) is a tool that helps businesses manage and monitor consumer consent for data collection, processing, and sharing. CCPMs automate the universal consent process, allowing businesses to obtain user consent, track first-party data, and enable users to update their preferences easily.

With a CCPM, businesses can gain insights from the moment a user opts in, tracking and responding to data subject requests and consent preferences.



What Is the Difference Between Consent and Preference Management?

A consent is a choice that, under a law, regulation, or other legal obligation, a consumer (or data subject) must be given with respect to their personal information. Consent management is therefore the process of obtaining and managing customer consent to collect, store, and process their personal data. Consent management ensures that businesses adhere to privacy regulations and only process personal data for customers who have explicitly consented. It typically involves “opt-in” or “opt-out” mechanisms for customers to express their consent preferences.

A preference, on the other hand, is any non-legally required choice, like how often you might want to receive emails or other notifications.

Preference management is therefore the process that allows users to make choices about the frequency, topics, and channels of communication they receive from a business. Preference management focuses on enhancing the user experience by allowing customers to provide zero-party data (i.e., data they willingly share) and customize their interactions with a brand.

Here are a couple of examples:

- **Consent:** *In California, a consumer must be given a choice that declares, “Do Not Sell or Share My Personal Information.”*
- **Preference:** *An example of a preference is, “Please notify me about new products or services via email.”*

These can be a little bit confusing, but it’s important to remember that **consent is a legally required choice**, whereas **a preference is optional**.

What Are Probabilistic IDs and Deterministic IDs?

When many people visit a website or a mobile app, they do not log in or actually identify themselves.

So the mobile app or the web app might know you as a device ID, your IP address, or other information about your browser... but it doesn't know who you actually are.

These are called **probabilistic IDs**, because there's a PROBABILITY that the company can figure out who you are from this information... but not for sure.

A **deterministic ID** means you have probably logged in in some way and proven exactly who you are. By the way, deterministic IDs are often collected in addition to the device ID, IP address or other probabilistic IDs.

A good example is a family with a shared computer. A company might be able to guess that a parent is using the computer, instead of a child, based on the probabilistic ID, but it cannot know for sure until the parent logs in. Once the parent logs in, then the company has a deterministic ID for the parent.

When Should You Use Consent Management?

Generally speaking, consent management should be used whenever a business collects, processes, or shares personal data from its customers.

The specific fashion depends on the type of data, the context, and applicable legal regime.

For example, in a number of US States, a company must obtain specific opt-in permission to collect sensitive personal information like location data. Other choices must be presented as "opt-out" options, including the selling or sharing of data for targeted advertising



Similarly, according to the General Data Protection Regulation (GDPR), consent is one of the six lawful bases for processing personal data. Obtaining consent is often the most appropriate method for businesses to ensure they're compliant with privacy regulations.

Why Do We Need Consent Management?

Consent management is crucial for several reasons:



Trust: It's critical for companies to give consumers and data subjects fair notice of how their data is being collected, shared, and processed, together with the ability to opt-in or opt-out of those choices. Without that, companies can seriously damage their reputations.



Compliance: The United States, states within the United States, and countries around the world require consent management, and prohibit collection, storage, and processing without it. These include CPRA, Virginia, Connecticut, Utah, and GDPR. Comprehensive Consent and Preference Management helps businesses maintain compliance by ensuring they only process personal data where the right opt-in or opt-out has been made available.



Fines: Failure to provide Consent and Preference Management can expose companies to serious fines and penalties.



Digital Experience: By allowing users to control their consent preferences, consent management contributes to a more personalized and customer-centric experience.

Consent Management and Compliance Under GDPR

Under GDPR, businesses must obtain explicit consent from users before collecting, processing, or sharing their personal data. Article 7 of GDPR outlines the conditions for obtaining consent, including:

- The ability to demonstrate that a user has provided consent for data processing.
- The presentation of consent requests in an easily distinguishable manner.
- The right for users to withdraw consent at any time, without affecting the lawfulness of processing based on consent before withdrawal.
- Ensuring that consent is freely given and not conditional on the performance of a contract.

Consent management helps businesses stay GDPR compliant by adhering to these requirements and documenting the consent process.

Consent Management and Compliance Under U.S. State Laws

The CPRA, along with the other 13 U.S. state data privacy laws (as of this writing) also requires businesses to obtain and manage user consent for data collection, processing, and sharing. Key aspects of CPRA compliance related to consent management include:

- Providing users with clear, comprehensive information about data collection practices.
- Offering a “Do Not Sell or Share My Personal Information” link on the business’s website to allow users to opt-out of the sale and sharing of their data.
- Implementing processes for handling data subject access requests and opt-out requests.

Consent management enables businesses to maintain compliance with the CPRA by addressing these requirements and fostering transparency in data processing practices.

Consent Management and Identity

Consent management is closely linked to identity management, as both processes involve handling and protecting customer data. Identity management focuses on verifying user identities, managing access to resources, and ensuring the security of customer data.

Consent management complements identity management by ensuring that businesses only process personal data for customers who have explicitly consented, thereby enhancing data protection and privacy

What is Global Privacy Control?

And Why Is It Important?

As a privacy professional, it's important to stay up-to-date with the latest regulations and technologies that help you protect consumer data.

One such technology you should be aware of is [Global Privacy Control](#) (GPC).

So, what exactly is the GPC? In a nutshell, it's a protocol that allows consumers to set a choice about the sharing of their data, and other legally required consents, right in their browser.

This means that users can easily opt-out by turning on the global privacy control in their browser. This protocol is gaining traction, particularly in states like California and Colorado, where the states are checking websites to ensure that they can detect and enforce the GPC.

For Your Website Owner: How to Integrate the GPC Signal into Your Website or Application

Integrating the Global Privacy Control (GPC) signal with your website will vary based on your marketing stack. In most cases, the GPC signal will be a means to automate a user's privacy preferences without having to interrupt their user experience on your website.

For Your Website Owner: How to Integrate the GPC Signal into Your Website or Application

Integrating the Global Privacy Control (GPC) signal with your website will vary based on your marketing stack. In most cases, the GPC signal will be a means to automate a user's privacy preferences without having to interrupt their user experience on your website. There are a few ways this can be accomplished:

Consent Management -

Automating a user's consent decision to prevent the firing of pixels and tags that collect or track user information is a primary use case of the Global Privacy Control. Your website owner can listen for this signal and respect the users' consent decision without the need for banners and complex forms.

Data Collection & Processing -

For organizations that collect user information, the GPC signal can be incorporated into your forms and passed through to your backend systems so that they understand how this information can be used based on the user's privacy preferences.

Why Do I Need to Adopt the GPC?

After the Sephora decision, it is expected that businesses take into account automated signals like the Global Privacy Control giving users a chance to express their consent before trackers are set.

For businesses, this means that companies need to ensure the GPC signal is being considered before data collection occurs so you are not collecting any information from consumers without their consent.

In today's digital world, understanding and respecting Global Privacy Control is essential for organizations to remain compliant with the latest regulations on consumer privacy protection.



→ **Access Your Copy** of the Sephora Enforcement Action Breakdown

Comprehensive Consent & Preference Management for Trust

Managing preference and consent is a crucial aspect of data privacy and security. It's essential to ensure that users are aware of the data being collected, how it is being used, and who it is being shared with.

By prioritizing user privacy and security, your organization can build trust and foster long-term relationships with your customers. Because companies with an eye toward privacy will become part of the next wave of trusted brands.

Interested in Learning More?

Explore Osano's Comprehensive Consent and Preference Management and learn about our Data Privacy Platform.

[Schedule a Demo](#)



@osano



[linkedin.com/company/osano](https://www.linkedin.com/company/osano)



[http://facebook.com/osanoatx](https://www.facebook.com/osanoatx)



osano.com



About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 websites to capture consent for more than 2.5 billion monthly visitors.

Copyright © 2024 Osano, Inc., a Public Benefit Corp. Osano is a registered trademark of Osano, Inc.