A Guide to Consent Management Platforms

An IAB Canada Guide to CMPS

IAB Canada Industry Paper

Published: Q1, 2021

TABLE OF CONTENTS

Introduction

Privacy concerns are quickly defining a new era of digital marketing around the globe. With a continuous flow of amended and redrafted privacy laws across Canada, and worldwide, the demand for enhanced transparency, accountability and increased control over individual consent to use personal data, has peaked. There is no turning back. Privacy and consent frameworks of the future must be secure, nuanced, interoperable across borders and scalable. Importantly, the industry must focus on the development of open-sourced frameworks that are accessible to the open market providing platforms with reliable updates and viability assurances across jurisdictions.

Consent Management Platforms are an essential tool that allows publishers and brands to communicate their privacy practices more openly while giving consumers enhanced control over their privacy preferences. This key element of the eco-system also links consumer choice to the ad tech universe.

Over the past two years, IAB Canada has been working towards the adaptation of the highly successful model used in the EU in response to the GDPR referred to as the Transparency and Consent Framework (TCF). The TCF provides nuanced, standardization of purposes of data usage as well as a robust, signal-based approach to consented bid requests within the supply chain. TCF Canada, will be released under the IAB Tech Lab's Global Privacy Framework in 2021, and in developing standards for Consent Management Platform stakeholders, IAB Canada has been exploring the vast landscape of service providers and their range of offerings.

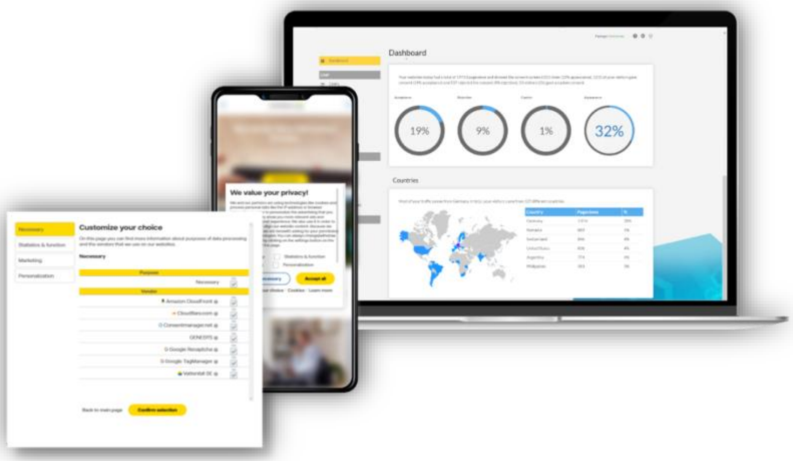
In 2021, we have spent most of our time focusing on cookie depreciation while actively participating in the discussions taking place across all IAB Tech Lab working groups as well as the privacy sandbox and other industry body meetings. Early evaluations of the proposed solutions for the replacement of cookies, indicate that some sort of consent adaptation via a CMP will most likely be necessary. It is worth noting that IAB Canada is committed to supporting an open and fair marketplace to ad tech providers specializing in privacy and as such, have developed this industry guide.

The purpose of this guide is to provide information to the online advertising industry on CMP's, outlining its key purpose, critical components, individual features as well as introduce our community to some of the options that are already available in the Canadian marketplace, and act as a resource to guide the process of finding the CMP that is right for your business.

What is a Consent Management Platform?

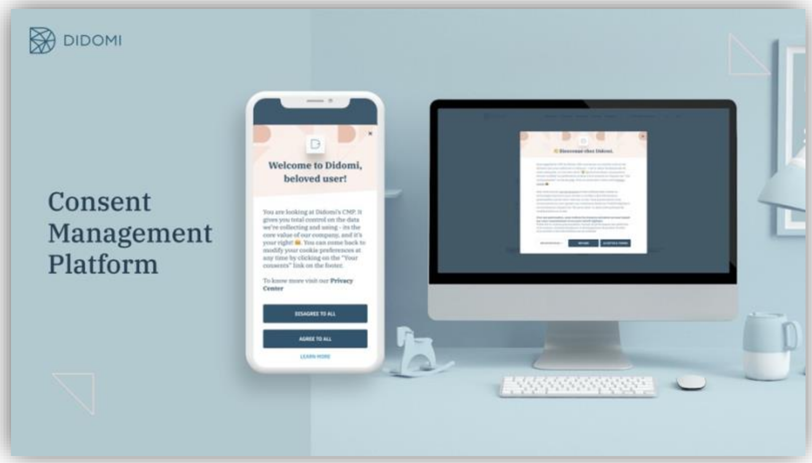
A Consent Management Platform (CMP) is a company or organization that centralizes and manages transparency for the consent and the objection of consent of users of a website. In other words, a CMP enables brands and publishers to automate their consent management process, aiding in privacy law compliance.

From a publisher perspective, a CMP is a platform that requests, receives and stores a users' consent. It is also used to store a list of preferred vendors along with explanations as to why they have been collecting the users' information, and for updating collected consent (i.e.: if a user triggered an action).



Within the Transparency and Consent Framework (TCF), the role of the approved CMP is to read and update the legal purposes of a company that participates in the delivery of digital advertising (commonly referred to as a vendor) within a publisher's website, app, or other digital content. Vendors declare purpose(s) or reason(s) for accessing a user's device or browser, or reason for processing their personal data in the Global Vendor List (GVL).

From a consumer perspective, the CMP is an interface that lives on a visited website and provides transparency to a user, allowing them to see the vendors that the publisher has agreed to work with along with the purposes or reasons that each vendor wishes to leverage. The CMP, within the TCF, stores a user's consent signals in the user's browser and makes consent information available to vendors in the TCF Canada string. It also ensures that consent for a purpose applies only to the vendors that have declared, via the Global Vendor List (GVL), that they use data for that purpose.

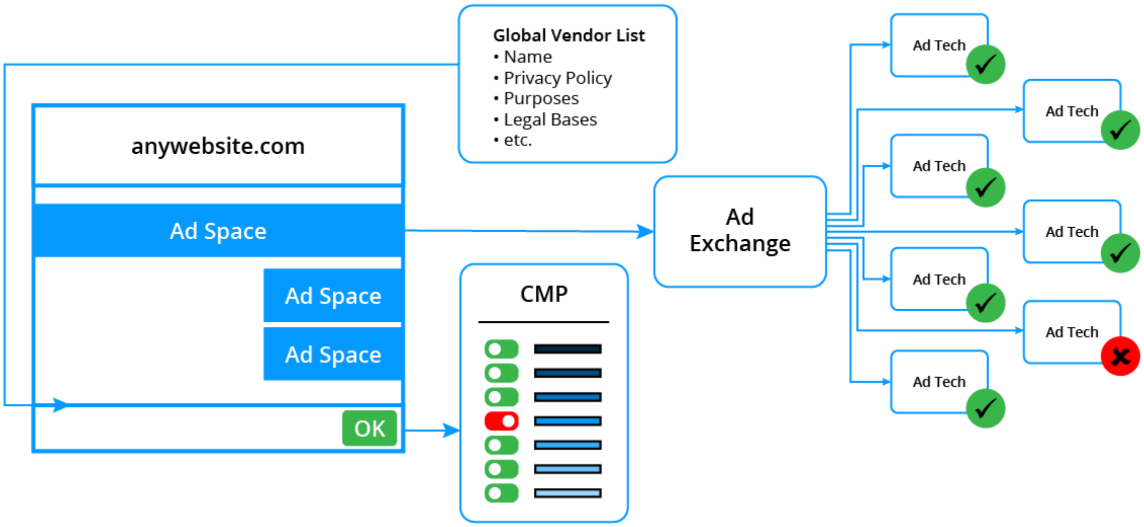


Welcome to Didomi, beloved user!

You are looking at Didomi's CMP. It gives you total control on the data we're collecting and using - its the core value of our company, and it's your right! 🤗. You can come back to modify your cookie preferences at any time by clicking on the "Your consents" link on the footer.

To know more visit our **Privacy Center**

The Role of the CMP in the Transparency and Consent Framework

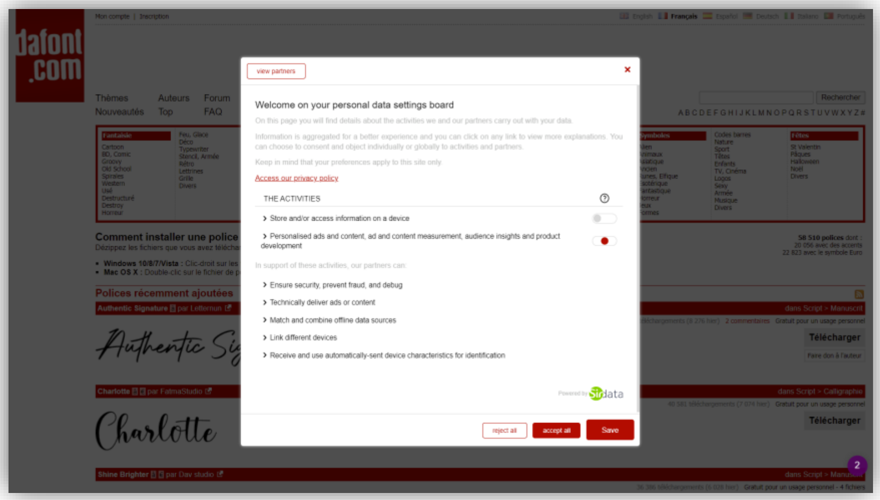


Why Are CMPs Important?

In May of 2020, the European Data Protection Board (EDPB), an organization encompassing many European DPAs with the aim of establishing guidelines for GDPR interpretation, made a set of recommendations that stated: “*swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action*”. They concluded that scrolling does not equate to a clear positive action on the part of the user, and that, when scrolling equals consent, it is too difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it, as the GDPR regulation requires.

This set a mark on the ground for tougher definitions of clear positive action, showing the complexities involved in defining what constitutes clear consent, and requiring many companies to change their consent collection infrastructure.

With these requirements came the introduction of the CMP into the ecosystem. This new interface enabled organizations to meet the stated recommendations providing enhanced transparency into privacy practices for the user, while putting the ultimate control of consent into the hands of the end user. The CMP makes transparency into the consent collection process a better user experience that is more fluid and straightforward.



Welcome on your personal data settings board

On this page you will find details about the activities we and our partners carry out with your data.

Information is aggregated for a better experience and you can click on any link to view more explanations. You can choose to consent and object individually or globally to activities and partners.

Keep in mind that your preferences apply to this site only.

Access our privacy policy

THE ACTIVITIES

- Store and/or access information on a device ○
- Personalised ads and content, ad and content measurement, audience insights and product development ●

In support of these activities, our partners can:

- Ensure security, prevent fraud, and debug
- Technically deliver ads or content
- Match and combine offline data sources
- Link different devices
- Receive and use automatically-sent device characteristics for identification

Here in Canada, under PIPEDA, organizations are required to obtain meaningful consent for the collection, use and disclosure of personal information. Consent is considered meaningful when individuals are provided with a clear explanation on what organizations are doing with their information. However, there are many exceptions to expressed consent under the current law, where implied consent (or an opt out) model often acts as the default.

With additional pressure from privacy advocates, new expectations from consumers, and the newly proposed CPPA (which includes many proposed additional exceptions to consent), opt out is quickly becoming "not enough" and increased transparency on behalf of business and enhanced consumer choice is imperative if trust is to be achieved between the two parties. Consumers are trusting you with their personal information and it is up to you to use it with the utmost care.

According to the recent Accenture Strategy study - "The Bottom Line on Trust - Achieve Competitive Agility" 25,000 global consumers found that, of customers who switched companies in the past year, 46 percent did so because they lost trust in the company. And switching isn't the total cost. Customers are willing to speak up, organize and boycott when their expectations aren't met.

Trust equals revenue and now is the time for business to do better and do what is right for citizens, not just what is written in the law.

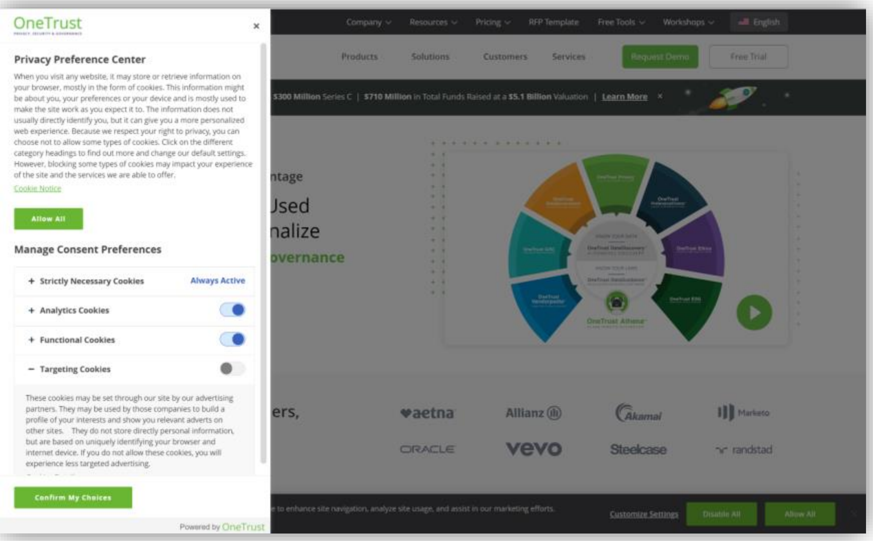
Businesses engaging in the following activities should consider implementing a CMP on their website:

1. Using the personal data of your website visitors for purposes like behavioural targeting, analytics, content or ad personalization, or any other kind of remarketing.
2. Using behavioural data for automated decision making.
3. Sharing/transferring data of your website visitors to third parties.

How Does a CMP Work?

Providing consumers with the CMP "dashboard" gives them access to an upfront menu of choice, allowing them to decide how and when a business can collect and use their personal data. Usually appearing as a pop up on a webpage, the user is shown all of their options regarding the usage of cookies or cohorts.

A user can set their consent status for all the vendors listed within the CMP (individually or in bulk) on a publisher's site, allowing or disallowing vendors to track and target them based on online behaviour and activity. If a user does not consent, they will then be shown contextually relevant advertisements versus personalized ads.



OneTrust

Privacy Preference Center

When you visit any website, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and change our default settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer.

Cookie Notice

Allow All

Manage Consent Preferences

+ Strictly Necessary Cookies — Always Active

+ Analytics Cookies ●

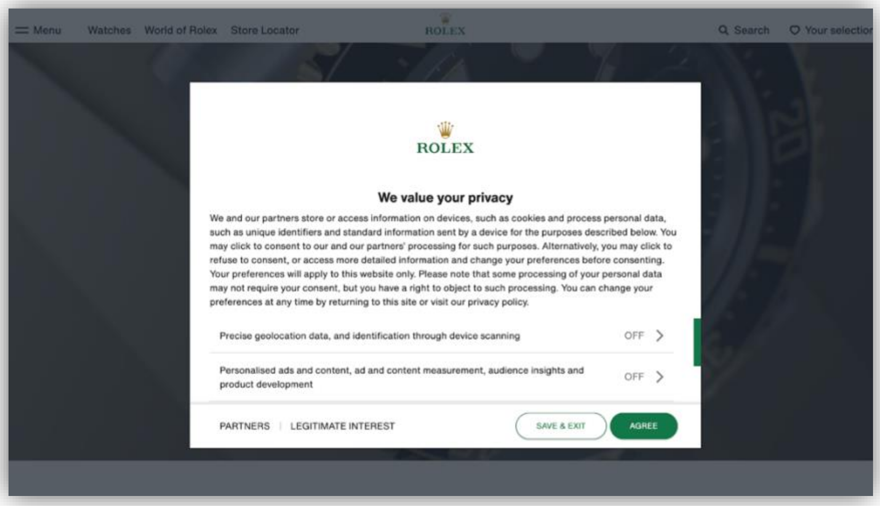
+ Functional Cookies ●

− Targeting Cookies ○

These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

Confirm My Choices

Powered by OneTrust



ROLEX

We value your privacy

We and our partners store or access information on devices, such as cookies and process personal data, such as unique identifiers and standard information sent by a device for the purposes described below. You may click to consent to our and our partners' processing for such purposes. Alternatively, you may click to refuse to consent, or access more detailed information and change your preferences before consenting. Your preferences will apply to this website only. Please note that some processing of your personal data may not require your consent, but you have a right to object to such processing. You can change your preferences at any time by returning to this site or visit our privacy policy.

Precise geolocation data, and identification through device scanning — OFF >

Personalised ads and content, ad and content measurement, audience insights and product development — OFF >

PARTNERS | LEGITIMATE INTEREST — SAVE & EXIT — AGREE

A CMP is responsible for the following:

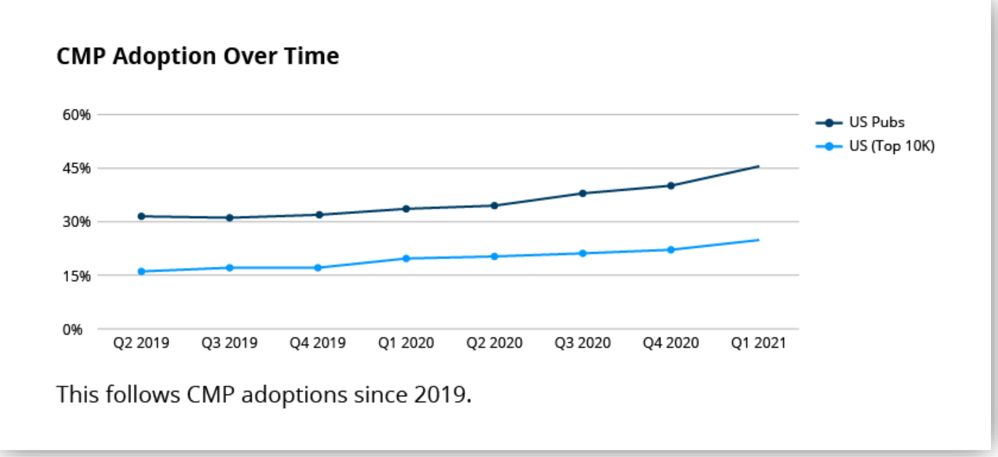
- **Consent Notification:** provides users notice about the data collection and processing of data that is both personal and non-personal.
- **Displaying a User's Privacy Preferences:** gives the user multiple options to exercise their consent for various purposes and scenarios.
- **Capturing and Sharing Consent within the TCF:** approved CMPs store user's preferences in an IAB-compliant cookie so it can be shared with approved vendors within the constraints of the law.
- **Providing Proof of Compliance:** provides access to log data to be audited.

From the perspective of the business, the CMP allows you to:

- Display consent banners and pop-ups to users in an upfront, privacy first manner.
- Collect and handle user consent.
- Helps store consented user information and filter those who have not agreed to the terms and conditions.
- Prevent any collection of personal information before legal consent is obtained.
- Collect data in a manner compliant with user's consent choices.
- In compliance with applicable regional privacy laws that are becoming a crucial part of privacy programs.

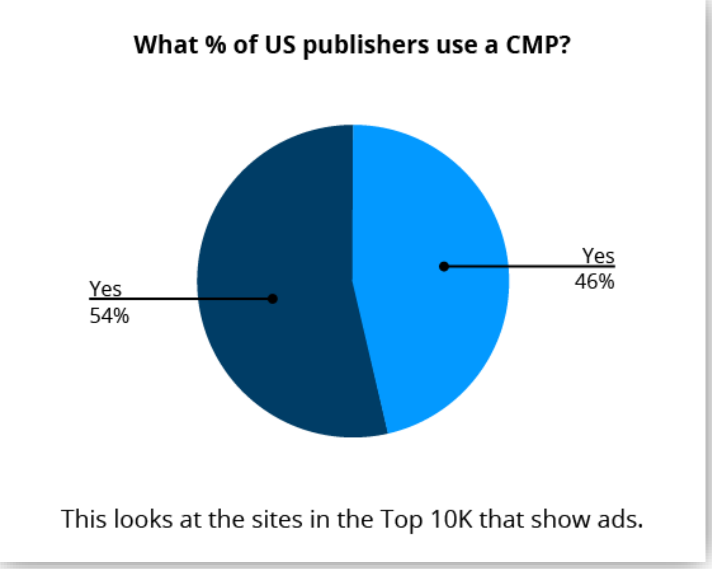
If a visitor to your site disagrees with, or does not consent to, any of your collection purposes, you must respect their choices. A CMP is a valuable tool to add to your privacy toolkit, making you a more responsible and respected marketer in the eyes of your consumers.

According to the Kevel Consent Management Platform (CMP) 2021 Tracker the adoption of CMP's across non-GDPR nations, such as the US, is growing and here in Canada, we will surely follow the trend; 45% of US publishers currently use a CMP and adoption is on the rise:



CMP Adoption Over Time

This follows CMP adoptions since 2019.



What % of US publishers use a CMP?

This looks at the sites in the Top 10K that show ads.

Enhanced trust equals enhanced revenues making the implementation of a CMP a good business decision.

The Future of CMPs

In 2022, with the death of the third-party cookie, the role of the CMP will undoubtedly change. However, the need for organizations to have a mechanism in place to comply with regulations and to capture consent for other means of reaching and tracking consumers will still exist. This requirement for transparency and upfront consent and user control will be a necessary component for publishers and marketers alike, and although no one is entirely sure what exactly this will look like we can begin to imagine how it will play out.

In the example of audience cohorts, which could represent almost 80% of the online addressable audience, non-identified users will be placed into groupings based on their behavior and shown ads corresponding to their group's profile. Within this model we can be sure to predict that visitors to a publisher's site will still need to be able to manage their profile and not only consent to have ads shown to them based on their cohort, but also allow them to modify the groups that they are being identified as a part of within the framework of a CMP.

Meanwhile the remaining estimated 20% of the online population – those who are authenticated by an identifier such as an email or phone number, will also require a mechanism to express their consent to using this personal information as well as allowing them to indicate how they do and do not want their data being used when moving across the ecosystem.

The CMP clearly has a role in both scenarios and is here to stay.

How to Choose A CMP

Before choosing a CMP for your business you should assess your business needs and set out and prioritize your requirements.

There are hundreds of ready-made solutions to choose from - each with some common features and those with some exclusive features, so before choosing you should identify and prioritize your requirements. From there you can choose to use a premade solution or go the route of developing your own proprietary consent management tool. Whatever path you choose to take, you should consider the following:

Operational Considerations:	• Implementation Costs • Implementation Time

	• CRM Integration • Data Ownership
Compliance Considerations:	• Multi-jurisdictional compliance • IAB Certified/TCF Compliant • Conforms to the highest industry standards, practices and taxonomy
Brand/Market Considerations:	• Mobile Support • Cross-platform consent management • Multiple feature and functionality service offering • A/B testing • Meets consumer expectations • Ability to customize • Multiple language capabilities • Real time dashboards for tracking

How to Get Started

IAB Canada continues to build educational resources to help our members become and think privacy-first. We have started to build a resource of presentations by TCF approved CMPs that you can find in our Resource Centre, and continue to build this library. If looking to add a CMP to your privacy toolkit, we suggest that you start here.

Glossary of Terms

Term	Definition
CMP	Consent Management Platform: the company or organization that centralizes and manages transparency for, and consent and objections of the end user. The CMP can read and update the Permission status of Vendors on the GVL, and acts as an intermediary between a Publisher, an end user, and Vendors to provide transparency, help Vendors and Publishers establish Permissions for collecting, using, or disclosing personal information, acquire user consent as needed and manage user objections, and communicate Permissions, and/or consent or objection status to the ecosystem. A CMP may be the party that surfaces, usually on behalf of the publisher, the UI to a user, though that may also be another party. CMPs may be private or commercial. A private CMP means a Publisher that implements its own CMP for its own purposes. A commercial CMP offers CMP services to other parties.
TCF	Transparency and Consent Framework: Framework comprising the various parts defined under standard Policies. It has the objective to help all parties in the digital advertising chain to comply with Privacy Law when collecting, using, or disclosing personal information.
GVL	Global Vendor List: the list of Vendors who have registered with IAB for participating in the Framework. The list is currently managed and maintained by IAB Europe, and is referenced by CMPs, Publishers and individual Vendors. Its structure and content shall be defined by the Specifications.
Purpose	One of the defined purposes for which personal information is collected, used, or disclosed by participants in the Framework that are defined in the Policies or the Specifications for which Vendors seek Permission and for which the user is given choice, i.e. to seek Permission to collect, use or disclose personal information.
Special Purpose	One of the defined purposes for collecting, using, or disclosing of personal information by participants in the Framework that are defined in the Policies or the Specifications, for which Vendors collect, use or disclose personal information and for which the user is not given choice by a CMP because the collection, use or disclosure may occur without consent under Canadian Privacy law.
PIPEDA	PIPEDA is an acronym for the Personal Information Protection and Electronic Documents Act which is our current privacy law in Canada. This is a Canadian

	law relating to data privacy that governs how private sector organizations collect, use and disclose personal information in the course of commercial business.
CPPA	The Consumer Privacy Protection Act, if passed would act as an update and expansion to the pre-existing federal, privacy law – PIPEDA. The CPPA was introduced in an effort to significantly increase protections for Canadians' personal information by giving Canadians more control over how companies handle their personal information. Other key new features include monetary penalties, increased order-making power for the Commissioner and new transparency rules for automated decision systems.
CCPA	The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States. gives consumers more control over the personal information that businesses collect about them and offers them the right ask companies to delete that information or opt-out of its collection altogether.
GDPR	The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). It also addresses the transfer of personal data outside the EU and EEA areas.
DPA	Data Protection Authorities (DPAs) are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws.

Additional Resources

Click here to find all available information and resources for the IAB Europe TCF.

For quick access to a full list of IAB Europe certified CMPs you can look here.

Getting Involved

If you would like to contribute to either of the TCF, Privacy or Project Rearc working groups, or have suggestions on content for this document, please contact us at policy@iabcanada.com