wirewheel

# Ultimate Guide to **Preference and Consent Management, and the Global Privacy Control in Healthcare**

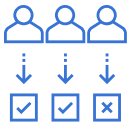
## Healthcare practices today face a formidable task: maintaining compliance with stringent privacy regulations such as HIPAA, while also engaging in effective digital marketing.

In this guide we provide an overview of the complex relationship between consumer choice management and privacy laws to help healthcare organizations balance these needs. We dive deep into topics like opt-out management, cookies, pixels and scripts for a deeper understanding of consent requirements. Featuring use cases where fines were levied for violations as well as insights into how WireWheel is leading the way in managing customer identities through responsible practices involving consent management protocols - helping ensure peace of mind so that both patients & medical providers can feel secure no matter what communication methods they choose!

# 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.

Under California Consumer Privacy Act (CCPA), for example, there are two specific opt-outs that companies should support:



### Opt-Out of Sale of Personal Information:

Under CCPA, consumers have the right to opt-out of the sale of their personal information. Businesses must provide a clear and conspicuous link on their website or mobile app, titled "Do Not Sell 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:

Though not explicitly stated in the CCPA, businesses should consider providing 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. By offering an opt-out mechanism for targeted advertising, businesses can reduce the risk of non-compliance.

wirewheel

# What is a Cookie?

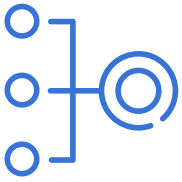
A cookie is a small text file that a website stores on a user's device when they visit the site. Cookies are used to store information about a user's browsing activities, preferences, and other data that helps improve their experience on the website. They enable businesses to deliver personalized content, 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.


*Nike's example of a cookie notice*

# 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.

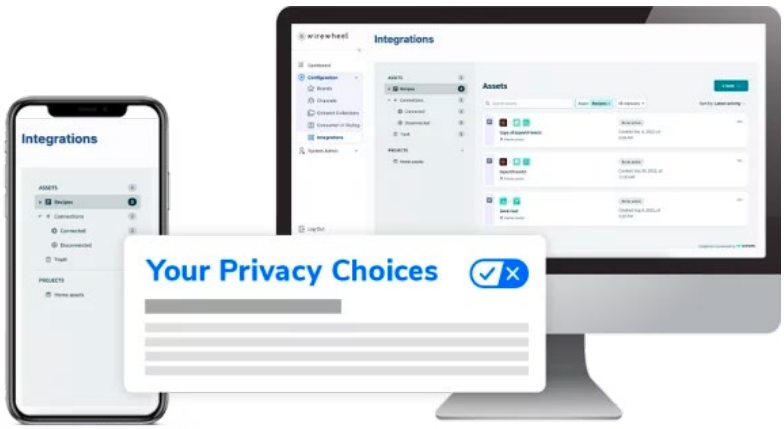
# What Is Consent Management?

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 Universal Preference and Consent Management Platform?

A Universal Preference and Consent Management Platform (UPCP) is a tool that helps businesses manage and monitor customer consent for data collection, processing, and sharing. UPCPs automate the consent process, allowing businesses to obtain user consent, track first-party data, and enable users to update their preferences easily.

With a UPCP, 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.

> **Let's just walk through a couple of examples.**
>
> ***For example, in California, a consumer must be given a choice that declares: "Do Not Sell My Personal Information." That is a consent.***
>
> ***The FTC alleged BetterHelp shared its customers' sensitive health data with third-parties such as Facebook and Snapchat for advertising purposes, contrary to online representations the company made to customers.***

These can be a little bit confusing, but it's important to remember **that a consent is a legally required choice,** whereas a **preference is one that 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, it might know your IP address, or it might know 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.

That is the difference between a probabilistic ID and a deterministic ID.

# 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.

Obtaining consent is often the most appropriate method for businesses to ensure they’re compliant with privacy regulations.

## States and Regions Where Consent is Required

*As of June 2023*

**European Union**

**California**

**Colorado**

**Connecticut**

**Indiana**

**Iowa**

**Montana**

**Utah**

**Virginia**

You can see more about the specific legal requirements **here.**

# 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 CCPA, CPRA, Virginia, Connecticut, Utah. Universal Preference and Consent 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 Preference and Consent 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.

**In February 2023, the FTC fined GoodRx $1.5M for Sending Medication Data to Facebook and Google for Ads**

**In March 2023, BetterHelp found itself in hot water with the FTC over allegations of deceptive marketing practices and violations of both data tracking and health privacy regulations. The settlement resulted in a fine of $2.2 million and requirements for BetterHealth to implement stronger privacy and data security measures.**

By being transparent about data collection, following health privacy regulations, implementing strong data privacy measures, and training employees on compliance, digital marketing leaders can avoid costly consequences and protect their customers' personal information.

# Consent Management and Compliance Under US State Laws:

California

Virginia

Connecticut

Colorado

Iowa

Montana

Indiana

Utah

The CCPA also requires businesses to obtain and manage user consent for data collection, processing, and sharing. Key aspects of CCPA compliance related to consent management include:

- Providing users with clear, comprehensive information about data collection practices
- Offering a “Do Not Sell 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 CCPA 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 digital marketing leader, it's important to stay up-to-date with the latest regulations and technologies that impact your industry.

One such technology that you should be aware of is the **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.

## As a Website Owner, How Do I integrate the GPC Signal Into My Website or Application?

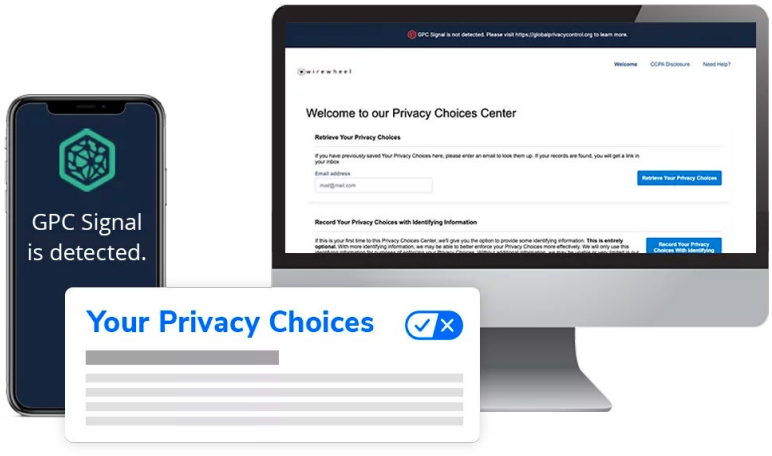
Integrating the Global Privacy Control (GPC) signal with your website will vary based on your marketing stack. In most cases, the GPC signal will be a means to automate a user's privacy preferences without having to interrupt their user experience on your website. There are a few ways this can be accomplished:

**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. As a website owner, you 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.

wirewheel

# WireWheel Leads the Way With Its **Universal Preference and Consent Management Platform**

**WireWheel offers an industry-leading consent management platform that helps businesses maintain compliance with privacy regulations while fostering customer trust. WireWheel's consent management features include:**

- Client-side governance for cookies, scripts, tags and pixels
- Service-side connections for more than 700 systems, including CRMs and marketing systems
- Simple connections into identity management systems, like Ping, Auth0, and more
- Support for multiple brands and channels (web, mobile, connected TVs)
- Configurable Out-Of-The-Box User Experiences
- And more!

---

**See for yourself how WireWheel's Universal Preference and Consent Platform allows you to implement Global Privacy Control (GPC) with a single line of code.**

**Get Started for Free for 30 Days!**

---