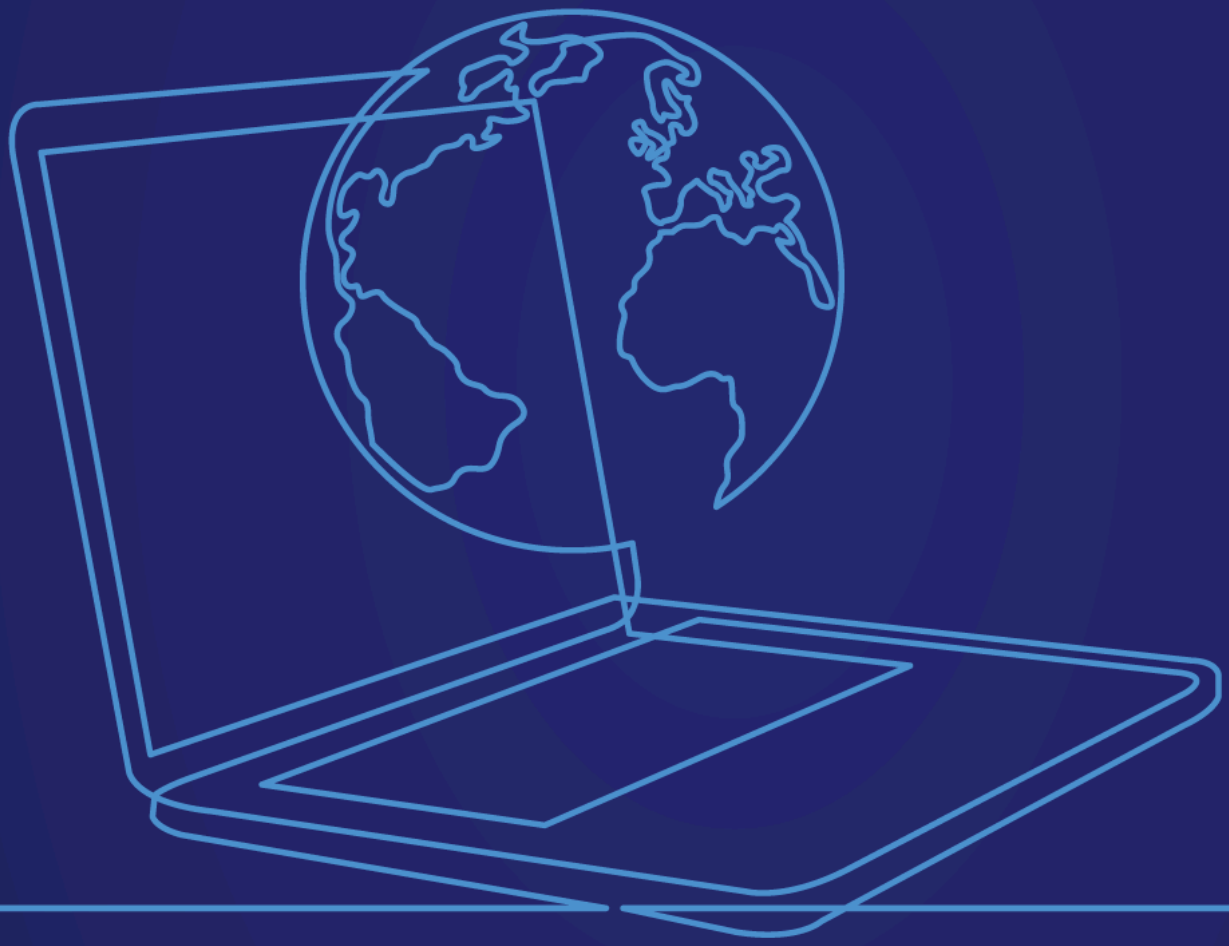
TrustArc



Global Consent Laws & Configuration Guide

Table of Contents

About This Document **3**
Cookie Consent Manager (CCM) Configuration Basics **3**
Types of Consent 3
Cookie and Tracker Activation Settings 4
Tracker Categorization 4
Consent Interface Implementation Options 4
Consent Interface Design Considerations 5
Suggested CCM Configurations **6**
Consent Laws & Applicability Matrix **8**
Regional Considerations **9**
Europe 10
U.S. and Canada 11
Asia-Pacific 16
South America 18
Africa 18
Middle East 18
CIPA Considerations **19**
Tag Manager Considerations **20**
Recording Consent FAQs **22**
Additional Privacy Solutions **24**

Legal Disclosure

Please note that this document and its contents should not be construed as legal advice, nor is it intended to be a substitute for legal counsel. You are solely responsible for customer-specific use decisions and should not act or refrain from acting on the basis of any information included in this document without seeking the advice of legal counsel.

Revision History

Version 1.0	August 14, 2023	Published Document
Version 2.0	December 10, 2024	Revised to supplement existing guidelines, include additional U.S. state guidance and for readability.
Version 3.0	September 18, 2025	Added CIPA Considerations section to address wiretapping lawsuit and arbitration risks and guidance.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

		Added Tag Management Consideration Section to address German Administrative Court ruling

About This Document

This document is designed to provide helpful configuration and select jurisdiction-specific information and considerations to take into account when configuring your cookie consent manager (CCM) instance. As a reminder, this information is not meant to substitute or replace your need to obtain independent legal and privacy advice – consult counsel or your privacy team before finalizing and implementing any CCM settings.

Cookie Consent Manager (CCM) Configuration Basics

Before setting up CCM, we recommend that you first understand key terms and concepts, including the different types of consent, consent experiences, and interface implementation options, as well as consider some design tips. As noted above, while this is not meant to replace legal counsel, this knowledge is designed to provide some helpful guidelines to consider when configuring CCM to take into account a variety of regulatory requirements.

Types of Consent

First, it's important to understand the types of consent you can offer to users. The type of consent required will depend not only on the jurisdictions where you are implementing your CCM instance and applicable legal requirements, but also your own business and risk tolerance position with respect to tracking technologies. While there are various types of consent, two common approaches are described below:

Implied consent (opt-out)	Explicit consent (opt-in)
• Tracker-related information may be placed on a user's device or collected from the user unless the user pro-actively opts out/elects to change their settings. • Users are informed that tracker-related information, other than essentially/strictly necessary trackers that cannot be disabled, will be collected unless they specifically decline or disable it.	• Users must actively provide their consent before any non-essential tracker-related data is collected or processed. • This requires clear, affirmative action from the user, such as clicking a checkbox or pressing an "Accept" button.

While the above is a general explanation of different common approaches, jurisdiction-specific consent considerations are outlined in the Regional Considerations section below.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Cookie and Tracker Activation Settings

The type of consent offered to users will determine the types of cookies and trackers that are, by default, active when a user visits your website. Below are two common default cookie and tracker activation settings:

1. **Required Cookies (i.e., Essential or Strictly Necessary Cookies Only)**: This approach is typically used in jurisdictions that require explicit or "opt-in" consent. When a user visits your website, only cookies and trackers that are considered essential or strictly necessary are activated by default. These are necessary for the basic functionality of your site. Non-essential cookies and trackers, which aren't required for the website to function, will remain inactive until the user provides opt-in consent. In regions where explicit consent is required, non-essential cookies must not be pre-enabled—there should be no pre-checked consent boxes.
2. **Default Tracker Load (i.e. Opt-Out)**: This approach is typically used in jurisdictions that permit implied (opt-out) consent. All trackers are activated when a user enters the website, but they must be adjusted to respect the user's consent preferences once provided. Pre-checked boxes may be used, depending on the type of personal data collected through cookies and trackers.

Tracker Categorization

The next step is to identify which cookies and trackers should be activated when a user visits your website. For example, which cookies and trackers are considered essential/strictly necessary and may load by default vs., in an opt-in jurisdiction, are considered non-essential functional or advertising trackers and will only load upon consent. TrustArc will perform a scan of your site to determine the types of cookies and trackers in use. The results of this scan will provide an initial possible categorization of the identified cookies and trackers. You will then need to carefully review the scan results and suggested categories to verify if they are accurate or, based on the actual use case of each cookie and tracker, they need to be recategorized.

Consent Interface Implementation Options

Once you have identified the required type of consent, determined the types of cookies and trackers to activate, and categorized them, you are ready to design your consent interface. CCM offers two interface implementation options for setting up the consent experience further described in the table below.

With either option, you may configure the experience such that users can access the website without being forced to make an immediate consent decision (e.g., accepting or rejecting trackers). The default preferences will remain if users continue to use the website without indicating a preference.

These options can be used together or separately. For instance, you might use a banner to present the consent options, which then leads to a modal for configuring granular settings or you may use a modal to present consent choices and permit configuration changes.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Banner	Modal
• Typically some form of banner displayed at the top or bottom of a webpage that informs users about the website's use of trackers • May have an overlay where the site is grayed out requiring a user to make a choice before proceeding to navigate the website. • Typically provides users with options to provide some form of broad consent directly through the banner or “click in” to a link to make more granular selections.	• A window that popups the CCM on the website to present information about the tracking technologies used. • Also seen when clicking the Cookie Preferences link/icon or the "More information" button on a banner. • Can be set as the default presentation. This is more common in jurisdictions that require individuals to explicitly indicate a preference (opt-in).

Both interfaces allow for customizable verbiage, translations, size, dimensions, placement, styling and consent preference categorization.

Consent Interface Design Considerations

We recommend that when choosing your consent interface to take into account your users and keep them in mind, ensuring they can easily understand their preference options and how to exercise them freely.

Here are some tips to consider when designing your consent interface:

1. **Use Clear Language**: Make preference options easy to understand by using simple, plain language and avoiding industry jargon or technical terms.
2. **Consider Your Audience**: Tailor how you present consent options based on the unique characteristics of your primary users. For example, if your website is aimed at children (under age 13) or minors (age 13-17), use language that they can easily comprehend.
3. **Avoid Manipulative Tactics**: Avoid language, visuals, or choice options that may be intentionally or unintentionally misleading or manipulative. For example, making the opt-out option harder to find or read. Allow users to clearly indicate their preferences.
4. **Provide Equal Options**: If you provide multiple choices (e.g., to accept or reject optional tracking), it is important to take into account if it is as easy for users to accept or reject all options. The styling for accept and reject options should be identical. For example, accept and reject buttons should be equally placed and sized to avoid behavior that may trigger regulatory scrutiny in certain jurisdictions.
5. **Clarify Consent**: Silence or inaction should not be interpreted as explicit consent. For example clicking away from a banner or clicking an X may not be sufficient to consider it explicit consent. Consider only acknowledging consent from more explicit and obvious actions like clicking “Accept.”
6. **Avoid Bundling Options**: Exercise caution to avoid grouping multiple preference options into a single choice, as this can impair the user's ability to make clear decisions."

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Suggested CCM Configurations

There are two primary and common methods to consider when configuring CCM based on the consent type, experience, and interface, as well as tracker activation settings.

Implied Consent (Opt-Out) Configuration	Explicit Consent (Opt-in) Configuration
• Banner consent interface • Standard tracker load activation	• Banner or modal consent interface • Required cookies activation

Tips for Configuring Trackers and Honoring Preferences

- **Ensure trackers' consent categorization is accurate:** Run scans and review trackers' current consent categorization on a regular basis. Clients with complex scanning requirements should consider setting aside additional time to review scans.

  There are three main categories of cookies and trackers.
  - **Required Cookies:** are cookies and trackers that are typically considered necessary to enable the basic features of your website to function, such as providing secure log-in, allowing images to load, or allowing users to select their cookie preferences.
  - **Functional Cookies**: are generally web analytics trackers collecting visitor usage information such as page views, session information, and bounce rate for purposes of understanding and optimizing the performance of the site. They may also allow for an enhanced user experience, such as retaining previously set site preferences or personalized features.
  - **Advertising Cookies:** are used in Interest Based Advertising (IBA), such as in relation to advertising network activities including, but not limited to, targeted ad placement, social media, and/or the building of user profiles.

  Some companies may have additional buckets to further segregate their cookies and trackers. For example, Functional Cookies are often split into Functional, Performance, Personalization and Analytics trackers. Advertising Cookies may be split out into Targeting Ads, Social Media, and User Profiling buckets.

  NOTE: Please reach out to your Technical Account Manager to request the Tracker Audit Review Guide for assistance with categorizing trackers on your website.

- **Implement mechanisms to manage trackers in alignment with your CCM configuration:** Ensure any non-required scripts loading on your website have activation and blocking controls based on the trackers' defined categorization.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

- **Tag Management Systems (TMS):** TMS are widely used by organizations to efficiently manage and deploy tracking tags and scripts across websites or mobile applications. These systems (e.g., Google Tag Manager, Adobe Launch, or Tealium) help streamline the implementation of analytics, advertising, and other third-party tools without requiring direct code changes. When integrated with CCM, a TMS enables the enforcement of user consent by blocking non-essential trackers until appropriate permissions are obtained. TrustArc provides implementation guidance to ensure the TMS configuration aligns with your organization's consent requirements.
  Note: To ensure uninterrupted tracker management, the TMS domain should be classified as required, as the TMS plays a critical role in facilitating tracker management. Before implementing a TMS, consider whether it is necessary for the jurisdictions you are operating in. For more information, see the Tag Manager Consideration section.

- **Autoblock**: Serves as a supplementary solution to help prevent some third party trackers from activating without proper consent. It is a TMS-like feature that can be enabled at the country level through CCM's back-end, and can be configured to activate only essential first and third party trackers until the user consents to any other non-essential tracker. Autoblock may not work if a tracker does not have a source code ("SRC") attribute. In this case Manual Block, a feature within Autoblock, may need to be enabled.

- **Manual Block:** Enables users to manually block tags that are not automatically filtered. This feature works by changing the tag's src attribute so that it does not load automatically when the page is accessed. For further information, please refer to the auto-block implementation guide.

- **Application Programming Interface (API):** A set of rules and protocols that allows different software applications to communicate and interact with each other, enabling functionality integration. Based on the level of end-user consent received via the CCM, the API allows companies to create custom logic on the website code to programmatically manage tags that cannot be moved to a TMS. Our API Integration guide outlines the CCM functions that enable customers to customize and implement user consent options tailored to their website's specific needs.

- **Ensure all trackers are configured in CCM:** Whenever new trackers are added, make sure that they are already categorized in the cookie consent manager and that the proper controls have been implemented to ensure trackers load according to the user's preference or deployment strategy in case preferences are yet to be chosen. Establishing a governance process is crucial to ensure your site meets your privacy requirements.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Consent Laws & Applicability Matrix

This matrix lists key jurisdictions with laws governing the use of cookies and trackers, along with the suggested CCM configurations for each jurisdiction to consider. Specific additional regional elements can be found in the Regional Considerations section below.

Region	Jurisdiction	Law	Suggested Configurations
Europe	 EU & UK	General Data Protection Regulation (GDPR) ePrivacy Directive 2002/58/EC UK GDPR The Privacy and Electronic Communications Regulations (PECR) 2003	Explicit Consent Configuration
U.S. and Canada	 U.S.	U.S. State Privacy Laws	Implied Consent Configuration
	 Canada (Federal)	Protection and Electronic Documents Act (PIPEDA)	Explicit Consent Configuration
	 Québec	Québec Law 25	Explicit Consent Configuration
Asia-Pacific	 Japan	Act on the Protection of Personal Information (APPI)	Implied Consent Configuration
	 China	Personal Information Protection Law (PIPL)	Explicit Consent Configuration
	 Republic of Korea	Personal Information Protection Act (PIPA)	Explicit Consent Configuration
	 Australia	The Privacy Act	Explicit Consent Configuration
South America	 Brazil	Brazilian General Data Protection Law (LGPD)	Explicit Consent Configuration
Africa	 Kenya	Data Protection Act 2019	Explicit Consent Configuration
	 Nigeria	Data Protection Regulation	Explicit Consent Configuration
Middle East	 Saudi Arabia	Personal Data Protection Law	Explicit Consent Configuration

Regional Considerations

Below, we highlight some additional region-specific details to consider.

First, let's define some terms that are used throughout the remainder of this document:

- **Personal Information.** Personal Information means any information relating to: (i) an identified or identifiable natural person (e.g., a Data Subject or Consumer); (ii) a household under CCPA; and/or (iii) any elements that constitute personal information or a similar construct under applicable law, in each case, where such information is maintained on behalf of the Controller by the Processor within its Solutions environment and is protected similarly as personal data, personally identifiable information, or the equivalent construct under Data Protection Laws and Regulations.
  NOTE: The above is the same definition you will find in your Subscription Service Agreement and Data Processing Addendum associated with your purchase of TrustArc Solutions (found at https://trustarc.com/legal-center/).
- **Sensitive Personal Information.** Sensitive Personal Information is a particular category of personal information that requires additional special protection and/or considerations if accessed, used, or disclosed without authorization and would cause additional harms, such as financial, physical, discriminatory, or reputational harm to an individual.

  While commonly prescribed under applicable law, some typical examples of Sensitive Personal Information include:
  - racial or ethnic origin of the Individual
  - political opinions of the Individual
  - religious, philosophical, or similar beliefs or activities of the Individual
  - individual's trade union membership or activities
  - Individual's precise geolocation
  - precise information regarding the Individual's past, present, or future physical or mental health condition and treatments including genetic, genomic, and family medical history
  - Individual's neural data
  - information regarding the Individual's sexual life or orientation
  - the commission or alleged commission of any offense by the Individual.

Note: Please be aware that this document and this "Regional Considerations" section only addresses a limited subset of geographies or considerations pertaining to personal information and may not address any or all of the considerations around particularly regulated data (e.g., sensitive information, consumer health, and children's data).

Europe



European Union

Explicit Consent. The General Data Protection Regulation (GDPR) and the ePrivacy Directive are the legal frameworks regulating the use of cookies in the EU. Opt-in consent for non-essential cookies in the EU must be freely given, specific, informed, and unambiguous, and provided by a statement of clear affirmative action of the individual. Under Recital 32 of the GDPR, using pre-ticked boxes, silence or inactivity, or scrolling or swiping through a webpage does not constitute valid consent. According to EDPB guidance regarding GDPR-compliant consent, users must be given granular options to accept/decline some or all cookies while retaining the possibility to change the cookie settings in the future through an easily accessible solution allowing them to withdraw their consent at any time (i.e., through an icon or link placed in a visible and standardized place).

Consent may be obtained through splash screens, banners, or modal dialog boxes. Consent may be obtained through browser settings only where such settings are developed in line with the conditions or valid consent under the GDPR.



The European Data Protection Board (EDPB) has published guidelines that provide a detailed analysis of the concept of consent under the GDPR.

Also, the EDPB has released guidelines to clarify how Article 5(3) of the ePrivacy Directive applies to various technical solutions.



United Kingdom

Explicit Consent. The Privacy and Electronic Communications Regulations (PECR), generally considered the UK-equivalent of the EU's ePrivacy Directive, requires opt-in consent for the placement of non-essential cookies. Consent under the PECR must meet the conditions for valid consent under the UK General Data Protection Regulation (UK GDPR - which is similar to the EU GDPR) - consent must be freely given, specific, informed, and unambiguous, and provided by a statement or clear affirmative action taken by the individual. The Information Commissioner's Office (ICO), who is the data protection regulator in the UK, confirms that consent must be obtained for all non-essential cookies (i.e., social media trackers and plugins, cross-device tracking, advertising, analytics). The use of pre-ticked boxes, silence or continuing to use a website do not constitute valid consent. Consent mechanisms must allow individuals to control the setting of all cookies, with consent for cookies being separate from all other matters, and allow individuals to easily withdraw their consent. Consent obtained by clicking "Accept All" on the first layer of the cookie banner is not considered valid if there is not an equivalent option to "Reject All" (or other non-ambiguous option to refuse).

Note: The PECR allows for consent to be collected through a user's browser settings. However, the ICO cautions against this practice because there is insufficient evidence to confirm that users have properly configured their browsers or that they are satisfied with the default settings provided by their browsers.

U.S. and Canada



United States

Implied Consent. Most U.S. States with modern privacy laws require implied consent. The use of personal information collected through cookies for secondary purposes[1], and the collection and processing of sensitive personal information and children's data require explicit consent. When it comes to obtaining consent, most enacted modern US state privacy laws impose prescriptive obligations on businesses, including:

- Obtaining consent that is freely given, specific, informed, and unambiguous;
- Avoiding requests for consent that are presented within general or broad terms of use or similar documents with unrelated information;
- Recognizing that hovering over, muting, pausing, or closing a piece of content does not constitute valid consent; and
- Avoiding the use of dark patterns, which are manipulative tactics designed to obtain consent.

Note: Some States, such as Utah and Iowa, only require notice and the option to opt out of processing sensitive data, including through the use of cookies. Maryland prohibits the sale of sensitive personal information, even with consent, unless specific exceptions apply. Additionally, organizations cannot sell or process personal information for targeted advertising if they know or should know that the consumer is under 18 (See Section 14–4607 of Maryland's Online Data Privacy Act).

Utah, Iowa, and Rhode Island do not require consent for secondary purposes. This means that personal data collected through cookies can be used for purposes beyond what is reasonably necessary or compatible with the disclosed purposes.



Wiretap-related lawsuits and arbitrations are increasing as cookies and other tracking technologies are viewed as privacy-invasive under wiretapping laws like the California Invasion of Privacy Act (CIPA). Further details on the application of wiretapping laws and risk management can be found in the "CIPA Considerations" section of this document.

[1]In most states, "secondary purposes" refers to the processing of personal information for reasons that are neither essential nor compatible with the initially disclosed purposes for which that data was collected. In California, "secondary purposes" means using personal information in ways that do not align with the reasonable expectations of consumers.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Right to Opt-Out.
Consumers have the right to opt out of the sale of their personal information (as well as from sharing in California) and targeted advertising (except in Iowa) as defined under applicable laws (see below for more information on what a "Sale" is under some applicable U.S. laws). Businesses that process personal data for these purposes, including through the use of cookies or other tracking technologies, must provide a clear and conspicuous method to exercise the right to opt out of such processing, such as a conspicuous link "do not sell/share my personal information."

Most states require that the opt-out link be located clearly and conspicuously on the business website. Some states, like California, have specified that the link should be located at the top or bottom of the home website. Colorado requires businesses to locate the opt-out link outside the privacy notice. That link can: 1) take consumers to the opt-out notice, which includes information on the sale of personal information or targeted advertising practices and includes the method to opt out; or 2) direct the user to the page where they can opt out. In the second option, the notice must be included in the privacy policy.



Sell/Share. Sale is generally defined as the exchange of data by the business with a third party for monetary or valuable consideration. Some states, such as Indiana, Utah, Virginia, Iowa, and Kentucky, don't consider data exchanges for a valuable consideration as a sale of personal information. This is relevant when assessing whether the use of third-party cookies constitutes a sale of personal information or if these requirements don't apply. The majority of U.S. state privacy laws only require implied consent or opt-out for the selling of personal information. California has extended that right to include the sharing[2] of personal information. Below are common considerations for when a Sale or Share has occurred.

- **Monetary Consideration:** A monetary benefit typically refers to the exchange of goods or services for money. This can include direct financial payments (such as cash or traditional currency) as well as other financial advantages like discounts, rewards, rebates, commissions, or any form of compensation that holds tangible economic value.
- **Non-Monetary Consideration:** Although this term is not typically defined, based on the Sephora ruling[3] regarding the use of online tracking technology, non-monetary considerations can include: a) analytics or b) free or discounted services. For example, businesses may benefit from data about consumers' online activities, such as using that data to target advertisements to individuals who browse products on their website.

Additionally, Maryland broadened the sale definition to include data exchanges from businesses to third parties and exchanges made by vendors or other affiliates.

[2] Disclosure of consumer's personal information by the organization to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including the benefit of an organization where no money is exchanged, unless an exclusion applies (Section 1798.140 (ah) of the CCPA).
[3] The People of the State of California v. Sephora USA Inc. - Final Judgment and Permanent Injunction - Superior Court of the State of California

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Businesses must be clear about whether they are “selling” or “sharing” personal information with their tracking technology vendors. If their tracking practices qualify as a sale or sharing, they must provide consumers with specific options to opt out of those practices. Consider the following questions when assessing a vendor and identifying any potential data protection or sale of data risks.

1) **Applicability.** Do any U.S. State consumer privacy laws apply?
2) **Tracking Technologies.** Does the vendor use online tracking technologies as part of its service? Examples of online tracking technologies include: pixels, web beacons, software development kits (SDKs), third-party libraries, and cookies
3) **Disclosure/Access.** Does the vendor disclose to third parties or provide them access to personal information? For example, does the vendor allow third parties to embed tracking technologies into the provided service?
4) **Benefit of the Exchange.** If yes to all of the above, is the benefit of the exchange monetary *or* non-monetary?
5) **Exception.** It is possible that even if all of these requirements are met, a sale may not have taken place where an exception under applicable law applies.

Executing service provider agreements outlining the vendor's services and the purposes for processing personal information is essential for determining whether disclosing personal information constitutes selling or sharing it.

Note: TrustArc cannot determine whether your business is engaging in a sale or share of personal information. We recommend making this determination with your legal counsel.



The banner. Although the U.S. State consumer privacy laws do not explicitly require cookie banners, these are an easy way to comply with transparency requirements or respond to individuals’ rights, such as the right to opt out from selling/sharing.

Cookie consent banners like CCM are a quick and easy way to meet requirements around providing consumers with relevant privacy information and the opportunity to consent and set their preferences. Consider the following when configuring your banner:

- Ensure available options to provide consent are as symmetrical as possible (e.g., same number of steps to engage with each option).
- Include a link to the privacy notice or other privacy disclosure (e.g., a Cookie Notice) that discloses privacy practices.
- Inform the web visitors why and how your business uses cookies.
- May include custom verbiage and link to opt-out of Do Not Sell/Share Opt-out in the banner.
- If the user opts out of Sell/Share, businesses must immediately also opt out of advertising trackers where the advertising tracker is not serving as a vendor.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Universal Opt-Out Mechanisms (UOOMs[4]). Several U.S. state consumer privacy laws now require businesses to allow individuals to opt out of the sale of personal information, targeted advertising, and profiling. This can be done by designating an authorized agent through an internet link, browser setting, browser extension, global device setting, or similar technology. UOOMs are also known as opt-out preference mechanisms, such as the Global Privacy Control (GPC), which is recognized by multiple states, though it is not the only option.

States like Virginia, Utah, Iowa, Indiana, Tennessee, Kentucky, and Rhode Island do not require businesses to recognize opt-out preference signals sent by UOOMs. However, Colorado, Connecticut, Montana, New Hampshire, and Maryland will require businesses to honor such signals starting January 1, 2025.

Must UOOM *signals be recognized*? Only if the organization engages in a sale, share, or targeted advertising and the applicable state consumer privacy act requires organizations to recognize such signals. States like California, Colorado, and Connecticut may conduct sweeps to verify whether GPC signals are being recognized and honored[5].

The effect? For online sale or share, the UOOM will signal CCM to opt out of non-required trackers which can prevent advertising trackers from firing when a tag manager or code logic is present on the website.

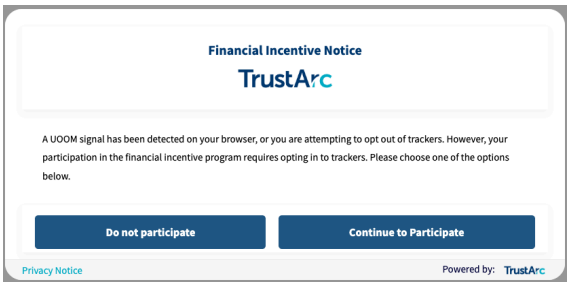
Financial Incentive Programs. Organizations are permitted to offer financial incentives to consumers in exchange for collecting, selling, or deleting a consumer's personal information. For instance, a consumer might need to provide personal information, such as an email address, to receive a discount on the organization's products or services. Financial incentives are allowed as long as the consumer is given a clear description of the program's terms, provides prior opt-in consent, and has the option to revoke their consent at any time.

Obligations with UOOM signals. If a user's opt-out preference signal conflicts with the consumer's participation in an organization's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business *may* notify the consumer of the conflict. The business may provide the consumer with a pop-up notifying them that honoring the opt-out preference signal would withdraw the consumer from the financial incentive program. With that pop-up, the business may offer the consumer the choice to confirm either the business-specific privacy setting or withdraw their participation in the financial incentive program. The image below is an example of how to confirm the consumer's choice when there is a conflict.

[4] The Universal Opt-Out Mechanism includes Global Privacy Controls (GPC), which are required under California's Consumer Privacy Act (CCPA).

[5] California Privacy Protection Agency Announces Joint Investigative Privacy Sweep: CA, CO, and CT Investigate Businesses Refusing to Honor Consumers' Right to Opt-Out of the Sale of Their Personal Information

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com



Known user. A business must treat the known user's opt-out preference signal as a valid request to opt out of sale or sharing for that user. If the business recognizes the same user on different devices or browsers, it must ensure the user's opt-out preference is honored on all those devices and browsers. TrustArc's CCM now has the functionality to store an identifier, allowing a business to comply with this requirement[6].

Canada

Under Canada's federal law, PIPEDA, generally speaking, consent can be either explicit or implied; explicit consent is suggested where sensitive personal information is being collected. All consent must be informed through a notice setting out the purposes for which personal information will be used or disclosed. Note, however, that additional province or Canadian region-specific may also apply, such as those in Quebec, outlined immediately below.

Additionally, Canadian Anti SPAM Legislation (CASL) requires consent for the installation of software, including cookies. If notice has been provided as required under PIPEDA and the user has not taken action to opt-out of the use of cookies it is reasonable to believe from the user's conduct that they have consented to the installation of cookies as required by CASL. If a user has disabled cookies in their browser, then the user has not consented to the installation of cookies meaning cookies cannot be activated.

Quebec

Explicit Consent (suggested). The Act Respecting the Protection of Personal Information in the Private Sector (PPIPS) requires explicit (opt-in) consent for the use and/or disclosure of personal information, particularly where personal information is processed by automated means using technology that can identify, locate or profile an individual. Users must be informed of the use of the technology (e.g., cookies) and the means available to activate the functions of that technology that allow them to be identified, located or profiled. Consent must be freely given, informed, and given for specific purposes, and users must be given the opportunity to withdraw their consent at any time. Consent must be asked for each of these purposes, in simple and clear terms. Where consent is required to disclose Sensitive Personal Information, the consent experience must be expressed

[6] A known user is when the business has associated the browser or device with a user's profile. A user may be identified via: (1) a logged-in user account; (2) a unique identifier; or (3) any online identifier, for example, any online identifiers that can be associated with pseudonymous profiles–Custom IDs, Cookies, Ad Network Accounts, Subnetwork ID, Identity Link, IP Address, Mobile Advertising ID, Mobile User ID, Connected Television ID, TV subscriber ID, or Identity envelopes.

meaning the user must indicate a preference. Given the differences between the requirements for personal information and sensitive personal information, consider using an Explicit Consent configuration.

Configuring banner language

TrustArc has the functionality to identify Canadian provinces, like Quebec. Consider the following configurations for the banner.

- **Browser Language Detection (Dynamic Browser Language Detection).** By default, the consent manager is displayed according to the language set in the browser's setting. In order for this to work, translations need to be enabled for CCM.
- **Forcing language for a specific location is an option.** This is made possible by adding a language or locale parameter to the TrustArc javascript along with the language code to force the consent manager to show in a particular localized language.
- **Primary language.** French should be the primary language displayed on the banner for Quebec. Note: written French is generally considered the same for Quebecois French and Parisian French.
- **Secondary language.** If a second language is used (e.g., English), it must be displayed in a manner that would neither minimize nor disrupt the individual's ability to read the French language (i.e., The second language should not be bigger than the French language and should not be presented in a way that the French language cannot be read easily).
    - The translation of the second language should be identical in meaning (i.e., a word-for-word translation may not result in a translation identical in meaning).
- **Configure the modal/banner for Canada with two languages:** French and the Secondary language.

Asia-Pacific



Japan

Implied Consent. Japan's Act on the Protection of Personal Information (APPI) generally permits the collection of non-sensitive personal information without prior consent; however, if the organization's use of the personal information changes, then opt-in consent will be required for further processing. This user will need to be provided new notice and the opportunity to provide consent meaning the banner will need to be re-displayed. Consent is required to share personal information with third parties (i.e., in the case of third party cookies) - consent for sharing personal information with third parties can be implied where the individuals are provided with adequate notice about the disclosure and given the option to object or opt-out. Opt-in consent is required to collect sensitive personal information, where personal information is used for reasons that are either unnecessary to achieve the specified purpose of use or beyond the originally specified purpose of use, or where personally referable information (information that can become personal with combined with additional data elements) is shared with third parties (e.g., third-party advertising cookies, social plug-in technologies).

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com



China

Explicit Consent. The Personal Information Protection Law of the People's Republic of China (PIPL) requires informed, voluntary, free and explicit consent for the processing of personal information through the use of cookies, unless another valid legal ground for processing the personal information exists (e.g., performance of a contract with the individual). Explicit consent requires the user to take an affirmative action; the use of default settings does not constitute explicit consent. Users must be provided with a convenient way to withdraw consent[7]. Separate consent is required for the processing of sensitive personal information, and parental or guardian consent must be obtained to process minors' personal information.



Republic of Korea (South Korea)

Explicit Consent. Cookies that involve the processing of personal information require prior opt-in consent. Requests for consent must be presented to individuals in a clearly recognizable manner, where each purpose of processing requiring consent is distinctly presented. Consent may be obtained by posting the content to be consented to on a website and letting the data subject express their consent to it. There is no requirement to set up a separate cookie notice; however, South Korea's Personal Information Protection Act (PIPA) requires organizations to disclose in the privacy policy details of processing personal information, including any configuration and management of internet access information files and other devices which automatically collect personal information, including methods for users to opt-out from usage of such tools. The Korea Internet and Security Agency (KISA), the Korean data privacy regulator, is an active regulator known to target companies for being out of compliance with their consent and notice practices.



Australia

Explicit Consent (Suggested). The Privacy Act generally requires consent (express or implied) for the collection, use and disclosure of personal information. Consent cannot be inferred merely by providing an individual with a privacy notice, or by the individual's silence or lack of objection to a proposed handling of their personal information. However, the use of an opt-out mechanism to infer consent for the use of cookies may not be viewed favorably because the user's intention in failing to opt-out may be ambiguous and the opt-out mechanism must meet prescriptive requirements to be deemed valid for this purpose. Express consent must be obtained to process sensitive personal information. Consider an Explicit Consent configuration given some of the law's ambiguities as noted above.

[7] For example, a cookie preference banner would be a convenient way to withdraw consent.

South America



Brazil

Explicit Consent. Brazil's General Personal Data Protection Law (LGPD) requires consent for the processing of personal information for a specified purpose[8]. The Autoridade Nacional de Proteção de Dados (ANPD), Brazil's data protection authority, expects consent options to be shown in a way that are easy to see, manage and understand, and be presented in an equally prominent way that is concise and without excessive information that could lead to "information fatigue." Consent must be a clear and positive act of will (e.g., no pre-ticked boxes); refusal to provide consent cannot lead to consequences for individuals, such as denying full access to a website. Consent must be obtained for each specific purpose, with non-essential cookies disabled by default in the cookie banner, requiring individuals to expressly consent to their enablement. Also, language options must be available for users to understand information about cookies.

Africa



Kenya

Explicit Consent. The Data Protection Act requires an individual's consent for the processing of personal information (Article 30), and requires consent to be express, unequivocal, free, specific, informed and provided by a statement or a clear affirmative action (Article 2). Consent is especially required where personal information is processed for commercial purposes, which could include the use of cookies for advertising purposes (Article 37).



Nigeria

Explicit Consent (Suggested). The Implementation Framework for the Data Protection Regulation 2019 explicitly confirms that the use of cookies requires consent, which must be freely given, informed and specific. However, consent for cookies does not necessarily need the ticking of a box or similar method; the continued use of a website upon a clear notice indicates consent meaning the user does not have to take an affirmative action to indicate consent. In deploying cookies, websites must make cookie information clear and easy to understand, notify users of the presence and purpose of the cookies, identify the entity responsible for the cookies, and inform users on how to withdraw consent from the use of cookies. Consider an Explicit Consent configuration given some of the law's ambiguities as noted above.

Middle East



Saudi Arabia

Explicit Consent. The Personal Data Protection Law (PDPL) requires that consent be obtained prior to processing personal data, and that data subjects be informed about the purposes of processing.

[8] If your business is considering legitimate interest as the lawful basis for processing personal information, including personal information collected through cookies, a Privacy Impact Assessment must be conducted prior to using cookies to do this.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Consent must be obtained for each distinct processing purpose, and documented for evidentiary purposes. Users must be able to easily withdraw their consent at any time. The PDPL prohibits making the provision of a service or benefit conditional on consent to the processing of personal data for purposes not related to the service or benefit, such as the use of a cookie wall to force users to consent to the use of cookies to obtain access to a website.

CIPA Considerations

Wiretapping is the interception of electronic communications, such as phone calls, digital messages, and emails, to secretly monitor and capture information without the knowledge of the parties involved. It involves using a device or method to listen in on or record conversations or other communications. All U.S. states except for Vermont have laws restricting eavesdropping or recording private conversations. Eleven U.S. states passed laws requiring consent from both parties prior to recording whereas the other 39 states plus the District of Columbia only require consent from one party.

Wiretapping laws like CIPA, the California Invasion of Privacy Act, a 1967 law intended to prevent eavesdropping on telephone calls are now being used to bring lawsuits and arbitration actions against companies saying that the privacy of individuals is being violated through the use of cookies and other tracking technologies. Cookies and tracking technologies collect a user's IP address and record the user's interaction with the website creating a 'pen register" recording "dialing, routing, addressing, or signaling information" transmitted from a device but not the content of the communication."[9] These cases are causing businesses to rethink their consent management strategy along with their legal one.

Some legal associations and firms[10] recommend implementing an Explicit Consent (Opt-In) banner design configuration to manage wiretap lawsuit and arbitration related risks. However, implementing an Explicit Consent (Opt-In) has business implications, especially on a business' marketing initiatives. Rulings by the courts on wiretapping cases widely vary, even for cases brought within the same state.[11] For this reason, TrustArc suggests taking a risk-based approach to managing these risks following the seven steps outlined below.

1. **Verify that your cookie banner is working properly.** Even if you implement a third party cookie banner solution like TrustArc's CCM, you need to verify that it is working properly. We suggest that you check that your banner is working properly monthly.[12]
2. **Ensure that tags are being controlled.** When testing your cookie banner, verify that your tag manager is blocking non-essential trackers until appropriate permissions are obtained from the user. If you don't have a tag manager in place, you may want to consider implementing one. See our Tips for Configuring Trackers and Honoring Preferences to ensure that necessary measures are taken to control tags.

[9] Ca. Pen. Code § 638.50.
[10] American Bar Association, Law firm Perlman+Perlman, Law firm Jenner & Block
[11] Covington Inside Privacy Feb 27, 2025
[12] California Privacy Protection Agency required an online clothing retailer to pay a $345,178.00 fine for failing to oversee and configuring its cookie consent banner properly among other CCPA violations.

3. **Determine if highly scrutinized trackers are being used on your website.** Trackers such as those set by Linkedin, Meta, and TikTok have come under greater regulatory scrutiny due to their extensive data collection practices including sensitive data without consent.
4. **Know what type of data is being collected and tracked through highly scrutinized trackers.** Determine if the data captured through these trackers is sensitive or whether sensitive information can be inferred from the data being collected.
5. **Weigh the risk and reward of using highly scrutinized trackers.** Work with your stakeholders to understand the benefit to both your business and users gain from utilizing scrutinized trackers. The benefits to the business should not outweigh the risks to users, especially where the content on your website and the information collected or inferred is sensitive.
6. **Discuss legal and risk positions with internal stakeholders and potentially outside counsel.** If you are considering moving forward with implementing an Explicit Consent (Opt-In) approach for certain categories of ad tracking, this is a big decision that potentially has a big impact on the business and needs to be made along with relevant business stakeholders.
7. **Engaging suitable outside counsel if a CIPA letter or threat is received is critical**. Not all groups and parties sending the letters are the same and they take different approaches. Suitable counsel will know who the players are and how to respond including whether to settle is appropriate.

Tag Manager Considerations

The German administrative court ruling on Google Tag Manager has significant compliance implications. The court determined that tag managers require explicit user consent, reclassifying them from "required" to "functional" tools and reinforcing the need for a "Reject All" option on consent banners. Businesses operating in the EU—especially in Germany—must assess how their tag management systems collect data, evaluate whether they are technically necessary, and explore alternative implementations to ensure compliance with the German Telemedia Act (TTDSG) and the EU's General Data Protection Regulation (GDPR).

On March 19, 2025, a German administrative court ruled that Google Tag Manager requires explicit user consent before activation[13]. This decision was based on the fact that it automatically processes personal data and stores information on user devices without authorization, thereby violating both TTDSG and GDPR.

The court determined that legitimate interests cannot serve as the legal basis for processing for technical purposes, as the collection and transmission of information to Google serves commercial ends rather than being essential for the proper functioning of the technology. This ruling impacts how businesses categorize their tag management solutions when configuring their cookie consent banners. While it is often suggested that tag managers are considered functional under cookie and tracker categories, most companies reclassify them to be required. The ruling means companies will need to reclassify tag manager solutions as functional.

In cookie consent frameworks, "required" (or "strictly necessary") cookies and technologies are those essential for a website's basic operation, such as enabling shopping cart functionality or security features. "Functional" cookies

[13] https://ppc.land/german-court-ruling-on-cookie-consent-could-impact-tag-management-practices/

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

and technologies, by contrast, improve user experience or add features but are not strictly necessary—for example, saving user preferences, running non-personal-data analytics, or deploying scripts through tag managers. The German court ruled that when a tag manager collects and transmits personal data for commercial purposes, it cannot be classified as “required.” Instead, it falls under the “functional” category (or equivalent) and requires explicit user consent.

Furthermore, a consent banner that lacks a "Reject All" option fails to obtain consent as required by GDPR; therefore, banners must include a "Reject All" option[14].

In light of this ruling, TrustArc suggests companies operating in the EU and Germany specifically, and utilizing a tag management system along with a cookie banner solution, consider taking the following actions:

- **Understand how your tag management solution works.** Assess how the tag management system functions, understanding what information it collects and where that information is transmitted. Document the technical necessity claims of your tag management system and any marketing technologies used on your site that your business has categorized as required.
- **Evaluate the technical necessity of your tag management system.** Consider alternative approaches, such as the ones outlined here, for implementing your tag management system.
    - Loading the consent manager separately from the tag manager could involve ensuring your consent management platform loads and presents the consent banner before any tag manager scripts are loaded, preventing data transmission until consent is granted.
    - Architectural approaches that minimize client-side processing until after consent is obtained might include server-side tagging, where data processing and routing occur on your servers after user consent, rather than directly in the user's browser, reducing initial client-side data exposure. This will reduce the automated transmission of data, a concern raised in the German court ruling.

  Note, certain browser features, such as Safari’s Private Window mode, automatically block third-party tracking, which can include tag management tools. If a consent management platform loads the tag manager directly, users in these private browsing modes may be unable to give consent because the tag manager is blocked before the consent banner can function properly.
- **Know if you have localized versions of your website.** Most businesses have a .com, .org, .net, or .co domain. Check to see if you have localized versions of your domain, like .eu or .uk. Understanding what localized domains you have may provide you additional flexibility in categorizing your tag manager system at a jurisdictional level to address legal requirements for that jurisdiction.
- **Understand the location of visitors coming to your site from specific jurisdictions.** This, along with the assessment and documentation of the technical necessity of your tag management system, will enable you to assess the risks related to categorizing your tag management system, especially if you do not have localized versions of your website or are using a cookie banner solution that does not enable you to categorize your tag management system at a jurisdictional level.

14 https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/urteil-zu-manipulativem-cookie-banner-alles-ablehnen-schaltflache-ist-ein-muss-241960.html

- **Weigh the risks and benefits of your tag manager system implementation.** Work with your stakeholders to understand the benefit to both your business and users from how your tag management system is implemented. The benefits to the business should not outweigh the risks to users, especially if the tag management system is collecting and transmitting data to third parties prior to obtaining consent.
- **Discuss legal and risk positions with internal stakeholders and potentially outside counsel.** If you are considering changing how your tag management system is implemented, this is a big decision that potentially has a big impact on the business and needs to be made along with relevant business stakeholders.

Recording Consent FAQs

In some jurisdictions such as the EU and UK, your business may be required to retain a record that a user has consented to the use of cookies and trackers. Below are some frequently asked questions regarding how TrustArc records a user's consent.

Do you need to record a Data Subject's Consent?

Depending upon the law of the jurisdiction, a business may have to demonstrate a user's consent is recorded. TrustArc offers a UserID (UID) feature which when enabled creates a Cookie on the user's browser with a random generated UID. This UID is then stored into a "GDPR report"[15] which can then demonstrate that the user has made a consent choice. This identifier cannot be used to identify the data subject.

What pieces of data do we process and store in our platform?

- We temporarily look at the user's full IP Address at initiation to determine the user's location and serve the correct consent experience. We only store a hash of the IP address, creating a pseudonymized consent choice for reporting purposes.
- If the TrustArc UserID feature is enabled, we will process or store the user's consent choice, country location of the user, device type, OS, and website address of consent location. TrustArc is unable to identify the user without being provided the ID from the cookie that the user has.
- If the Known User feature is enabled in jurisdictions like California, we will process or store a single online identifier that your business provides us. Known User is described under the U.S. State consumer privacy laws in the Regional Considerations section above.

Is the information we collect personal information?

- TrustArc collects limited information most of which is not considered personal information under applicable law. However, it depends upon the jurisdiction's definition of personal information. For example, the information we collect might be considered personal information under the CCPA but not so in the EU due to a recent decision by the Court of Justice of the European Union.[16]

[15] We refer to this as a "GDPR" report in our system; however, this does mean this is only applicable for the GDPR.
[16] The Court of Justice of the European Union recently decided that pseudonymized information may be considered anonymized when the party holding the pseudonym does not have in its possession the pieces of PI needed to identify the data subject.

- If the Known Users feature is enabled, it is likely that the identifier we will collect and store will be considered personal information, depending upon the identifier provided.

How long do we retain the data?

- TrustArc retains the following information:
  - Partial IP address (last two octets)
  - User's pseudonymized profile, which includes the user's consent choice, country location, device type, OS, and website address of consent location,
  - URL where consent was obtained
- TrustArc retains the pseudonymized profile of the user for thirteen (13) months providing that the user disclosed their UID stored in the TAConsentID cookie on their browser, and the browser cookies/cache is not cleared and the cookie hasn't expired (13 months). The UID in the TAConsentID cookie is only dropped if the UID feature is enabled (UID feature is disabled by default).
- Online identifiers are retained for the duration of your business' contract.
- TrustArc does not retain the user's full IP address.

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

Additional Privacy Solutions

TrustArc has a number of offerings that can help your organization with its ongoing compliance with cookie and tracker requirements. Each of those solutions are described below. Contact your Account Manager for more information.



Nymity Research & Alerts

Stay up on current suggested practices or required actions, read the text of the law, and compare laws across countries, regions, and states, enabling the privacy teams to be more effective in their roles and collaborate with other relevant stakeholders (e.g., marketing, product, IT, legal).



PrivacyCentral

Create and manage your privacy program with continuous auto global law scanning, detection, and comparison based on your company profile. Track your compliance KPIs and audit your privacy program for accountability and governance.



Data Mapping & Risk Manager

Understand your data flows (internal systems, third parties, vendors/partners), automatically generate data flow maps, automate risk detection, scoring and remediation. Assess privacy risks and maintain compliance with data privacy regulations.

AI risk algorithms identify risk and remediations according to laws. Automated Risk Detection and Remediation includes alerts when your data flows are at risk and generate automated follow-up actions such as a PIA or Vendor Assessment. Includes built-in risk scoring based on 130+ laws including DPIA and PIA identification.



Assessment Manager

Utilize 65+ pre-built assessment templates and business process forms to save you time and ensure you are compliance. Templates include PIAs, DPIAs, vendor assessments, CCPA templates, and more, and includes annual assessment reminders.



Individual Rights Manager (IRM)

Automate and scale your data subject request fulfillment with compliance with GPC, GDPR, CCPA, and more. Logic-based intake templates based on local regulations and language detection combined with dynamic request routing. Role-based access control including partial and complete anonymization of form fields to ensure security of data and then easily connect/update/delete data

© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com

for DSR requests through Rapid API. An IRM integration with CCM is particularly important for the jurisdictions with Do Not Sell requirements (e.g., see CCPA analysis below).

TRUSTe Data Privacy Framework Verification

DPF Verification is a cost-effective means for US-based companies to safeguard personal data transfer compliance from the EU, Switzerland, and UK to the US in a government-to-government adequacy decision. The DPF verification provides oversight that appropriate data protection measures are in place, includes a public seal for verification, and provides a dispute resolution service.

TRUSTe APEC CBPR or PRP Certification

As a recognized Accountability Agent for APEC CBPR and PRP, we are authorized to certify data transfer practices. Businesses can demonstrate compliance to this internationally-recognized privacy protection standard, making it a powerful means of demonstrating your dedication to protecting customers' or employee personal data. Certification ensures your privacy compliance efforts as a trusted trade partner and a publicly certified brand that provides consumer confidence and can drive increased business.



© 2025 TrustArc Inc. | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com