IAB Canada Transparency & Consent Framework Policies

- This document lays out the Policies applicable to participants in the IAB Canada Transparency & Consent Framework.
- Participants may include publishers, advertisers, vendors, and/or CMPs. Each category of participant has specific obligations and requirements which are included in these Policies.
- Participants must adhere to these Policies to maintain their participation in the Framework.
- Participants must not amend, supplement, or modify their implementation of the Framework unless expressly provided for in the Policies or Specifications.
- Participants must comply with Canadian Privacy Law. In the event of a conflict between applicable law and the Policies, the law prevails.
- Participants should avoid profiling or categorizing individuals in a way that leads to unfair, unethical or discriminatory treatment contrary to human rights law.

Copyright © 2021 IAB Canada. All rights reserved.

Outline

Copyright © 2021 IAB Canada. All rights reserved.

Appendix A: Purposes and Features Definitions

A. Purposes

Purpose 2 - Select basic ads

Purpose 3 - Create a personalized ads profile

Purpose 4 - Select personalized ads

Purpose 5 - Create a personalized content profile

Purpose 6 - Select personalized content

Purpose 7 - Measure ad performance

Purpose 8 - Measure content performance

Purpose 9 - Apply market research to generate audience insights

Purpose 10 - Develop and improve products

B. Special Purposes

Special Purpose 1 - Ensure security, prevent fraud, and debug

Special Purpose 2 - Technically deliver ads or content

C. Features

Feature 1 - Match and combine offline data sources

Feature 2 - Link different devices

Feature 3 - Receive and use automatically sent device characteristics for identification

D. Special Features

Special Feature 1 - Use precise geolocation data

Special Feature 2 - Actively scan device characteristics for identification

E. Stacks

Stack 1 - Precise geolocation data, and identification through device scanning

Stack 2 - Basic ads and ad measurement

Stack 3 - Personalized ads

Stack 4 - Basic ads, ad measurement, and audience insights

Stack 5 - Basic ads, personalized ads profile, and ad measurement

Stack 6 - Personalized ads display and ad measurement

Stack 7 - Personalized ads display, ad measurement, and audience insights

Stack 8 - Personalized ads and ad measurement

Stack 9 - Personalized ads, ad measurement, and audience insights

Stack 10 - Personalized ads profile and display

Copyright © 2021 IAB Canada. All rights reserved.

Stack 11 - Personalized content

Stack 12 - Personalized content display and content measurement

Stack 13 - Personalized content display, content measurement and audience insights

Stack 14 - Personalized content and content measurement

Stack 15 - Personalized content, content measurement and audience insights

Stack 16 - Personalized content, content measurement, audience insights, and product development.

Stack 17 - Ad and content measurement, and audience insights

Stack 18 - Ad and content measurement

Stack 19 - Ad measurement and audience insights

Stack 20 - Ad and content measurement, audience insights, and product development

Stack 21 - Content measurement, audience insights, and product development

Stack 22 - Content measurement and product development

Stack 23 - Personalized ads and content display, ad and content measurement

Stack 24 - Personalized ads and content display, ad and content measurement, and audience insights

Stack 25 - Personalized ads and content, ad and content measurement

Stack 26 - Personalized ads and content, ad and content measurement, and audience insights

Stack 27 - Personalized ads and content profile

Stack 28 - Personalized ads and content display

Stack 29 - Basic ads, ad and content measurement, and audience insights

Stack 30 - Personalized ads display, personalized content, ad and content measurement, and audience insights

Stack 31 - Personalized ads display, personalized content, ad and content measurement, audience insights, and product development

Stack 32 - Basic ads, personalized content, ad and content measurement, and audience insights

Stack 33 - Basic ads, personalized content, ad and content measurement, audience insights, and product development

Stack 34 - Basic ads, personalized content, content measurement, and audience insights

Stack 35 - Basic ads, personalized content, content measurement, audience insights, and product development

Copyright © 2021 IAB Canada. All rights reserved.

Copyright © 2021 IAB Canada. All rights reserved.

Preamble

i. The Transparency and Consent Framework consists of a set of technical specifications and policies to which publishers, advertisers, technology providers, and others for whom the Framework is of interest may voluntarily choose to adhere.

ii. The goal of the Framework is to help players in the online ecosystem become compliant with Canadian Privacy Law. The Framework provides a way of informing users that their personal information is collected, used, or disclosed, the purposes for which their personal information is collected, used, or disclosed, and the companies that are seeking to collect, use, or disclose their personal information for these purposes. The Framework also provides users with choice about the same, and signals to third parties inter alia which information has been disclosed to users and what users' choices are.

iii. Achieving the goals of the Framework requires standardization of technology, for example of how information is disclosed or how user choices are stored and signaled to participants. It also requires standardizing certain information provided to users, choices given to users, and behaviours that participants engage in when interacting with users or responding to requests between participants.

iv. The Framework is not intended, nor has it been designed to facilitate the lawful collection, use, or disclosure of sensitive personal information except ones that are defined as special purposes.

v. While participation in the Framework may be a useful and essential building block for the online ecosystem's compliance with Canadian Privacy Law, it is not a substitute for individual participants taking responsibility for their obligations under the law.

vi. The Framework should only be used for the collection of personal information to the extent that this personal information is necessary to achieve the purposes disclosed by participants.

vii. The Framework is intended to be updated over time as legislation is updated, and legal requirements, regulatory practice, business practices, business needs and other relevant factors change.

Copyright © 2021 IAB Canada. All rights reserved.

Chapter I: Definitions

1. Definitions

1. "**Transparency and Consent Framework**" (the "**Framework**", or the "**TCF**") means the Framework comprising the various parts defined under these Policies. It has the objective to help all parties in the digital advertising chain to comply with Canadian Privacy Law when collecting, using, or disclosing personal information.

2. "**Interactive Advertising Bureau of Canada**" ("**IAB Canada**", the "**Managing Organization**", or the "**MO**") means the entity that manages and governs the Framework, including the Policies, Specifications, and the Global Vendor List. IAB Canada may update these Policies from time to time as it reasonably determines is necessary to ensure the ongoing success of the Framework. IAB Canada may designate a third party or third parties to take on certain functions and/or tasks of the MO under the Framework on its behalf.

3. "**Framework Policies**" (the "**Policies**") means this or any other official policy documentation disseminated by IAB Canada and updated from time to time, that defines the requirements for compliant participation in, and use of, the Framework, including, but not limited to, Appendix A and Appendix B of these Policies, and any associated policy guidance, or publicly communicated, enforcement actions.

4. "**Framework Specifications**" (the "**Specifications**") means any official technical documentation disseminated by IAB Canada in concert with IAB Tech Lab or future designated technical body, and updated from time to time, that defines the technical implementation of the Framework, including, but not limited to, the Transparency and Consent String with Global Vendor List Format specification, the Consent Management Platform API specification, and any associated implementation guidance.

5. "**Global Vendor List**" (the "**GVL**", or the "**Vendor List**") means the list of Vendors who have registered with IAB Canada for participating in the Framework. The list is managed and maintained by IAB Canada, and is referenced by CMPs, Publishers and individual Vendors. Its structure and content shall be defined by the Specifications.

6. "**Transparency and Consent Management Platform**" ("**Consent Management Platform**", or "**CMP**") means 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

Copyright © 2021 IAB Canada. All rights reserved.

that implements its own CMP for its own purposes. A commercial CMP offers CMP services to other parties. Unless specifically noted otherwise, these policies apply to both private and commercial CMPs.

7. "**Vendor**" means a company that participates in the delivery of digital advertising within a Publisher's website, app, or other digital content, to the extent that company is not acting as a Publisher or CMP, and that either accesses an end user's device or collects, uses, or discloses personal information about end users visiting the Publisher's content and adheres to the Policies.

8. "**Publisher**" means an operator of a Digital Property and who is primarily responsible for ensuring the Framework UI is presented to users and that Permissions, including consent, are established with respect to Vendors that may process personal information based on users' visits to the Publisher's content.

9. "**Digital Property**" means a website, app, or other content or service delivery mechanism where digital ads are displayed, or information is collected and/or used for any Purpose or Special Purpose.

10. "**Framework UI**" ("**UI**") means the user interface or user experience defined by the Specifications for presentation to a user in order to establish Permissions for GVL Vendors as part of their compliance with Canadian Privacy Law. The Policies and Specifications define requirements for the UI along with aspects that are configurable by Publishers.

11. "**Initial Layer**" refers to information that must be made visible to the user in the UI prior to the user being able to give his or her consent. For the avoidance of doubt, the use of the term "visible" should not be understood as excluding other forms of information presentation used, for example, for assisted internet access, or on devices with non-visual user interfaces.

12. "**Purpose**" means 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.

13. "**Special Purpose**" means 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.

14. "**Feature"** means one of the features for which personal information is used by participants in the Framework that are defined in the Policies or the Specifications used in pursuit of one or several Purposes for which the user is not given choice separately to the choice afforded regarding the Purposes for which they are used.

Copyright © 2021 IAB Canada. All rights reserved.

15. "**Special Feature**" means one of the features for which personal information is used by participants in the Framework that are defined in the Policies or the Specifications used in pursuit of one or several Purposes for which the user is given the choice to opt-in (e.g. collection, use or disclosure of precise geolocation) separately from the choice afforded regarding the Purposes for which they are used.

16. "**Stack**" means one of the combinations of Purposes and/or Special Features for which personal information is collected, used, or disclosed by participants in the Framework that may be used to substitute or supplement more granular Purpose and/or Special Feature descriptions in the Initial Layer of a UI.

17. "**Signal**" means any signal defined by the Policies or Specifications sent by a CMP, usually on behalf of a Publisher, to Vendors that includes Permission information, e.g., information about the transparency, and/or consent status of a Vendor and/or Purpose, the opt-in status of a Special Feature, and Publisher restrictions.

18. "**Precise Geolocation Data**" means information about a user's geographic location accurate to up to 500 meters and/or latitude and longitude data beyond two decimal points.

19. **"Permission"** means a permission for collecting, using, or disclosing personal information under the Framework using Consent as required in accordance with Canadian Privacy Law. Permissions in the Framework can be established with:

(a) Service-specific scope, which means a Permission is applicable only on the service (e.g. Permission is obtained and managed for a Publisher website or app);
(b) Group-specific scope, which means a Permission is applicable only on a pre-defined group of services (e.g. a number of Digital Properties of one or more Publishers that implement CMPs with their group's scope, each of which allows users to manage their choices regarding Permissions established for the group across all the services of the group);
(c) Global scope, which means a Permission is not only applicable on the service, on which the Permission is obtained and managed, but across all Publisher Digital Properties, that implement CMPs with global scope each of which allows users to manage their choices regarding globally established Permissions across all such Publisher Digital Properties; or
(d) Out-of-band ("OOB"), which means a Permission has not been established using the Framework and is therefore not reflected in any Signals within the Framework and cannot be managed by users within the Framework.

21. "**Canadian Privacy Law"** means any federal or provincial private or public sector privacy legislation which govern the collection, use and disclosure of personal information such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) or the *Privacy Act,* as amended.

Copyright © 2021 IAB Canada. All rights reserved.

22. **"Consent"** under the Framework means express consent unless the Policies or Specifications specify that implied consent is appropriate, as prescribed in accordance with Canadian Privacy Law.

23. "**Personal Information**" refers to any information that qualifies as personal information under Canadian Privacy Law.

Chapter II: Policies for CMPs

2. Applying and Registering

1. CMPs must apply to IAB Canada for participation in the Framework. IAB Canada shall take reasonable steps to vet and approve a CMP's application according to procedures adopted, and updated from time to time, by the MO.

2. CMPs must provide all information requested by IAB Canada that is required to fulfil IAB Canada's CMP application and approval procedures.

3. IAB Canada shall not approve a CMP's application unless and until IAB Canada can verify to its satisfaction the identity of the party or parties controlling the CMP, as well as the CMP's ability to maintain its service and adhere to the Policies and Specifications.

3. Adherence to Framework Policies

1. A CMP must adhere to all Policies applicable to CMPs that are disseminated by the MO in the Policies or in documentation that implements the Policies, such as in operating policies and procedures, guidance, and enforcement decisions.

2. A CMP must make a public attestation of compliance with the Policies in a prominent disclosure, such as in a privacy policy. This attestation must at minimum include: (i) an affirmation of the CMP's participation in the IAB Canada Transparency & Consent Framework; (ii) an affirmation of its compliance with the Policies and Specifications of the Transparency & Consent Framework; (iii) the IAB Canada-assigned ID of the CMP. Example:

> *<Organization> participates in the IAB Canada Transparency & Consent Framework and complies with its Specifications and Policies. <Organization> operates Consent Management Platform with the identification number <CMP ID>.*

Copyright © 2021 IAB Canada. All rights reserved.

4. Adherence to the Specifications

1. In addition to implementing the Framework according to the Specifications, a CMP must support the full Specifications, unless the Specifications expressly state that a feature is optional, in which case a CMP may choose to implement the optional feature but need not do so.

2. A private CMP need only implement the Specifications to the extent necessary to support the needs of the Vendors, Purposes, and Special Features selected by its Publisher owner.

3. A CMP must disclose Vendors' GVL information, including Permissions sought, as declared, and update Vendors' GVL information, including Permission status in the Framework, wherever stored, according to the Specifications, without extension, modification, or supplementation, except as expressly allowed for in the Specifications.

4. A CMP must not read, write, or communicate any Vendor's Permissions except according to and as provided for under the Specifications, and using the standard API.

5. Managing Purposes and Permissions

1. A CMP will remind the user of their right to withdraw consent for the collection, use, or disclosure of their personal information at least every 13 months with respect to any Vendor and Purpose.

2. A CMP must resolve conflicts in Signals or merge Signals before transmitting them (e.g. reconciliation between service-specific and global transparency and consent) in accordance with the Policies and Specifications.

3. A CMP must only generate a positive consent Signal on the basis of a clear affirmative action taken by a user that unambiguously signifies that user's agreement on the basis of appropriate information and in accordance with Canadian Privacy Law.

4. A CMP must only generate a positive Signal for implied consent on the basis of the provision of transparency by the CMP about collecting, using, or disclosing of personal information and a positive Signal must not persist if the user indicates an objection to such collection, use, or disclosure of personal information.

5. A CMP must only generate a positive Signal for Special Features with the consent of the user.

6. A CMP will establish Permissions only in accordance with the declarations made by Vendors in the GVL and using the definitions of the Purposes and/or their translations found in the GVL, without extension, modification, or supplementation, except as expressly allowed for in the Policies.

Copyright © 2021 IAB Canada. All rights reserved.

7. A CMP must resurface the Framework UI if the MO indicates, in accordance with the Policies and Specifications, that changes to the Policies are of such a nature as to require re-establishing Permissions.

8. A CMP may be instructed by its Publisher which Purposes, Special Features, and/or Vendors to disclose. If a Publisher instructs a CMP not to disclose a Purpose, Special Feature, and/or a Vendor, the Signals the CMP generates must appropriately reflect in the Signal that no Permissions have been established for the respective Purposes, Special Features, and/or Vendors. For the avoidance of doubt: Special Purposes, and Features must always be disclosed if at least one of the Vendors disclosed has declared itself using them.

9. A CMP must implement any Publisher restrictions, such as a restriction of Purposes per Vendors, by making appropriate changes in the User Interface to reflect such restrictions, and by creating the appropriate Signals containing the Publisher restrictions in accordance with the Policies and Specifications.

11. A CMP may be instructed by its Publisher to establish, record and transmit information about its own Permissions (that is, Permissions for collecting, using, or disclosing personal information by the Publisher), including Permissions for purposes that are not supported by the Framework. A CMP is prohibited from implementing Publisher-specific custom Permission Signals for Purposes that the Framework covers, or for any vendors rather than purposes. Management of Permissions that the Framework covers shall only take place if the Vendor has registered with the MO in accordance with the Policies. A CMP may exclusively implement Publisher-specific custom Permission Signals in conjunction with the Publisher's own collection, use, or disclosure of personal information or for collecting, using, or disclosing personal information on its behalf by a Vendor who processes such personal information under applicable Canadian Privacy Law and only for purposes not standardized by the Framework.

6. Working with Vendors

1. If a CMP works with Vendors who are not participating in the Framework and who are not published on the GVL, the CMP must make it possible for users to distinguish between those Vendors who are participating in the Framework, on the one hand, and those who are not, on the other. CMPs must not misrepresent Vendors who are not registered with IAB Canada as participating in the Framework and being published on the GVL.

2. If a Publisher or Vendor operates a CMP, the Policies for CMPs shall apply only to the extent of that party's CMP operation. For example, if a Publisher operates a CMP, the prohibition against a CMP discriminating against Vendors shall apply to the Publisher's CMP only, while the Publisher remains free to make choices with respect to Vendors appearing on its Digital Properties.

3. In any interaction with the Framework, a CMP may not exclude, discriminate against, or give preferential treatment to a Vendor except pursuant to explicit instructions from the Publisher involved in that interaction and in accordance with the Specifications and the Policies. For the

Copyright © 2021 IAB Canada. All rights reserved.

avoidance of doubt, nothing in this paragraph prevents a private CMP from fully implementing instructions from its Publisher owner.

4. If a Vendor operates a CMP, it may require a Publisher to work with its Vendor-owner as part of the terms and conditions of using the CMP. Such a requirement shall not constitute preferential treatment in the meaning of Policy 6(3).

5. If a CMP reasonably believes that a Vendor is not in compliance with the Specifications and/or the Policies, it must promptly notify IAB Canada according to MO procedures and may, as provided for by MO procedures, pause working with the Vendor while the matter is addressed.

7. Working with Publishers

1. A CMP shall only work with Publishers within the Framework that are in full compliance with the Policies, including but not limited to the requirement to make an attestation of compliance in a prominent location, such as a privacy policy.

2. A CMP is responsible for ensuring that its UIs and Signals comply with the Policies and Specifications. Where a commercial CMP is not able to ensure such compliance, for example because it offers Publishers the option to customize aspects that may impact compliance, the Publisher using such customization options must assume responsibility for compliance with the Policies for CMPs, register a private CMP within the Framework, and use the commercial CMPs offering in association with the Publisher's assigned private CMP ID.

3. If a CMP reasonably believes that a Publisher using its CMP is not in compliance with the Specifications and/or the Policies, it must promptly notify IAB Canada according to MO procedures and may, as provided for by MO procedures, pause working with the Publisher while the matter is addressed. For the avoidance of doubt, where a commercial CMP receives an instruction from a Publisher that is in violation of these Policies, the CMP shall not act on the instruction.

4. The MO may prevent a Publisher from participation in the Framework for violations of Framework Policies that are willful and/or severe according to MO procedures. The MO may enact a suspension or block of a Publisher by notifying CMPs that the Publisher is not in full compliance.

8. Record Keeping

1. A CMP will maintain records of all Permissions and will provide the MO access to such records upon request without undue delay.

2. A CMP will retain a record of the UI that has been deployed on any given Publisher at any given time and make this record available to its Publisher client, Vendors, and/or the MO upon request.

Copyright © 2021 IAB Canada. All rights reserved.

9. Accountability

1. IAB Canada shall take reasonable steps to periodically review and verify a CMP's compliance with the Policies and/or the Specifications according to procedures adopted, and updated from time to time, by the MO. A CMP will provide, without undue delay, any information reasonably requested by IAB Canada to verify compliance.

2. IAB Canada may suspend a CMP from participation in the Framework for any failure to comply with the Policies and/or the Specifications until the CMP comes into full compliance and demonstrates its intention and ability to remain so to the MO's satisfaction. The MO may expel a CMP from participation in the Framework for violations of Policies that are willful and/or severe.

3. Additionally, IAB Canada may, at its discretion and according to MO procedures, take additional actions in response to a CMP's non-compliance, including publicly communicating the CMP's non-compliance and reporting the non-compliance to the federal or provincial Privacy Regulator's Office, as the case may be.

Chapter III: Policies for Vendors

10. Applying and Registering

1. Vendors must apply to IAB Canada for participation in the Framework. IAB Canada shall take reasonable steps to vet and approve a Vendor's application according to procedures adopted, and updated from time to time, by the MO.

2. Vendors must provide all information requested by the MO that is reasonably required to fulfil the MO's application and approval procedures.

3. Vendors must have all legally required disclosures in a prominent, public-facing privacy policy on their websites.

4. The MO will not approve a Vendor's application unless or until the MO can verify to its satisfaction the identity of the party or parties controlling the Vendor, as well as the Vendor's ability to maintain its service and adhere to the Framework policies.

5. A Vendor will provide to the MO, and maintain as complete and accurate, all information required for inclusion in the GVL, according to the GVL Specifications. This includes the Purposes and Special Purposes for which it seeks Permission to collect, use, or disclose personal information, and the Features and Special Features it relies on in pursuit of such Purposes and Special Purposes. It will ensure its Purposes, Special Purposes, Features, and Special Features are completely and accurately included in the GVL. It will notify the MO of any changes in a timely manner.

Copyright © 2021 IAB Canada. All rights reserved.

11. Adherence to Framework Policies

1. A Vendor must adhere to all policies applicable to Vendors that are disseminated by the MO in this document or in documentation that implements the Policies, such as in operating policies and procedures, guidance, and enforcement decisions. See Accountability below regarding enforcement.

2. A Vendor must make a public attestation of compliance with the Policies in a prominent disclosure, such as in a privacy policy. This language must at a minimum include: (i) participation in the IAB Canada Transparency & Consent Framework; (ii) compliance with the Policies and Specifications with the Transparency & Consent Framework; (iii) the IAB Canada assigned ID that the Vendor uses. Example:

> *<Organization> participates in the IAB Canada Transparency & Consent Framework and complies with its Specifications and Policies. <Organization>'s identification number within the framework is <Vendor ID>.*

12. Adherence to the Specifications

1. In addition to implementing the Framework only according to the Specifications, a Vendor must support the full Specifications, including being able to retrieve and/or pass on Signals in the technical formats required by the Specifications and in accordance with Policies, when available.

13. Working with CMPs

1. A Vendor shall work with a CMP within the Framework only if the CMP is in full compliance with the Policies, including but not limited to the requirements to register with IAB Canada, and to make a public attestation of compliance.

2. If a Vendor reasonably believes that a CMP is not in compliance with the Specifications and/or the Policies, it must promptly notify IAB Canada according to MO procedures and may, as provided for by MO procedures, pause working with the CMP while the matter is addressed.

3. A Vendor must respect Signals communicated by a CMP or received from a Vendor who forwarded the Signal originating from a CMP in accordance, with the Specifications and Policies, and act accordingly. A Vendor must respect Signals on an individual basis in real-time and must not rely on a stored version of a previously received Signal to process personal information for any Purpose and/or use any Special Feature where a more recent Signal has been received by that Vendor.

4. If a Vendor is unable to read or process the contents of a received Signal, the Vendor must assume that it does not have Permission to collect, use, or disclose personal information for any Purpose and/or Special Purpose.

Copyright © 2021 IAB Canada. All rights reserved.

5. If a Vendor is unable to act in accordance with the contents of a received Signal, the Vendor must not collect, use, or disclose personal information for any Purpose and/or Special Purpose.

6. A Vendor must not create Signals where no CMP has communicated a Signal, and shall only transmit Signals communicated by a CMP or received from a Vendor who forwarded a Signal originating from a CMP without extension, modification, or supplementation, except as expressly allowed for in the Policies and/or Specifications.

14. Working with Publishers

1. A Vendor shall work with a Publisher within the Framework only if the Publisher is in full compliance with the Policies, including but not limited to the requirement to make a public attestation of compliance.

2. If a Vendor reasonably believes that a Publisher is not in compliance with the Specifications and/or the Policies, it must promptly notify IAB Canada according to MO procedures and may, as provided for by MO procedures, pause working with the Publisher while the matter is addressed.

3. For the avoidance of doubt, contractual obligations that a Vendor is subject to with respect to the use of data override more permissive Signals for that Vendor about permissions to that data.

4. A Vendor must update its software for use by its Publisher and Vendor partners, such as scripts and tags that result in the collection, use, or disclosure of personal information to ensure compliance with the Specifications, and/or the Policies. In particular, the requirement to not collect, use, or disclose personal information prior to verifiably receiving a Permission for collection, use, or disclosure of personal information as communicated by the appropriate Signal in accordance with the Policies and Specifications.

5. A Vendor shall update software provided by its Vendor partners present on its services, such as scripts and tags that result in the collection, use, or disclosure of personal information, if the Vendor partner has provided updated software for the purpose of complying with the Specifications and/or the Policies.

15. Demonstrating Permissions

1. A Vendor must be able to demonstrate Permissions, either by maintaining records of Permissions granted by users, or an equivalent mechanism designed to demonstrate that Permissions have been obtained in a manner compliant with the Policies and the Specifications, and will provide the MO access to such records upon request without undue delay.

2. A Vendor can choose to maintain records of user identification, timestamps, and received Signals for the full duration of the relevant collection, use, or disclosure of personal information. A Vendor may additionally choose to maintain such records of user identification, timestamps, and Signals beyond the duration of the collection, use, or disclosure of personal information as

Copyright © 2021 IAB Canada. All rights reserved.

required to comply with legal obligations or to reasonably defend or pursue legal claims, and/or for other collection, use, or disclosure allowed by law consistent with the purposes for which the data was originally collected or received.

3. Alternatively, a Vendor may choose to demonstrate Permissions through other means, such as providing a demonstration of the Vendor's received Signals workflow.

16. Purposes, Special Purposes, Special Features, and Opt-Ins

1. A Vendor must not collect, use, or disclose personal information relating to a user without a Permission to do so.

2. A Vendor shall indicate on the GVL that it seeks Permissions under the Framework to collect, use, or disclose personal information toward a Purpose and/or Special Purpose;

3. A Vendor shall indicate on the GVL that it will collect, use, or disclose personal information for a Special Purpose.

4. A Vendor shall indicate on the GVL the Features it relies on in support of one or more Purposes and/or Special Purposes.

5. A Vendor shall indicate on the GVL the Special Features it relies on in support of one or more Purposes and/or Special Purposes.

6. Where a situation falls within the Framework, in addition to complying with relevant Canadian Privacy Law, a Vendor wishing to rely on the user's consent for the collection, use, or disclosure of his or her personal information will only do so if it can verify by way of the appropriate Signal in accordance with the Specifications and Policies that the user has given his or her appropriate consent (implied or otherwise) for collection, use, or disclosure of his or her personal information before or at the moment any personal information is collected, used, or disclosed.

7. Where a situation falls within the Framework, in addition to complying with relevant Canadian Privacy Law, a Vendor wishing to make use of a Feature will only do so if it has indicated on the GVL its use of the Features it wishes to rely on in support of one or more Purposes and/or Special Purposes.

8. By way of derogation of Policy 16(7), a Vendor may receive and use automatically sent device characteristics for identification without having indicated on the GVL its use of the Feature to receive and use automatically sent device characteristics for identification to:

(a) Collect, use, or disclose the identifiers obtained through automatically sent device characteristics for identification for the Special Purpose of ensuring security, preventing fraud, and debugging provided that
    (i) the Vendor complies with relevant Canadian Privacy Law;

Copyright © 2021 IAB Canada. All rights reserved.

(ii) the Vendor has conducted a privacy impact assessment for the collection, use, or disclosure of identifiers obtained through automatically sent device characteristics for identification collected, used, or disclosed under this derogation;

(iii) the Vendor actively minimizes collection, use, or disclosure of identifiers obtained through automatically sent device characteristics for identification collected, used, or disclosed under this derogation;

(iv) the Vendor puts in place reasonable retention periods for the identifiers obtained through automatically sent device characteristics for identification collected, used, or disclosed under this derogation;

(v) the Vendor only retains the identifiers obtained through automatically sent device characteristics for identification collected, used, or disclosed under this derogation in an identifiable state for as long as is necessary to fulfil the Special Purpose of ensuring security, preventing fraud, and debugging;

(vi) the Vendor erases the personal information associated with identifiers obtained through automatically sent device characteristics for identification collected, used, and/or disclosed under this derogation as soon as possible; and

(vii) the data associated with identifiers obtained through automatically sent device characteristics for identification collected, used, or disclosed under this derogation is never used for any other Purposes and/or Special Purposes. The prohibition of change of purpose of the collecting, using, or disclosing of data associated with identifiers obtained through automatically-sent device characteristics for identification under this derogation does not preclude a Vendor from indicating on the GVL its use of the Feature to use automatically-sent device characteristics for identification at a later time and associating data with such identifiers for other Purposes and/or Special Purposes after having made the indication. However, the prohibition does not permit using any data associated with the identifier for the Special Purpose of ensuring security, preventing fraud, and debugging that has occurred under this derogation for any other Purposes and/or Special Purposes and, for example, also precludes changing Purpose with the explicit consent of the user.

9. Where a situation falls within the Framework, in addition to complying with relevant Canadian Privacy Law, a Vendor wishing to make use of a Special Feature will only do so with the opt-in of the user and if it can verify by way of the appropriate Signal in accordance with the Specifications and Policies that the user has given his or her opt-in for the use of the Special Feature before any Special Feature is used by the Vendor, unless expressly provided for by, and subject to, the Policies and/or Specifications.

10. By way of derogation of Policy 16(9), a Vendor may process Precise Geolocation Data without the opt-in of the user to the Special Feature of using Precise Geolocation Data to:

(a) immediately render the Precise Geolocation Data into a non-precise state, for example by truncating decimals of latitude and longitude data, without collecting, using, or disclosing the Precise Geolocation Data in its precise state in any other way;

Copyright © 2021 IAB Canada. All rights reserved.

(b) process the Precise Geolocation Data for the Special Purpose of ensuring security, preventing fraud, and debugging, provided that
   (i) the Vendor complies with relevant Canadian Privacy Law;
   (ii) the Vendor has conducted a privacy impact assessment for the collection, use, or disclosure of Precise Geolocation Data collected, used, or disclosed under this derogation;
   (iii) the Vendor actively minimizes collection, use, or disclosure of Precise Geolocation Data collected, used, or disclosed under this derogation;
   (iv) the Vendor puts in place reasonable retention periods for the Precise Geolocation Data collected, used, or disclosed under this derogation;
   (v) only retains the Precise Geolocation Data collected, used, or disclosed under this derogation in an identifiable and/or precise state for as long as is necessary to fulfill the Special Purpose of ensuring security, preventing fraud, and debugging;
   (vi) erases the Precise Geolocation Data collected, used, or disclosed under this derogation as soon as possible; and
   (vii) the Precise Geolocation Data collected, used, or disclosed under this derogation is never used for any other Purposes and/or Special Purposes. The prohibition of change of purpose of the collection, use, or disclosure of Precise Geolocation Data collected under this derogation is absolute, and, for example, also precludes changing Purpose with the explicit consent of the user.

11. By way of derogation of Policy 16(9), a Vendor may actively scan device characteristics for identification without the opt-in of the user to the Special Feature of actively scanning device characteristics for identification to:

(a) Collect, use, or disclose the identifiers obtained through actively scanning device characteristics for identification for the Special Purpose of ensuring security, preventing fraud, and debugging provided that
   (i) the Vendor complies with relevant Canadian Privacy Law;
   (ii) the Vendor has conducted a privacy impact assessment for the collection, use, or disclosure of identifiers obtained through actively scanning device characteristics for identification collected, used, or disclosed under this derogation;
   (iii) the Vendor actively minimizes collection, use, or disclosure of identifiers obtained through actively scanning device characteristics for identification collected, used, or disclosed under this derogation;
   (iv) the Vendor puts in place reasonable retention periods for the identifiers obtained through actively scanning device characteristics for identification collected, used, or disclosed under this derogation;
   (v) only retains the identifiers obtained through actively scanning device characteristics for identification collected, used, or disclosed under this derogation in an identifiable state for as long as is necessary to fulfil the Special Purpose of ensuring security, preventing fraud, and debugging;
   (vi) the Vendor erases the data associated with identifiers obtained through actively scanning device characteristics for identification collected, used, or disclosed under this derogation as soon as possible;

Copyright © 2021 IAB Canada. All rights reserved.

(vii) the data obtained through actively scanning device characteristics for identification collected, used, or disclosed and any data associated with this identifier under this derogation are never used for any other Purposes and/or Special Purposes. The prohibition of change of purpose of the collection, use, or disclosure of identifiers obtained through actively scanning device characteristics for identification and data associated with this identifier under this derogation does not preclude obtaining an opt-in for actively scanning device characteristics for identification at a later time and associating data with such identifiers for other Purposes and/or Special Purposes after having obtained such an opt-in. However, the prohibition does not permit using any data associated with the identifier for the Special Purpose of ensuring security, preventing fraud, and debugging that has occurred under this derogation for any other Purposes and/or Special Purposes and, for example, also precludes changing Purpose with the explicit consent of the user.

12. By way of derogation of Policy 16(6), 16(7), and Policy 16(9), Vendors may obtain Permissions to collect, use, or disclose personal information for one or more Purposes and/or Special Purposes outside of the Framework, or establish express consent for making use of Special Features outside of the Framework, for collecting, using, or disclosing personal information in association with a user's visit to a Publisher that participates in the Framework, so long as the OOB Permissions for collecting, using, or disclosing personal information for one or more Purposes and/or Special Purposes, and/or the OOB opt-ins for making use of one or more Special Features, are sufficient for such collection, use or disclosure. Use within the Framework of such OOB Permissions and/or opt-ins established outside of the Framework is subject to Policy 16(13).

13. Where a situation falls within the Framework, a Vendor must not process personal information for any Purpose and/or Special Purpose in reliance on Permissions obtained outside of the Framework, nor make use of Special Features in reliance on Permissions established outside of the Framework, for any collection, use, or disclosure in association with a user's visit to a Publisher that participates in the Framework, unless

(a) the Publisher's CMP is configured to make use of the global Permission scope;
(b) the Publisher informs users of the possibility that Vendors, whom the Publisher does not disclose directly, may process their personal information for one or more Purpose, Special Purposes, and/or use one or more Special Feature disclosed by the Publisher in line with an OOB Permission and/or OOB opt-in established in previous interactions with those Vendors in other contexts;
(c) the user has not interacted with and/or made a choice about the Vendor, for example by giving or refusing consent, and the Vendor does not process any data on the basis of an OOB Permission for any
    (i) Purpose for which the user has refused or withdrawn consent within the Framework;
    (ii) Special Feature for which the user has refused to opt-in, or opted-out, within the Framework;

Copyright © 2021 IAB Canada. All rights reserved.

(d) the Vendor is able to verify by way of the appropriate Signal, in accordance with the Specifications and Policies, that the requirements of Policy 16(13)(a)-(c) for relying on OOB Permissions are met; and
(e) the Vendor is able to demonstrate that it has obtained Permission outside of the Framework for use in the Framework by keeping appropriate records other than a mere contractual obligation requiring a third party to organize valid Permissions on its behalf, and will make such records available to the MO without undue delay upon request.

17. A Vendor must not transmit personal information to another Vendor unless the Framework's Signals show that the receiving Vendor has a Permission for the disclosure of the personal information. For the avoidance of doubt, a Vendor may in addition choose not to transmit any data to another Vendor for any reason.

18. By way of derogation of Policy 16(17), a Vendor may transmit personal information to another Vendor if it can verify by way of the appropriate Signal in accordance with the Specifications and Policies that the receiving Vendor may process personal information on the basis of a Permission established outside of the Framework under Policy 16(12) and 16(13), and it has a justified basis for relying on the recipient Vendor's having a Permission to collect, use, or disclose the personal information in question.

19. A Vendor must not transmit a user's personal information to an entity outside of the Framework unless it has a justified basis for relying on that entity's having a Permission to collect, use, or disclose the personal information in question or is compelled to do so by way of statute, government regulation or judicial order.

20. If a Vendor receives a user's personal information without having a Permission for the collection, use, or disclosure of that personal information, the Vendor must quickly cease collecting, using, or disclosing the personal information and must not further transmit the personal information to any other party, even if that party has a Permission to collect, use, or disclose the personal information in question.

17. Accountability

1. The MO may adopt procedures for periodically reviewing and verifying a Vendor's compliance with the Policies. A Vendor will provide, without undue delay, any information reasonably requested by the MO to verify compliance.

2. The MO may suspend a Vendor from participation in the Framework for its failure to comply with the Policies until the Vendor comes into full compliance and demonstrates its intention and ability to remain so. The MO may expel a Vendor from participation in the Framework for violations of the Policies that are willful and/or severe.

Copyright © 2021 IAB Canada. All rights reserved.

3. Additionally, the MO may, at its discretion and according to MO procedures, take additional actions in response to a Vendor's non-compliance, including publicly communicating the Vendor's non-compliance and reporting the non-compliance to data protection authorities.

Chapter IV: Policies for Publishers

18. Participation

1. A Publisher may adopt and use the Framework in association with its content as long as it adheres to the Policies and the Specifications.

2. Publishers must have and maintain all legally required disclosures in a public-facing privacy policy prominently linked to from the content in association with which they are using the Framework.

19. Adherence to Framework Policies

1. In addition to implementing the Framework only according to the Specifications, a Publisher must adhere to all policies applicable to Publishers that are disseminated by the MO in this document or in documentation that implements the Policies, such as in operating policies and procedures, guidance, and enforcement decisions. See Accountability below regarding enforcement.

2. A Publisher must make a public attestation of compliance with the Policies in a prominent disclosure, such as in a privacy policy. This language must at a minimum include: (i) an affirmation of its participation in the IAB Canada Transparency & Consent Framework; (ii) an affirmation of its compliance with the Policies and Specifications with the Transparency & Consent Framework; (iii) the IAB Canada assigned ID of the CMP that the publisher uses. Example:

> *<Organization> participates in the IAB Canada Transparency & Consent Framework and complies with its Specifications and Policies. <Organization> [operates|uses] the Consent Management Platform with the identification number <CMP ID>.*

20. Adherence to the Specifications

1. A Publisher must support and adhere to the full Specifications, without extension, modification, or supplementation except as expressly allowed for in the Specifications.

2. A Publisher must not read, write, or communicate any Vendor's Permissions except according to and as provided for under the Specifications, and using the standard API.

Copyright © 2021 IAB Canada. All rights reserved.

21. Working with CMPs

1. A Publisher will work with a CMP within the Framework only if the CMP is in full compliance with the Policies and the Specifications, including but not limited to the requirement for the CMP to register with the MO.

2. If a Publisher reasonably believes that a CMP is not in compliance with the Specifications and/or the Policies, it must promptly notify the MO according to MO procedures and may, as provided for by MO procedures, pause working with the CMP while the matter is addressed.

3. A Publisher may operate a private CMP. A Publisher's private CMP is subject to the Policies for CMPs just as a commercial CMP is, unless expressly stated otherwise in the Framework Policies or the Specifications.

22. Working with Vendors

1. A Publisher may choose the Vendors for which it wishes to provide transparency and help establish Permissions within the Framework. A Publisher may further specify the individual Purposes for which it wishes to help establish Permissions for each Vendor. The Publisher communicates, or instructs its CMP to communicate, its preferences to Vendors in accordance with the Specifications and Policies

2. A Publisher will, in accordance with the Specifications and Policies, and considering and respecting each Vendor's declarations on the GVL, signal to Vendors which Permission it has established on behalf of each Vendor.

3. For the avoidance of doubt, contractual obligations that a Publisher is subject to with respect to the Permissions of a Vendor to use of data must be reflected in the Signals to align with those contractual obligations.

4. A Publisher may work with Vendors that are not in the GVL but must be careful not to confuse or mislead users as to which Vendors are operating within the Policies.

5. For the avoidance of doubt, contractual obligations that a Vendor is subject to with respect to the use of data override more permissive Signals for that Vendor about Permissions to that personal information.

6. If a Publisher reasonably believes that a Vendor is not in compliance with the Specifications and/or the Policies, it must promptly notify the MO according to MO procedures and may, as provided for by those procedures, pause working with the Vendor while the matter is addressed.

7. A Publisher will undertake to update software present on its services of its Vendor-partners, such as scripts and tags that result in the collection, use, or disclosure of personal information, if

Copyright © 2021 IAB Canada. All rights reserved.

the Vendor has provided updated software for the purpose of complying with the Specifications and/or the Policies.

23. Managing Purposes and Permissions

1. The Framework does not dictate how Publishers respond to a user's acceptance or rejection of Purposes, Special Features, and/or Vendors.

2. A Publisher using the Framework is required to help establish transparency and Permissions in accordance with the Policies and Specifications.

3. A Publisher may choose which Purposes, Special Features, and/or Vendors to disclose. If a Publisher chooses not to disclose a Purpose, Special Feature, and/or a Vendor, the Signals must appropriately reflect in the Signal that no Permissions have been established for the respective Purposes, Special Features, and/or Vendors. For the avoidance of doubt: Special Purposes, and Features must always be disclosed if at least one of the Vendors disclosed has declared to be using them.

4. A Publisher may restrict certain Purposes for specific Vendors, these restrictions must be implemented by the CMP, which shall reflect Publisher restrictions in both the User Interface and the Signals in accordance with the Policies and Specifications.

5. A Publisher must not modify, or instruct its CMP to modify the Purpose, Special Purpose, Feature, or Special Feature names, definitions and/or their translations, or Stack names or their translations.

6. A Publisher must not modify, or instruct its CMP to modify, Stack descriptions and/or their translations unless

(a) the Publisher has registered a private CMP with the Framework, or its commercial CMP is using a CMP ID assigned to the Publisher for use with a private CMP;

(b) the modified Stack descriptions cover the substance of standard Stack descriptions, such as accurately and fully covering all Purposes that form part of the Stack;

(c) Vendors are alerted to the fact of a Publisher using custom Stack descriptions through the appropriate Signal in accordance with the Specification.

WARNING: MODIFYING STACK DESCRIPTIONS EVEN WHEN PERMITTED IS DISCOURAGED AS IT MAY INCREASE PUBLISHER AND VENDOR LEGAL RISKS AND MAY THEREFORE RESULT IN VENDORS REFUSING TO WORK WITH PUBLISHERS USING MODIFIED STACK DESCRIPTIONS. THIS COULD NEGATIVELY IMPACT PUBLISHER AD REVENUE.

Copyright © 2021 IAB Canada. All rights reserved.

7. If a Vendor that was not included in a prior use of the Framework UI is added by the Publisher, the Publisher must resurface or instruct its CMP to resurface the Framework UI to establish that Vendor's Permissions before signaling that the Vendor's Permissions have been established. It also means resurfacing the UI, for example, when a previously surfaced Vendor claims a previously undisclosed Purpose before signaling that the Vendor's Permissions have been established.[1]

8. Publishers should remind users, or instruct their CMPs to do so, of their right to withdraw consent, as applicable, at least every 13 months.

9. A Publisher will not be required to resurface the Framework UI, or instruct its CMP to do so, if it has disclosed a Vendor's Purposes and established a Vendor's Permissions in accordance with the Policies prior to a Vendor joining the GVL.

10. A Publisher must resurface the Framework UI, or instruct its CMP to do so, if the GVL indicates in accordance with the Specifications that changes to the Framework are of such a nature as to require re-establishing Permissions.

11. A Publisher may use the Specification to manage and store, or instruct its CMP to do so, its own Permissions, including Permissions for purposes that are not supported by the Framework. A Publisher must not use Publisher-specific custom Permissions Signals to formally or informally agree signaling with any Vendor for Purposes that the Framework covers. Such management of Permissions shall only take place if the Vendor has registered with the MO in accordance with the Policies. A Publisher may only use Publisher-specific custom Permissions Signals in conjunction with its own collection, use, or disclosure of personal information.

24. Accountability

1. The MO may adopt procedures for periodically reviewing and verifying a Publisher's compliance with Framework Policies. A Publisher will provide, without undue delay, any information reasonably requested by the MO to verify compliance.

2. The MO may suspend a Publisher from participation in the Framework for its failure to comply with Framework Policies until the Publisher comes into full compliance and demonstrates its intention and ability to remain so. The MO may block a Publisher from participation in the Framework for violations of Framework Policies that are willful and/or severe. The MO may enact a suspension or block of a Publisher by notifying CMPs that the Publisher is not in full compliance.

[1] This can be done by comparing current vs prior version of the GVL and then comparing to the Publisher's list.

Copyright © 2021 IAB Canada. All rights reserved.

3. Additionally, the MO may, at its discretion and according to MO procedures, take additional actions in response to a Publisher's non-compliance, including publicly communicating the Publisher's non-compliance and reporting the non-compliance to data protection authorities.

Chapter V: Interacting with Users

1. Chapter II (Policies for CMPs), Chapter IV (Policies for Publishers), Appendix A (Purposes and Features Definitions), and Appendix B (User Interface Requirements) set out requirements for interacting with users. CMPs and/or Publishers are responsible for interacting with users in accordance with these Policies and the Specifications.

Copyright © 2021 IAB Canada. All rights reserved.

Appendix A: Purposes and Features Definitions

A. Purposes

Purpose 2 - Select basic ads

Number	2
Name	Select basic ads
Legal text	To select basic ads vendors can: ● Use real-time information about the context in which the ad will be shown, to show the ad, including information about the content and the device, such as: device type and capabilities, user agent, URL, IP address ● Use a user's non-precise geolocation data ● Control the frequency of ads shown to a user ● Sequence the order in which ads are shown to a user ● Prevent an ad from serving in an unsuitable editorial (brand-unsafe) context Vendors cannot: ● Create a personalized ads profile using this information for the selection of future ads without a separate Permission to create a personalized ads profile. N.B. Non-precise means only an approximate location involving *at least* a radius of 500 meters is permitted.
User-friendly text	Ads can be shown to you based on the content you're viewing, the app you're using, your approximate location, or your device type.
Vendor guidance	● Vendors cannot: ● Create an advertising profile about a user (including a user's prior activity, interests, visits to sites or apps, location, or demographic information) without having obtained consent or met requirements for collecting, using, or disclosing the user's personal information under a legitimate interest for Purpose 3. ● Use an advertising profile to select future ads about a user (including a user's prior activity, interests, visits to sites or apps, location, or

Copyright © 2021 IAB Canada. All rights reserved.

	demographic information) without having obtained consent or met requirements for collecting, using, or disclosing the user's personal information under a legitimate interest for Purpose 4. ● Selection and delivery of an ad based on real-time data (e.g. information about the page content, app type, device type and capabilities, user agent, URL, IP address etc.) ● Real time data, as referenced above, may be used for positive or negative targeting ● *Note*: This purpose allows collection, use, or disclosure of non-precise geolocation data to select and deliver an ad. However, collecting, using, or disclosing precise geolocation data for this purpose requires the user's opt-in (i.e. express consent) to Special Feature 1 in addition to having obtained consent or met requirements for collecting, using, or disclosing under a legitimate interest for this Purpose. ● [with Feature 1] Combine data obtained offline with data available in the moment, about the user, to select an ad. ● [with Feature 2] Link different devices in order to select an ad. ● [with Feature 3] Identify a device by receiving and using automatically sent device characteristics in order to select an ad in the moment. ● [with opt-in for Special Feature 1] Use precise geolocation data to select and deliver an ad in the moment, without storing it. ● [with opt-in for Special Feature 2] Identify a device by actively scanning device characteristics in order to select an ad in the moment.

Purpose 3 - Create a personalized ads profile

Number	3
Name	Create a personalized ads profile
Legal text	To create a personalized ads profile vendors can: ● Collect information about a user, including a user's activity, interests, visits to sites or apps, demographic information, or location, to create or edit a user profile for use in personalized advertising. ● Combine this information with other information previously collected, including from across websites and apps, to create or edit a user profile for use in personalized advertising.

Copyright © 2021 IAB Canada. All rights reserved.

User-friendly text	A profile can be built about you and your interests to show you personalized ads that are relevant to you.
Vendor guidance	● Associate data collected, including information about the content and the device, such as: device type and capabilities, user agent, URL, IP address with a new or existing ad profile based on user interests or personal characteristics of the user. ● When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate Permission. ● Establish retargeting criteria ● Establish negative targeting criteria ● For offline data collection, a Permission for Purpose 3 (Create a personalized profile) needs to be achieved out of band - the TCF signal will take precedence for collection of data online (see Policies) ● Feature 2: Collecting data for deterministic cross-device mapping (e.g. if a user logs into an account on one device and then on another) may be done on the basis of an out of band Permission ● Keeping track of ad frequency and ad sequence may be done on the basis of Purpose 2, and do not require Purpose 3. ● Other purposes, including ad measurement, are not included in this purpose ● If a vendor uses a shared profile for personalized ads and personalized content, the vendor should only create and/or update that profile with the appropriate established Permissions for both Purpose 3 and 5. ● [with Feature 1] Associate data obtained offline with an online user to create or edit a user profile for use in advertising. ● [with Feature 2] Store a user identifier, obtained by actively scanning device characteristics, in a profile for use in advertising. ● [with Feature 3] Associate an identifier obtained by receiving and using automatically sent device characteristics, with a profile for use in advertising ● [with opt-in for Special Feature 1] Select a personalized ad, based on a personalized ads profile, by collecting, using, or disclosing precise geolocation previously stored or made available in the moment. ● [with opt-in for Special Feature 2] Associate an identifier obtained by actively scanning device characteristics with a profile for use in advertising

Copyright © 2021 IAB Canada. All rights reserved.

Purpose 4 - Select personalized ads

Number	4
Name	Select personalized ads
Legal text	To select personalized ads vendors can: ● Select personalized ads based on a user profile or other historical user data, including a user's prior activity, interests, visits to sites or apps, location, or demographic information.
User-friendly text	Personalized ads can be shown to you based on a profile about you.
Vendor guidance	● Requires having obtained consent or met requirements for collecting, using, or disclosing under a legitimate interest for Purpose 2 (Basic ads) to be used ● This purpose is intended to enable the following collection, use or disclosure activities: ○ Select ads based on a personalized ads profile ○ Select an ad based on retargeting criteria ○ Select an ad based on negative targeting criteria tied to a profile ○ Select dynamic creative based on an ad profile, or other historical information ● Selecting and/or ads based on ad frequency and ad sequence may be done on the basis of Purpose 2, and do not require Purpose 4. ● [with Feature 1] Select a personalized ad, based on a personalized ads profile, by matching and combining data obtained offline with the data stored in an online profile. ● [with Feature 2] Select a personalized ad, based on a personalized ads profile, by linking different devices. ● [with Feature 3] Select an ad based on a personalized profile associated with an identifier obtained by receiving and using automatically sent device characteristics ● [with opt-in for Special Feature 1] Select an ad based on precise geolocation previously stored ● [with opt-in for Special Feature 2] Select an ad based on a personalized profile associated with an identifier obtained by actively scanning device characteristics.

Copyright © 2021 IAB Canada. All rights reserved.

	• If you use a single profile for **both** personalized ads and personalized content, users will need to grant the appropriate Permissions for **both** purpose 4 and purpose 6.

Purpose 5 - Create a personalized content profile

Number	5
Name	Create a personalized content profile
Legal text	To create a personalized content profile vendors can: • Collect information about a user, including a user's activity, interests, visits to sites or apps, demographic information, or location, to create or edit a user profile for personalizing content. • Combine this information with other information previously collected, including from across websites and apps, to create or edit a user profile for use in personalizing content.
User-friendly text	A profile can be built about you and your interests to show you personalized content that is relevant to you.

Vendor guidance	• **Content** refers to non-advertising content. Creating a profile for advertising personalization, such as, paid cross-site content promotion and native advertising is *not* included in Purpose 5, but the corresponding ad-related Purpose 3
	• When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate Permission.
	• This purpose is intended to enable the following collection, use or disclosure activities:
	  ○ Associate data collected, including information about the content and the device, such as: device type and capabilities, user agent, URL, IP address with a new or existing content profile based on user interests or personal characteristics of the user. When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate Permission.
	  ○ Establish negative targeting criteria
	  ○ If a vendor uses a shared profile for personalized ads and personalized content, the vendor should only create and/or

Copyright © 2021 IAB Canada. All rights reserved.

	update that profile with the appropriate established Permissions for both purpose 3 and 5. ● [with Feature 1] Associate offline data with an online user to create or edit a user profile for use in content personalization ● [with Feature 2] Link different devices and store that data point in a profile for use in content personalization. ● [with Feature 3] Associate an identifier obtained by receiving and using automatically sent device characteristics, with a profile for use in content personalization ● [with opt-in for Special Feature 1] Store precise geolocation data in a profile for use in content personalization. ● [with opt-in for Special Feature 2] Associate an identifier obtained by actively scanning device characteristics with a profile for use in content personalization

Purpose 6 - Select personalized content

Number	6
Name	Select personalized content
Legal text	To select personalized content vendors can: ● Select personalized content based on a user profile or other historical user data, including a user's prior activity, interests, visits to sites or apps, location, or demographic information.
User-friendly text	Personalized content can be shown to you based on a profile about you.
Vendor guidance	● **Content** refers to non-advertising content. Personalizing advertising content, such as, paid cross-site content promotion and native advertising is *not* included in Purpose 6, but the corresponding ad-related Purpose 4. ● This purpose is intended to enable the following collection, use or disclosure activities: ○ Select content based on a personalized content profile ○ [with Feature 1] Select personalized content, based on a personalized content profile, by matching and combining data obtained offline with the data stored in an online profile. ○ [with Feature 2] Select personalized content, based on a personalized content profile, by linking different devices.

Copyright © 2021 IAB Canada. All rights reserved.

	○ [with Feature 3] Select personalized content based on a personalized profile associated with an identifier obtained by receiving and using automatically sent device characteristics ○ [with opt-in for Special Feature 1] Select personalized content, based on a content profile, by collecting, using, or disclosing precise geolocation previously stored or made available in the moment. ○ [with opt-in for Special Feature 2] Select personalized content, based on a personalized content profile by using an identifier obtained by actively scanning device characteristics. ○ If you use a single profile for **both** personalized ads and personalized content, users will need to grant the appropriate Permissions for **both** purpose 4 and purpose 6.

Purpose 7 - Measure ad performance

Number	7
Name	Measure ad performance
Legal text	To measure ad performance vendors can: ● Measure whether and how ads were delivered to and interacted with by a user ● Provide reporting about ads including their effectiveness and performance ● Provide reporting about users who interacted with ads using data observed during the course of the user's interaction with that ad ● Provide reporting to publishers about the ads displayed on their property ● Measure whether an ad is serving in a suitable editorial environment (brand-safe) context ● Determine the percentage of the ad that had the opportunity to be seen and the duration of that opportunity ● Combine this information with other information previously collected, including from across websites and apps Vendors cannot: ● Apply panel- or similarly derived audience insights data to ad measurement data without a separate Permission to apply market research to generate audience insights.

Copyright © 2021 IAB Canada. All rights reserved.

User-friendly text	The performance and effectiveness of ads that you see or interact with can be measured.
Vendor guidance	● This purpose is intended to enable the following collection, use or disclosure activities: ● Measure how brand suitable or safe the content of the digital property where the ad was served was ● Measure the percentage of the ad that had the opportunity to be seen and for how long ● Measure how many users engaged with an ad, for how long and what was the nature of that engagement (click, tap, hover, scroll etc.) ● Determine how many unique users or devices an ad was served to ● Measure the time when users saw the ad ● Measure/analyze the characteristics of the device the ad was served to (non-precise location, type of device, screen size, language of the device, operating system/browser, mobile carrier) ● Measure ad attribution, conversions, sales lift ● Data collected, used, or disclosed for ad measurement must not be used to improve individual profile or segment data for other purposes ● When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate Permission. ● This purpose permits reporting on an individual and aggregate level ● This purpose does not permit applying panel-derived demographic information to the measurement data unless the user has also granted the appropriate Permission for Purpose 9. ● [with Feature 1] Measure ad performance by matching and combining data obtained offline with the data obtained online. ● [with Feature 2] Measure ad performance by linking different devices. ● [with Feature 3] Measure ad performance by using an identifier obtained by receiving and using automatically sent device characteristics ● [with opt-in for Special Feature 1] Measure ad performance by collecting, using, or disclosing precise geolocation previously stored or made available in the moment. ● [with opt-in for Special Feature 2] Measure ad performance by using an identifier obtained by actively scanning device characteristics.

Purpose 8 - Measure content performance

Number	8

Copyright © 2021 IAB Canada. All rights reserved.

Name	Measure content performance
Legal text	To measure content performance vendors can: ● Measure and report on how content was delivered to and interacted with by users. ● Provide reporting, using directly measurable or known information about users who interacted with the content. ● Combine this information with other information previously collected, including from across websites and apps. Vendors cannot: ● Measure whether and how ads (including native ads) were delivered to and interacted with by a user without a separate Permission. ● Apply panel- or similarly derived audience insights data to ad measurement data without a separate Permissions to apply market research to generate audience insights.
User-friendly text	The performance and effectiveness of content that you see or interact with can be measured.
Vendor guidance	● **Content** refers to non-advertising content. Ad measurement should be conducted under Purpose 7. ● This purpose does not permit applying panel-derived demographic information to the measurement data, this requires Purpose 9. ● This purpose is intended to enable the following collection, use or disclosure activities: ○ Measure how many users engaged with content, for how long and what was the nature of that engagement (click, tap, hover, scroll etc.) ○ Determine how many unique users or devices content was served to ○ Measure the time when users saw content ○ Measure/analyze the characteristics of the device content was served to (non-precise location, type of device, screen size, language of the device, operating system/browser, mobile carrier) ○ Measure user referrals ● When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate Permission without an appropriate Permission for these purposes.

Copyright © 2021 IAB Canada. All rights reserved.

	● Data collected, used, or disclosed for measuring content must not be used to improve individual profiles and segment data for other purposes ● [with Feature 1] Measure content performance by matching and combining data obtained offline with the data obtained online. ● [with Feature 2] Measure content performance by linking different devices. ● [with Feature 3] Measure content performance by using an identifier obtained by receiving and using automatically sent device characteristics. ● [with opt-in for Special Feature 1] Measure content performance by collecting, using, or disclosing precise geolocation previously stored or made available in the moment. ● [with opt-in for Special Feature 2] Measure content performance by using an identifier obtained by actively scanning device characteristics.

Purpose 9 - Apply market research to generate audience insights

Number	9
Name	Apply market research to generate audience insights
Legal text	To apply market research to generate audience insights vendors can: ● Provide aggregate reporting to advertisers or their representatives about the audiences reached by their ads, through panel-based and similarly derived insights. ● Provide aggregate reporting to publishers about the audiences that were served or interacted with content and/or ads on their property by applying panel-based and similarly derived insights. ● Associate offline data with an online user for the purposes of market research to generate audience insights if vendors have declared to match and combine offline data sources ● Combine this information with other information previously collected, including from across websites and apps Vendors cannot: ● Measure the performance and effectiveness of ads that a specific user was served or interacted with, without a separate Permission to measure ad performance.

Copyright © 2021 IAB Canada. All rights reserved.

	• Measure which content a specific user was served and how they interacted with it, without a separate Permission to measure content performance.
User-friendly text	Market research can be used to learn more about the audiences who visit sites/apps and view ads.

Vendor guidance	• Unique Reach
	• Audience segmentation (Demographic attributes of the users)
	  ○ Website/Apps KPIs across ads and contents
	  ○ usually panel-derived:
	  ○ Age
	  ○ Gender
	  ○ interests / affinity / in-market categories: what else are users interested in
	• When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate Permission.
	• Data collected, used, or disclosed for audience measurement must not be used to improve individual profiles for Purposes 3 and 5 without an appropriate Permissions for these purposes
	• Audience Measurement reports include only aggregate data
	• Those are data related to market research and “currency” data e.g.: Syndicated data from JICs, Ad Audience certifications, etc.
	• Vendors cannot provide reporting about the audiences using methods covered in Purposes 7 and 8.
	• [with Feature 1] This purpose serves to match offline obtained data (panel data) to online obtained data (through Purpose 7 or 8).
	• [with Feature 2] Apply market research to generate audience insights by linking different devices.
	• [with Feature 3] Use identifiers generated by receiving and using automatically sent device characteristics.
	• [with opt-in for Special Feature 1] Use precise geolocation data to apply market research data in order to generate audience insights.
	• [with opt-in for Special Feature 2] Use identifiers generated by actively scanning device characteristics to apply market research data in order to generate audience data

Copyright © 2021 IAB Canada. All rights reserved.

	• This purpose does not permit applying measurement data to the panel-derived demographic information unless the user has also granted the appropriate Permission for Purpose 7.

Purpose 10 - Develop and improve products

Number	10
Name	Develop and improve products
Legal text	To develop new products and improve products vendors can: • Use information to improve their existing products with new features and to develop new products • Create new models and algorithms through machine learning Vendors cannot: • Collect, use, or disclose any other personal information which is allowed under a different purpose for this purpose
User-friendly text	Your data can be used to improve existing systems and software, and to develop new products.
Vendor guidance	• You may only process information here for the explicit purpose of product improvement or new product development. • Do not collect, use or disclose any other personal information, such as improving individual user profiles, allowed under a different purpose under this purpose, unless you have Permission for this purpose. • [with Feature 1] Develop and improve products by matching and combining data obtained offline with the data obtained online. • [with Feature 2] Develop and improve products by linking different devices. • [with Feature 3] Develop and improve products by using an identifier obtained by receiving and using automatically sent device characteristics. • [with opt-in for Special Feature 1] Develop and improve products by collecting, using, or disclosing precise geolocation previously stored or made available in the moment.

Copyright © 2021 IAB Canada. All rights reserved.

	• [with opt-in for Special Feature 2] Develop and improve products by using an identifier obtained by actively scanning device characteristics.

B. Special Purposes

Special Purpose 1 - Ensure security, prevent fraud, and debug

Number	1
Name	Ensure security, prevent fraud, and debug
Legal text	To ensure security, prevent fraud and debug vendors can: ● Ensure data are securely transmitted ● Detect and prevent malicious, fraudulent, invalid, or illegal activity. ● Ensure correct and efficient collection, use, or disclosure operations of systems, including monitoring and enhancing the performance of systems and collection, use, or disclosure engaged in permitted purposes Vendors cannot: ● Collect, use, or disclose any other personal information which is allowed under a different purpose for this purpose. Note: Data collected and used to ensure security, prevent fraud, and debug may include automatically sent device characteristics for identification, precise geolocation data, and data obtained by actively scanning device characteristics for identification without separate disclosure and/or opt-in.
User-friendly text	Your data can be used to monitor for and prevent fraudulent activity, and ensure systems that collect, use or disclose your personal information work properly and securely.
Vendor guidance	• Special Purpose: No right-to-object to the collection, use, or disclosure via the Framework. • This purpose is to be used by 3rd parties operating on digital property, and it does not affect publishers' ability to run fraud checks outside of the TCF and independently. • This purpose is intended to enable collection, use, or disclosure activities such as:

Copyright © 2021 IAB Canada. All rights reserved.

	○ Monitoring, preventing ex and post ante: ■ General Invalid Traffic Detection and Blocking ■ Sophisticated Invalid Traffic Detection and Blocking • Automated Browsing, Dedicated Device • Automated Browsing, Non-Dedicated Device • Incentivized Human Activity • Manipulated Human activity • Falsified Measurement Events • Domain Misrepresentation • Hidden Ads ○ Process of identifying product errors - making products work (not improving them) ○ Ensuring operability of the system/platform

Special Purpose 2 - Technically deliver ads or content

Number	2
Name	Technically deliver ads or content
Legal text	To deliver information and respond to technical requests vendors can: ● Use a user's IP address to deliver an ad over the internet ● Respond to a user's interaction with an ad by sending the user to a landing page ● Use a user's IP address to deliver content over the internet ● Respond to a user's interaction with content by sending the user to a landing page ● Use information about the device type and capabilities for delivering ads or content, for example, to deliver the right size ad creative or video file in a format supported by the device Vendors cannot: ● Collect, use, or disclose any other personal information which is allowed under a different purpose for this purpose.
User-friendly text	Your device can receive and send information that allows you to see and interact with ads and content.
Vendor guidance	• Special Purpose: No right-to-object to the collection, use, or disclosure via the Framework.

Copyright © 2021 IAB Canada. All rights reserved.

	• This purpose covers both ads and content
	• This purpose is intended to enable the following collection, use or disclosure activities:
	  ○ Receiving and responding to ad requests
	  ○ Delivery of ad-files to an IP address
	  ○ Receiving and responding to content requests
	  ○ Delivery of content files to an IP address
	  ○ Logging that an ad was delivered, without recording any personal information about the user
	  ○ Logging that content was delivered, without recording any personal information about the user

C. Features

Feature 1 - Match and combine offline data sources

Number	1
Name	Match and combine offline data sources
Legal text	Vendors can: • Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.
User-friendly text	Data from offline data sources can be combined with your online activity in support of one or more purposes.
Vendor guidance	• Use offline data matching for one or more Purposes or Special Purposes, for which you have established appropriate Permissions. • As the TCF only works online, “appropriate Permissions” in the preceding bullet refers to Permissions established offline at the point of data collection.

Feature 2 - Link different devices

Number	2

Copyright © 2021 IAB Canada. All rights reserved.

Name	Link different devices
Legal text	Vendors can: ● Deterministically determine that two or more devices belong to the same user or household ● Probabilistically determine that two or more devices belong to the same user or household ● Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)
User-friendly text	Different devices can be determined as belonging to you or your household in support of one or more purposes.
Vendor guidance	● Use cross-device matching for one or more Purposes or Special Purposes, for which you have established appropriate Permissions.

Feature 3 - Receive and use automatically sent device characteristics for identification

Number	3
Name	Receive and use automatically sent device characteristics for identification
Legal text	Vendors can: ● Create an identifier using data collected automatically from a device for specific characteristics, e.g. IP address, user-agent string. ● Use such an identifier to attempt to re-identify a device. Vendors cannot: ● Create an identifier using data collected via actively scanning a device for specific characteristics, e.g. installed font or screen resolution without users' separate opt-in to actively scanning device characteristics for identification. ● Use such an identifier to re-identify a device.

Copyright © 2021 IAB Canada. All rights reserved.

User-friendly text	Your device might be distinguished from other devices based on information it automatically sends, such as IP address or browser type.
Vendor guidance	Use of this data for security or fraud prevention is separately covered by Special Purpose 1 and does not require separate declaration of this feature.

D. Special Features

Special Feature 1 - Use precise geolocation data

Number	1
Name	Use precise geolocation data
Legal text	Vendors can: • Collect and process precise geolocation data in support of one or more purposes. Note: Precise geolocation means that there are no restrictions on the precision of a user's location; this can be accurate to within several meters.
User-friendly text	Your precise geolocation data can be used in support of one or more purposes. This means your location can be accurate to within several meters.
Vendor guidance	• Users must opt IN to this feature before vendors may use it. • Use geolocation data with an accuracy of up to 500 meters and/or latitude and longitude data with more than two decimals for one or more Purposes or Special Purposes, for which you have established appropriate Permissions. • Any uses of precise geolocation for security & fraud fall under that purpose and do NOT require this feature. • The use of the special feature will depend on the context and the language of the purpose for which the Permissions has been established, and precise geolocation data is used in support of (e.g. precise geolocation data can be used only in the moment to select an ad in the context of Purpose 4 - Selection of personalized ads)

Copyright © 2021 IAB Canada. All rights reserved.

Special Feature 2 - Actively scan device characteristics for identification

Number	2
Name	Actively scan device characteristics for identification
Legal text	Vendors can: ● Create an identifier using data collected via actively scanning a device for specific characteristics, e.g. installed fonts or screen resolution. ● Use such an identifier to re-identify a device.
User-friendly text	Your device can be identified based on a scan of your device's unique combination of characteristics.
Vendor guidance	● Special feature: Users must opt IN to this feature before vendors may use it. ● Collect data about a user's browser or device to distinguish the user from other users across visits, using a combination of information accessed via JavaScript or APIs such as time zone, system fonts, screen resolution, and installed plugins. ● Not in scope: IP address, user agent; information that does not require access via JavaScript or API ● Any uses of active device characteristic scanning for security & fraud fall under that purpose and do NOT require this feature.

E. Stacks

Stacks may be used to substitute Initial Layer information about two or more Purposes and/or Special Features (also see Appendix B). Purposes must not be included in more than one Stack and must not be presented as part of a Stack and outside of Stacks at the same time. Conversely, any Stacks used must not include the same Purpose more than once, nor include Purposes presented separately from Stacks.

Copyright © 2021 IAB Canada. All rights reserved.

Stack 1 - Precise geolocation data, and identification through device scanning

Number	1
Name	Precise geolocation data, and identification through device scanning
Description	Precise geolocation and information about device characteristics can be used.
Special Features included	● Special Feature 1: Use precise geolocation data ● Special Feature 2: Actively scan device characteristics for identification

Stack 2 - Basic ads and ad measurement

Number	2
Name	Basic ads and ad measurement
Description	Basic ads can be served. Ad performance can be measured.
Purposes included	● Purpose 2: Select basic ads ● Purpose 7: Measure ad performance

Stack 3 - Personalized ads

Number	3
Name	Personalized ads
Description	Ads can be personalized based on a profile. More data can be added to better personalize ads.
Purposes included	● Purpose 2: Select basic ads ● Purpose 3: Create a personalized ads profile ● Purpose 4: Select personalized ads

Stack 4 - Basic ads, ad measurement, and audience insights

Number	4
Name	Basic ads, ad measurement, and audience insights
Description	Basic ads can be served. Ad performance can be measured. Insights about the audiences who saw the ads and content can be derived.

Copyright © 2021 IAB Canada. All rights reserved.

Purposes included	● Purpose 2: Select basic ads ● Purpose 7: Measure ad performance ● Purpose 9: Apply market research to generate audience insights

Stack 5 - Basic ads, personalized ads profile, and ad measurement

Number	5
Name	Basic ads, personalized ads profile, and ad measurement
Description	Basic ads can be served. More data can be added to better personalized ads. Ad performance can be measured.
Purposes included	● Purpose 2: Select basic ads ● Purpose 3: Create a personalized ads profile ● Purpose 7: Measure ad performance

Stack 6 - Personalized ads display and ad measurement

Number	6
Name	Personalized ads display and measurement
Description	Ads can be personalized based on a profile. Ad performance can be measured.
Purposes included	● Purpose 2: Select basic ads ● Purpose 4: Select personalized ads ● Purpose 7: Measure ad performance

Stack 7 - Personalized ads display, ad measurement, and audience insights

Number	7
Name	Personalized ads display, ad measurement, and audience insights
Description	Ads can be personalized based on a profile. Ad performance can be measured. Insights about the audiences who saw the ads and content can be derived.

Copyright © 2021 IAB Canada. All rights reserved.

Purposes included	● Purpose 2: Select basic ads ● Purpose 4: Select personalized ads ● Purpose 7: Measure ad performance ● Purpose 9: Apply market research to generate audience insights

Stack 8 - Personalized ads and ad measurement

Number	8
Name	Personalized ads and ad measurement
Description	Ads can be personalized based on a profile. More data can be added to better personalized ads. Ad performance can be measured.
Purposes included	● Purpose 2: Select basic ads ● Purpose 3: Create a personalized ads profile ● Purpose 4: Select personalized ads ● Purpose 7: Measure ad performance

Stack 9 - Personalized ads, ad measurement, and audience insights

Number	9
Name	Personalized ads, ad measurement, and audience insights
Description	Ads can be personalized based on a profile. More data can be added to better personalized ads. Ad performance can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 2: Select basic ads ● Purpose 3: Create a personalized ads profile ● Purpose 4: Select personalized ads ● Purpose 7: Measure ad performance ● Purpose 9: Apply market research to generate audience insights

Stack 10 - Personalized ads profile and display

Number	10
Name	Personalized ads profile and display

Copyright © 2021 IAB Canada. All rights reserved.

Description	Ads can be personalized based on a profile. More data can be added to better personalized ads.
Purposes included	● Purpose 3: Create a personalized ads profile ● Purpose 4: Select personalized ads

Stack 11 - Personalized content

Number	11
Name	Personalized content
Description	Content can be personalized based on a profile. More data can be added to better personalized content.
Purposes included	● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content

Stack 12 - Personalized content display and content measurement

Number	12
Name	Personalized content display and content measurement
Description	Content can be personalized based on a profile. Content performance can be measured.
Purposes included	● Purpose 6: Select personalized content ● Purpose 8: Measure content performance

Stack 13 - Personalized content display, content measurement and audience insights

Number	13
Name	Personalized content display, content measurement and audience insights
Description	Content can be personalized based on a profile. Content performance can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 6: Select personalized content ● Purpose 8: Measure content performance

Copyright © 2021 IAB Canada. All rights reserved.

	● Purpose 9: Apply market research to generate audience insights

Stack 14 - Personalized content and content measurement

Number	14
Name	Personalized content and content measurement
Description	Content can be personalized based on a profile. More data can be added to better personalized content. Content performance can be measured.
Purposes included	● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 8: Measure content performance

Stack 15 - Personalized content, content measurement and audience insights

Number	15
Name	Personalized content, content measurement and audience insights
Description	Content can be personalized based on a profile. More data can be added to better personalized content. Content performance can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights

Stack 16 - Personalized content, content measurement, audience insights, and product development.

Number	16
Name	Personalized content, content measurement, audience insights, and product development
Description	Content can be personalized based on a profile. More data can be added to better personalized content. Content performance can be measured. Insights about the audiences who saw the ads and content can be derived. Data can be used to build or improve user experience, systems, and software

Copyright © 2021 IAB Canada. All rights reserved.

Purposes included	● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights ● Purpose 10: Develop and improve products

Stack 17 - Ad and content measurement, and audience insights

Number	17
Name	Ad and content measurement, and audience insights
Description	Ad and content performance can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights

Stack 18 - Ad and content measurement

Number	18
Name	Ad and content measurement
Description	Ad and content performance can be measured.
Purposes included	● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance

Stack 19 - Ad measurement and audience insights

Number	19
Name	Ad measurement and audience insights
Description	Ad can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 7: Measure ad performance ● Purpose 9: Apply market research to generate audience insights

Copyright © 2021 IAB Canada. All rights reserved.

Stack 20 - Ad and content measurement, audience insights, and product development

Number	20
Name	Ad and content measurement, audience insights, and product development
Description	Ad and content performance can be measured. Insights about the audiences who saw the ads and content can be derived. Data can be used to build or improve user experience, systems, and software. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights ● Purpose 10: Develop and improve products

Stack 21 - Content measurement, audience insights, and product development

Number	21
Name	Content measurement, audience insights, and product development.
Description	Content performance can be measured. Insights about the audiences who saw the ads and content can be derived. Data can be used to build or improve user experience, systems, and software.
Purposes included	● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights ● Purpose 10: Develop and improve products

Stack 22 - Content measurement and product development

Number	22
Name	Content measurement and product development
Description	Content performance can be measured. Data can be used to build or improve user experience, systems, and software.
Purposes included	● Purpose 8: Measure content performance ● Purpose 10: Develop and improve products

Copyright © 2021 IAB Canada. All rights reserved.

Stack 23 - Personalized ads and content display, ad and content measurement

Number	23
Name	Personalized ads and content display, ad and content measurement
Description	Ads and content can be personalized based on a profile. Ad and content performance can be measured.
Purposes included	● Purpose 2: Select basic ads ● Purpose 4: Select personalized ads ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance

Stack 24 - Personalized ads and content display, ad and content measurement, and audience insights

Number	24
Name	Personalized ads and content display, ad and content measurement, and audien insights
Description	Ads and content can be personalized based on a profile. Ad and content performance can be measured. Insights about the audiences who saw the ads and content can be derived. Data can be used to build or improve user experience, systems, and software.
Purposes included	● Purpose 2: Select basic ads ● Purpose 4: Select personalized ads ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights

Stack 25 - Personalized ads and content, ad and content measurement

Number	25
Name	Personalized ads and content, ad and content measurement

Copyright © 2021 IAB Canada. All rights reserved.

Description	Ads and content can be personalized based on a profile. More data can be added to better personalized ads and content. Ad and content performance can be measured.
Purposes included	● Purpose 2: Select basic ads ● Purpose 3: Create a personalized ads profile ● Purpose 4: Select personalized ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance

Stack 26 - Personalized ads and content, ad and content measurement, and audience insights

Number	26
Name	Personalized ads and content, ad and content measurement, and audience insights
Description	Ads and content can be personalized based on a profile. More data can be added to better personalized ads and content. Ad and content performance can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 2: Select basic ads ● Purpose 3: Create a personalized ads profile ● Purpose 4: Select personalized ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights

Stack 27 - Personalized ads and content profile

Number	27
Name	Personalized ads and content profile

Copyright © 2021 IAB Canada. All rights reserved.

Description	More data can be added to personalize ads and content.
Purposes included	● Purpose 3: Create a personalized ads profile ● Purpose 5: Create a personalized content profile

Stack 28 - Personalized ads and content display

Number	28
Name	Personalized ads and content display
Description	Ads and content can be personalized based on a profile.
Purposes included	● Purpose 2: Select basic ads ● Purpose 4: Select personalized ads ● Purpose 6: Select personalized content

Stack 29 - Basic ads, ad and content measurement, and audience insights

Number	29
Name	Basic ads, ad and content measurement, and audience insights
Description	Basic ads can be served. Ad and content performance can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 2: Select basic ads ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights

Stack 30 - Personalized ads display, personalized content, ad and content measurement, and audience insights

Number	30
Name	Personalized ads display, personalized content, ad and content measurement, a audience insights
Description	Ads and content can be personalized based on a profile. More data can be added to better personalized content. Ad and content performance can be

Copyright © 2021 IAB Canada. All rights reserved.

	measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 2: Select basic ads ● Purpose 4: Select personalized ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights

Stack 31 - Personalized ads display, personalized content, ad and content measurement, audience insights, and product development

Number	31
Name	Personalized ads display, personalized content, ad and content measurement, audience insights, and product development
Description	Ads and content can be personalized based on a profile. More data can be added to better personalized content. Ad and content performance can be measured. Insights about the audiences who saw the ads and content can be derived. Data can be used to build or improve user experience, systems, and software.
Purposes included	● Purpose 2: Select basic ads ● Purpose 4: Select personalized ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights ● Purpose 10: Develop and improve products

Stack 32 - Basic ads, personalized content, ad and content measurement, and audience insights

Number	32
Name	**Basic ads, personalized content, ad and content measurement, and audience insights**

Copyright © 2021 IAB Canada. All rights reserved.

Description	Basic ads can be served. Content can be personalized based on a profile. More data can be added to better personalized content. Ad and content performance can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 2: Select basic ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights

Stack 33 - Basic ads, personalized content, ad and content measurement, audience insights, and product development

Number	33
Name	Basic ads, personalized content, ad and content measurement, audience insight and product development
Description	Basic ads can be served. Content can be personalized based on a profile. More data can be added to better personalized content. Ad and content performance can be measured. Insights about the audiences who saw the ads and content can be derived. Data can be used to build or improve user experience, systems, and software.
Purposes included	● Purpose 2: Select basic ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights ● Purpose 10: Develop and improve products

Stack 34 - Basic ads, personalized content, content measurement, and audience insights

Number	34
Name	Basic ads, personalized content, content measurement, and audience insights
Description	Basic ads can be served. Content can be personalized based on a profile. More data can be added to better personalized content. Ad and content

Copyright © 2021 IAB Canada. All rights reserved.

	performance can be measured. Insights about the audiences who saw the ads and content can be derived.
Purposes included	● Purpose 2: Select basic ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights

Stack 35 - Basic ads, personalized content, content measurement, audience insights, and product development

Number	35
Name	**Basic ads, personalized content, content measurement, audience insights, and product development**
Description	Basic ads can be served. Content can be personalized based on a profile. More data can be added to better personalized content. Content performance can be measured. Insights about the audiences who saw the ads and content can be derived. Data can be used to build or improve user experience, systems, and software.
Purposes included	● Purpose 2: Select basic ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 8: Measure content performance ● Purpose 9: Apply market research to generate audience insights ● Purpose 10: Develop and improve products

Stack 36 - Basic ads, personalized content, and ad measurement

Number	36
Name	Basic ads, personalized content, and ad measurement
Description	Basic ads can be served. Content can be personalized based on a profile. More data can be added to better personalized content. Ad performance can be measured.
Purposes	● Purpose 2: Select basic ads

Copyright © 2021 IAB Canada. All rights reserved.

included	● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance

Stack 37 - Basic ads, personalized content, ad measurement, and product development

Number	37
Name	Basic ads, personalized content, ad measurement, and product development
Description	Basic ads can be served. Content can be personalized based on a profile. More data can be added to better personalized content. Ad performance can be measured. Data can be used to build or improve user experience, systems, and software.
Purposes included	● Purpose 2: Select basic ads ● Purpose 5: Create a personalized content profile ● Purpose 6: Select personalized content ● Purpose 7: Measure ad performance ● Purpose 10: Develop and improve products

F. Example Stack Combinations

Example Stack Combination 1

- **Special Feature 1: Use precise geolocation data**
- **Stack 3: Personalized ads**
    - Purpose 2: Select basic ads
    - Purpose 3: Create a personalized ads profile
    - Purpose 4: Select personalized ads
- **Stack 11: Personalized content**
    - Purpose 5: Create a personalized content profile
    - Purpose 6: Select personalized content
- **Stack 17: Ad and content measurement, and audience insights**
    - Purpose 7: Measure ad performance
    - Purpose 8: Measure content performance
    - Purpose 9: Apply market research to generate audience insights
- **Purpose 10: Develop and improve products**

Copyright © 2021 IAB Canada. All rights reserved.

Example Stack Combination 2

- **Special Feature 1: Use precise geolocation data**
- **Stack 8:** Personalized ads, and ad measurement
    - Purpose 2: Select basic ads
    - Purpose 3: Create a personalized ads profile
    - Purpose 4: Select personalized ads
    - Purpose 7: Measure ad performance
- **Stack 14: Personalized content, and content measurement**
    - Purpose 5: Create a personalized content profile
    - Purpose 6: Select personalized content
    - Purpose 8: Measure content performance
- **Purpose 9:** Apply market research to generate audience insights
- **Purpose 10: Develop and improve products**

Example Stack Combination 3 (Advertisers)

- **Special Feature 1: Use precise geolocation data**
- **Stack 3: Personalized ads**
    - Purpose 2: Select basic ads
    - Purpose 3: Create a personalized ads profile
    - Purpose 4: Select personalized ads
- **Stack 19: Ad measurement, and audience insights**
    - Purpose 7: Measure ad performance
    - Purpose 9: Apply market research to generate audience insights
- **Purpose 10: Develop and improve products**

Copyright © 2021 IAB Canada. All rights reserved.

Appendix B: User Interface Requirements

A. Scope

a. This Appendix applies to any party deploying a user interface in connection with the Framework ("Framework UI"). Typically, this is the first party in the interaction with the user, such as a Publisher operating its own private CMP, or relying on the services of a commercial CMP. Both the Publisher and the CMP are responsible to ensure that these requirements are met. Appendix B should be read in conjunction with Chapter II (Policies for CMPs), Chapter IV (Policies for Publishers), and Chapter V (Policies for Interacting with Users).

b. A Publisher and/or CMP is responsible for determining when the Framework UI will be shown in accordance with the Framework Policies and the Specifications, consistent with legal requirements to support the transparent and lawful collection, use, or disclosure of users' personal information by Vendors. The Framework UI may be used to support the Publisher's own transparent and lawful collection, use, or disclosure of users' personal information.

c. The Framework Policies and the Specifications establish minimum requirements for language, design, and other elements in the Framework UI. These minimum requirements are intended to align with legal requirements of Canadian Privacy Law. In the event of a conflict between applicable Canadian law and Appendix B, the law prevails. Unless stated otherwise, nothing in Appendix B is intended to prevent the creation of Framework UIs that go beyond these minimum requirements.

B. General Rules and Requirements for Framework UIs

a. When providing transparency and/or consent choices to users, the Framework UI may make use of a so-called layered approach that provides key information immediately in an Initial Layer and makes more detailed information available elsewhere in additional layers for those users who are interested in it. Appendix B provides minimum requirements for certain layers, in particular the Initial Layer, where the Framework UI makes use of a layered approach.

b. When providing transparency about Purposes, Special Purposes, Features and Special Features, the Framework UI must do so only on the basis of the standard Purpose, Special Purpose, Feature, and Special Feature names and definitions of Appendix A as they are published on the Global Vendor List or using Stacks in accordance with the Policies and Specifications. UIs must make available the standard legal text of Purposes, Special Purposes, Features, and Special Features of Appendix A but may substitute or supplement the standard legal definitions with the standard user-friendly text of Appendix A so long as the legal text remains available to the user and it is explained that these legal texts are definitive. Either way, the language used must be user-friendly and generally understandable.

Copyright © 2021 IAB Canada. All rights reserved.

c. Where the Framework UI uses a language other than English, the Framework UI must do so only on the basis of official translations of the standard Purpose, Special Purpose, Feature and Special Feature names and definitions of Appendix A as they are published on the Global Vendor List.

d. When providing transparency about Vendors, the Framework UI must do so only on the basis of the information provided, and declarations made by Vendors as they are published on the Global Vendor List.

e. For the avoidance of doubt, Framework UIs may be used to also provide transparency, and request consent, for purposes and/or vendors, that are not covered by the Framework. However, users must not be misled to believe that any non-Framework purpose and/or vendor are part of the Framework or subject to its Policies. If the Framework UI includes non-Framework purposes and/or vendors the Framework UI must make it possible for users to distinguish between Vendors registered with the Framework, and Purposes defined by the Framework, and those who are not.

f. In cases in which the Publisher permits Vendors which it does not disclose directly, to collect, use, or disclose users' personal information for one or more Purposes, Special Purposes, and/or using one or more Special Features disclosed by the Publisher in line with a OOB Permissions and/or OOB opt-in established in previous interactions with those Vendors in other contexts, the Framework UI must inform users of the same.

g. The Framework UI must inform users that their Vendor choices are limited to Purposes and Special Features and that it does not enable them to refuse consent to disclosed Vendors collecting, using, or disclosing personal information for Special Purposes and that Special Features may be used for Special Purpose 1 (ensure security, prevent fraud, and debug) regardless of the user's choice about Special Features.

h. The Framework UI must inform users that their personal information may be stored outside of Canada and therefore the legislation of the jurisdiction it is stored in will apply. Users should also be notified of the risk in having their data stored outside of the Canadian jurisdiction.

C. Specific Requirements for Framework UIs in Connection with Requesting a User's Consent

a. When providing transparency about Purposes, Features and Vendors in connection with requesting a user's consent for the same, the Framework UI's must be displayed prominently and separately from other information, such as the general terms and conditions or the privacy policy, in a modal or banner that is clearly visible to a user first visiting a Digital Property.

b. When making use of a so-called layered approach, the Initial Layer of the Framework UI providing transparency and requesting a user's consent must include at least the following:

Copyright © 2021 IAB Canada. All rights reserved.

i. Must include information about the fact that personal information is collected, used, or disclosed, and the nature of the personal information that is collected, used, or disclosed (e.g. unique identifiers, browsing data);
ii. Must include information about the fact that third party Vendors will be collecting, using, or disclosing personal information of the user; and a link to the list of named third parties.
iii. Must include the list of the distinct and separate Purposes for which the Vendors are collecting, using, or disclosing personal information, using at least the standardised names and/or Stack names as defined in Appendix A;
iv. Must include information about the Special Features used by the Vendors when collection, using, or disclosing personal information;
v. Should include information about the consequences (if any) of consenting or not consenting (including withdrawing consent);
vi. Must include information about the scope of the Permission, i.e. global consent, service-specific consent, or group-specific consent. If group-specific consent, a link with information about the group.
vii. Must include information about the fact that the user can withdraw their Permission at any time, and how to resurface the Framework UI in order to do so;
viii. Must include a call to action for the user to express their objection if they choose to withhold Permission (for example “Advanced Settings”, “Customise Choices”, etc.)

c. When using a layered approach, if a user accesses a secondary layer which allows them to make granular and specific consent choices with respect to each Special Feature, the default choice must be “no consent”, “no opt-in” or “off”.

d. If a UI displays Vendors who are not registered with IAB Canada for participation in the Framework, the UI must make it possible for users to distinguish between Vendors registered with the Framework, and those who are not. The UI must not mislead others as to the Framework participation of any of the Vendors who are not registered with the MO.

e. A user must be able to resurface the Framework UI from an easily accessible link, such as a Privacy Policy or a separate icon available on the Publisher’s Digital Property as to allow them to withdraw their Permission as easily as it was to give it, notably by including a call to action for the user to withdraw their consent (for example “Withdraw consent”).

f. Calls to action in a Framework UI must not be invisible, illegible, or appear disabled. While calls to action do not need to be identical, to ensure they are clearly visible, they must have matching text treatment (font, font size, font style) and, for the text of each, a minimum contrast ratio of 5 to 1. To the extent that an Initial Layer has more than two calls to action, this policy only applies to the two primary calls to action.

Copyright © 2021 IAB Canada. All rights reserved.