# IAB Europe Transparency & Consent Framework Policies

- This document lays out the Policies applicable to participants in the IAB Europe 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 follow applicable privacy data protection laws. In the event of a conflict between applicable law and the Policies, the law prevails.

# Outline

# Appendix A: Purposes and Features Definitions

## A. Purposes

**Purpose 1 - Store and/or access information on a device**

**Purpose 2 - Select basic ads**

**Purpose 3 - Create a personalised ads profile**

**Purpose 4 - Select personalised ads**

**Purpose 5 - Create a personalised content profile**

**Purpose 6 - Select personalised 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 - Personalised ads**

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

**Stack 5 - Basic ads, personalised ads profile, and ad measurement**

**Stack 6 - Personalised ads display and ad measurement**

**Stack 7 - Personalised ads display, ad measurement, and audience insights**

**Stack 8 - Personalised ads and ad measurement**

**Stack 9 - Personalised ads, ad measurement, and audience insights**

**Stack 10 - Personalised ads profile and display**

**Stack 11 - Personalised content**

**Stack 12 - Personalised content display and content measurement**

**Stack 13 - Personalised content display, content measurement and audience insights**

**Stack 14 - Personalised content and content measurement**

**Stack 15 - Personalised content, content measurement and audience insights**

**Stack 16 - Personalised 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 - Personalised ads and content display, ad and content measurement**

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

**Stack 25 - Personalised ads and content, ad and content measurement**

**Stack 26 - Personalised ads and content, ad and content measurement, and audience insights**

**Stack 27 - Personalised ads and content profile**

**Stack 28 - Personalised ads and content display**

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

**Stack 30 - Personalised ads display, personalised content, ad and content measurement, and audience insights**

**Stack 31 - Personalised ads display, personalised content, ad and content measurement, audience insights, and product development**

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

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

**Stack 34 - Basic ads, personalised content, content measurement, and audience insights**

# 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 meet certain requirements of the ePrivacy Directive (and by extension its successor, the upcoming ePrivacy Regulation), and General Data Protection Regulation by providing a way of informing users about inter alia the storing and/or accessing of information on their devices, the fact that their personal data is processed, the purposes for which their personal data is processed, the companies that are seeking to process their personal data for these purposes, providing users with choice about the same, and signalling 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 standardisation of technology, for example of how information is disclosed or how user choices are stored and signalled to participants. It also requires standardising certain information provided to users, choices given to users, 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 processing of special categories of personal data, data relating to criminal convictions, or engaging in certain more strictly regulated processing activities, such as transferring personal data outside of the EU, or taking automated decisions, including profiling, that produce legal or similarly significant effects, for which the law requires meeting additional requirements such as obtaining explicit consent.

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

vi. The Framework is intended to be updated over time as legislation is updated (e.g. with the upcoming ePrivacy Regulation replacing the ePrivacy Directive), and legal requirements, regulatory practice, business practices, business needs and other relevant factors change.

# 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 the EU's General Data Protection Regulation ("GDPR") and ePrivacy Directive ("ePD") when processing personal data and/or accessing and/or storing information on a user's device.

2. "**Interactive Advertising Bureau Europe aisbl**" ("**IAB Europe**", the "**Managing Organization**", or the "**MO**") means the entity that manages and governs the Framework, including the Policies, Specifications, and the GVL. IAB Europe may update these Policies from time to time as it reasonably determines is necessary to ensure the ongoing success of the Framework.

3. "**Framework Policies**" (the "**Policies**") means this or any other official policy documentation disseminated by IAB Europe 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 Europe 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 Europe for participating in the Framework. The list is managed and maintained by IAB Europe, and is referenced by CMPs, Publishers and individual Vendors. Its structure and content shall be defined by the Specifications.

6. "**Transparency and Consent Management Platform**" ("**Consent Management Platform**", or "**CMP**") means the company or organisation that centralises and manages transparency for, and consent and objections of the end user. The CMP can read and update the Legal Basis 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 Legal Bases for processing, acquire user consent as needed and manage user objections, and communicate Legal Basis, consent or and/or objection status to the ecosystem. A CMP may be the party that surfaces, usually on behalf of the publisher, the UI to a user, though that may also be another party. CMPs may be private or commercial. A private CMP means a Publisher that implements

its own CMP for its own purposes. A commercial CMP offers CMP services to other parties. 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 processes personal data about end users visiting the Publisher's content and adheres to the Policies. A Vendor may be considered under the GDPR to be a Controller, a Processor, or both, depending on specific circumstances.

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 Legal Bases, including consent, are established with respect to Vendors that may process personal data 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 Legal Bases for GVL Vendors as part of their compliance with European privacy and data protection laws. 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 processing of data, including users' personal data, by participants in the Framework that are defined in the Policies or the Specifications for which Vendors declare a Legal Basis in the GVL and for which the user is given choice, i.e. to consent or to object depending on the Legal Basis for the processing, by a CMP.

13. "**Special Purpose**" means one of the defined purposes for processing of data, including users' personal data, by participants in the Framework that are defined in the Policies or the Specifications for which Vendors declare a Legal Basis in the GVL and for which the user is not given choice by a CMP.

14. "**Feature"** means one of the features of processing personal data 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.

15. "**Special Feature**" means one of the features of processing personal data 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 separately from the choice afforded regarding the Purposes which they support.

16. "**Stack**" means one of the combinations of Purposes and/or Special Features of processing personal data used 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, amongst others, information about the transparency, consent, and/or objection 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. "**Legal Basis**" means a lawful ground for processing defined in Article 6 GDPR and supported by the Framework, which are consent in accordance with Article 6(1)(a) GDPR and legitimate interests in accordance with Article 6(1)(f) GDPR. Legal Bases in the Framework can be established with

(a) Service-specific scope, which means a Legal Basis is applicable only on the service, for example a Publisher website or app, on which the Legal Basis is obtained and managed;
(b) Group-specific scope, which means a Legal Basis is applicable only on a pre-defined group of services, for example 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 Legal Bases established for the group across all the services of the group;
(c) Global scope, which means a Legal Basis is not only applicable on the service, on which the Legal Basis 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 Legal Bases across all such Publisher Digital Properties; or
(d) Out-of-band ("OOB"), which means a Legal Basis 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.

20. "**Device**" means electronic equipment, such as a computer, tablet, phone, TV, watch, that is capable of accessing the internet, including any software run on the electronic equipment to connect to the internet, such as a browser or app.

# Chapter II: Policies for CMPs

## 2. Applying and Registering

1. CMPs must apply to IAB Europe for participation in the Framework. IAB Europe 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 Europe that is required to fulfil IAB Europe's CMP application and approval procedures.

3. IAB Europe shall not approve a CMP's application unless or until IAB Europe 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 Europe Transparency & Consent Framework; (ii) an affirmation of its compliance with the Policies and Specifications of the Transparency & Consent Framework; (ii) the IAB Europe-assigned ID of the CMP. Example:

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

## 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 to 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 Legal Bases, as declared, and update Vendors' GVL information, including Legal Bases 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 Legal Bases except according to and as provided for under the Specifications, and using the standard API.

# 5. Managing Purposes and Legal Bases

1. A CMP will remind the user of their right to withdraw consent and/or the right to object to processing 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 it (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 in accordance with the law.

4. A CMP must only generate a positive legitimate interest Signal on the basis of the provision of transparency by the CMP about processing on the basis of a legitimate interest and must always generate a negative legitimate interest Signal if the user has indicated an objection to such processing on the basis of a legitimate interest.

5. A CMP must only generate a positive opt-in Signal for Special Features 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.

6. A CMP will establish Legal Bases 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.

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 Legal Bases.

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 Legal Bases and/or opt-ins 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 Legal Bases (that is, Legal Bases for data processing performed by the Publisher), including Legal Bases for purposes that are not supported by the Framework. A CMP is prohibited from implementing Publisher-specific custom Legal Bases Signals for Purposes that the Framework covers, or for any vendors rather than purposes. Management of Legal Bases 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 Legal Bases Signals in conjunction with the Publisher's own processing or for processing conducted on its behalf by a Vendor who is acting as a processor under the 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 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 Europe as participating in the Framework and 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 sites or apps.

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 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 has reasonably believes that a Vendor is not in compliance with the Specifications and/or the Policies, it must promptly notify IAB Europe 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 customise aspects that may impact compliance, the Publisher using such customisation 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 Europe 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 willfull 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 consent, as required under the Policies and/or the Specifications, 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.

# 9. Accountability

1. IAB Europe 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 Europe to verify compliance.

2. IAB Europe 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 Europe 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 data protection authorities.

# Chapter III: Policies for Vendors

## 10. Applying and Registering

1. Vendors must apply to IAB Europe for participation in the Framework. IAB Europe 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 collects and processes personal data, the Legal Bases it relies on for processing personal data toward each Purpose and Special Purpose, the Features and Special Features it relies on in pursuit of such Purposes and Special Purposes, and its requirements regarding storing and/or accessing information on users' devices. It will ensure its Purposes, Legal Bases, and access of a user's device, are completely and accurately included in the GVL. It will notify the MO of any changes in a timely manner.

## 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 Europe Transparency & Consent Framework; (ii) compliance with the Policies and Specifications with the Transparency & Consent Framework; (ii) the IAB Europe assigned ID that the Vendor uses. Example:

> *<Organisation> participates in the IAB Europe Transparency & Consent Framework and complies with its Specifications and Policies. <Organisation>'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 Europe, 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 Europe 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 store and/or access information on a device, or to process personal data 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 store and/or access information on a device, or to process personal data for any Purpose and/or Special Purpose.

5. If a Vendor is unable to act in accordance with the contents of a received Signal, the Vendor must not store and/or access information on a device, or process personal data 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.

7. A Vendor must not obtain a Signal from a CMP except according to and as provided for under the Specifications and using the API. For the avoidance of doubt, this shall not preclude sending a Signal that has been properly obtained using the API between Vendors in accordance with the 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 Europe 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 personal data processing or the storing and/or accessing of information on user devices, to ensure compliance with the Specifications, and/or the Policies. In particular, the requirement to not process personal data prior to verifiably establishing a Legal Basis for processing personal data as communicated by the appropriate Signal in accordance with the Policies and Specifications, and not storing and/or accessing information on a user's device that is not exempted from the obligation to obtain consent, prior to verifiablyhaving obtained consent as communicated by the appropriate Signal in accord 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 personal data processing or the storing and/or accessing of information on user devices, if the Vendor-partner has provided updated software for the purpose of complying with the Specifications and/or the Policies.

# 15. Record Keeping

1. A Vendor must maintain records of consent, as required under the Policies and the Specifications, and will provide the MO access to such records upon request without undue delay.

2. A Vendor must maintain records of user identification, timestamps, and received Signals for the full duration of the relevant processing. A Vendor may maintain such records of user identification, timestamps, and Signals beyond the duration of the processing as required to comply with legal obligations or to reasonably defend or pursue legal claims, and/or for other processing allowed by law, under a valid legal basis, and consistent with the purposes for which the data was collected.

# 16. Purposes, Special Purposes and Legal Bases, Special Features and Opt-Ins

1. A Vendor must not store information or access information on a user's device without consent, unless the law exempts such storage of information or accessing of information on a user's device from an obligation to obtain consent.

2. A Vendor shall indicate on the global vendor list if it seeks consent for storing information or accessing information on a user's device where such consent is necessary. A Vendor must not store information or access information on a user's device without consent where such consent is necessary.

*2bis. A Vendor shall indicate on the GVL the maximum duration of information stored on a user's device and may, in addition, provide more detailed and purpose-specific storage and access information in accordance with the Specifications. Where a situation falls within the Framework, and to the extent that the maximum storage duration indicated on the GVL is not indefinite a Vendor must not refresh the maximum storage duration, unless the Framework signals indicate that the user has renewed their consent.*

3. A Vendor must not process personal data relating to a user without a Legal Basis to do so.

4. A Vendor shall indicate on the Global Vendor List:

(a) that it seeks to establish one of the Legal Bases available under the Framework for processing toward a Purpose;

(b) the Legal Basis or Legal Bases it seeks to establish for processing toward a Purpose, specifically whether it wishes to rely on:

i. consent as its sole legal base
ii. legitimate interest as its sole legal base
iii. consent or legitimate interest as its Legal Bases, selected in accordance with the Policy and Specifications

(c) the default Legal Basis to be used by CMPs where the Vendor declares two possible Legal Bases under Policy 4(b)(iii).

5. A Vendor shall indicate on the Global Vendor List that it seeks to establish a legitimate interest for processing toward a Special Purpose.

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

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

8. Where a situation falls within the Framework, in addition to complying with relevant data protection laws, a Vendor wishing to rely on the user's consent for the processing of his or her personal data will only do so if it can verify by way of the appropriate Signal in accord with the Specifications and Policies that the user has given his or her appropriate consent for the storing and/or accessing of information on a user's device and/or processing of his or her personal data before any information is stored and/or accessed on the user's device or any personal data is processed.

9. Where a situation falls within the Framework, in addition to complying with relevant data protection laws, a Vendor wishing to rely on its legitimate interest for the processing of personal data will only do so if:

(a) it can verify by way of the appropriate Signal in accord with the Specifications and Policies that the appropriate information has been provided to the user at the time that the processing of his or her personal data starts.

(b) the user has not exercised his or her right to object to such processing as indicated in the appropriate Signal in accord with the Policies and the Specifications.

10. Where a situation falls within the Framework, in addition to complying with relevant data protection laws, a Vendor wishing to make use of a Feature will only do so if it has indicated on the Global Vendor List its use of the Features it wishes to rely on in support of one or more Purposes and/or Special Purposes.

11. By way of derogation of Policy 16(10), a Vendor may receive and use automatically-sent device characteristics for identification without having indicated on the Global Vendor List its use of the Feature to receive and use automatically-sent device characteristics for identification to:

(a) process 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 data protection law;
    (ii) the Vendor has conducted a data protection impact assessment for the processing of identifiers obtained through automatically-sent device characteristics for identification collected and/or processed under this derogation;
    (iii) the Vendor actively minimises collection and/or processing of identifiers obtained through automatically-sent device characteristics for identification collected and/or processed under this derogation;
    (iv) the Vendor puts in place reasonable retention periods for the identifiers obtained through automatically-sent device characteristics for identification collected and/or processed under this derogation;

(v) the Vendor only retains the identifiers obtained through automatically-sent device characteristics for identification collected and/or processed 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 automatically-sent device characteristics for identification collected and/or processed under this derogation as soon as possible; and

(vii) the data associated with identifiers obtained through automatically-sent device characteristics for identification collected and/or processed under this derogation is never used for any other Purposes and/or Special Purposes. The prohibition of change of purpose of the processing 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 Global Vendor List 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.

12. Where a situation falls within the Framework, in addition to complying with relevant data protection laws, 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 accord 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.

13. By way of derogation of Policy 16(12), a Vendor may process Precise Geolocation Data without the opt-in of the user to the Special Feature of using Precise Geolocation Data to:

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

(c) process the Precise Geolocation Data for the Special Purpose of ensuring security, preventing fraud, and debugging , provided that

(i) the Vendor complies with relevant data protection law;

(ii) the Vendor has conducted a data protection impact assessment for the processing of Precise Geolocation Data collected and/or processed under this derogation;

(iii) The Vendor actively minimises collection and/or processing of Precise Geolocation Data collected and/or processed under this derogation;

(iv) the Vendor puts in place reasonable retention periods for the Precise Geolocation Data collected and/or processed under this derogation;

(v) only retains the Precise Geolocation Data collected and/or processed 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 and/or processed under this derogation as soon as possible; and
(vii) the Precise Geolocation Data collected and/or processed under this derogation is never used for any other Purposes and/or Special Purposes. The prohibition of change of purpose of the processing of Precise Geolocation Data collected under this derogation is absolute, and, for example, also precludes changing Purpose with the explicit consent of the user.

14. By way of derogation of Policy 16(12), 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) process 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 data protection law;
(ii) the Vendor has conducted a data protection impact assessment for the processing of identifiers obtained through actively scanning device characteristics for identification collected and/or processed under this derogation;
(iii) the Vendor actively minimises collection and/or processing of identifiers obtained through actively scanning device characteristics for identification collected and/or processed under this derogation;
(iv) the Vendor puts in place reasonable retention periods for the identifiers obtained through actively scanning device characteristics for identification collected and/or processed under this derogation;
(v) only retains the identifiers obtained through actively scanning device characteristics for identification collected and/or processed 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 and/or processed under this derogation as soon as possible;
(vii) the Vendor identifiers obtained through actively scanning device characteristics for identification collected and/or processed 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 processing 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.

15. By way of derogation of Policy 16(8) to 16(10), and Policy 16(12), Vendors may establish legal bases for processing personal data for one or more Purposes and/or Special Purposes outside of the Framework, or establish opt-ins for making use of Special Features outside of the Framework, for processing of personal data in association with a user's visit to a Publisher that participates in the Framework, so long as the OOB legal bases for processing personal data 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 processing. Use within the Framework of such OOB legal bases and/or opt-ins established outside of the Framework is subject to Policy 16(16).

16. Where a situation falls within the Framework, a Vendor must not process personal data for any Purpose and/or Special Purpose in reliance on legal bases established outside of the Framework, nor make use of Special Features in reliance on opt-ins established outside of the Framework, for any processing 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 Legal Bases;
(b) the Publisher informs users of the possibility that Vendors whom the Publisher does not disclose directly may process their personal data for one or more Purposes, Special Purposes, and/or use one or more Special Features disclosed by the Publisher in line with a OOB legal basis 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, by having been notified of the Vendor's processing under a legitimate interest, and/or objecting to processing under a legitimate interest, and the Vendor does not process any data on the basis of a OOB legal basis for any
    (i) Purpose for which the user has objected to processing under a legitimate interest, and/or 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;
(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(16)(a)-(c) for relying on OOB legal bases are met; and
(e) the Vendor is able to demonstrate that it has established a legal basis outside of the Framework for use in the Framework by keeping appropriate records other than a mere contractual obligation requiring a third party to organise valid legal bases on its behalf, and will make such records available to the MO without undue delay upon request.

17. A Vendor must not transmit personal data to another Vendor unless the Framework's Signals show that the receiving Vendor has a Legal Basis for the processing of the personal data. 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 data to another Vendor if it can verify by way of the appropriate Signal in accord with the Specifications and Policies that the receiving Vendor may process personal data on the basis of a Legal Basis established outside of the Framework under Policy 16(15) and 16(16), and it has a justified basis for relying on the recipient Vendor's having a Legal Basis for processing the personal data in question.

19. A Vendor must not transmit a user's personal data to an entity outside of the Framework unless it has a justified basis for relying on that entity's having a Legal Basis for processing the personal data in question.

20. If a Vendor receives a user's personal data without having a Legal Basis for the processing of that data, the Vendor must quickly cease processing the personal data and must not further transmit the personal data to any other party, even if that party has a Legal Basis for processing the personal data 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.

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 Europe Transparency & Consent Framework; (ii) an affirmation of its compliance with the Policies and Specifications with the Transparency & Consent Framework; (ii) the IAB Europe assigned ID of the CMP that the publisher uses. Example:

> *<Organisation> participates in the IAB Europe Transparency & Consent Framework and complies with its Specifications and Policies. <Organisation> [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 Legal Bases except according to and as provided for under the Specifications, and using the standard API.

# 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 Legal Bases within the Framework. A Publisher may further specify the individual Purposes for which it wishes to help establish Legal Bases 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, or instruct to Vendors which Legal Basis 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 by 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 data.

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 personal data processing or the storing and/or accessing of information on user devices, if the Vendor has provided updated software for the purpose of complying with the Specifications and/or the Policies.

# 23. Managing Purposes and Legal Bases

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, Legal Bases and/or opt-ins for the specific Purposes, Special Purposes, Features, and Special Features that Vendors claim, in accord 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 Legal Bases and/or opt-ins have been established for the respective Purposes, Special Features, and/or Vendors. For the avoidance of doubt: Special Purposes, and Features must always 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.**

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 Legal Bases before signalling that the Vendor's Legal Bases have been established.[1] It also means resurfacing the UI, for example, when a previously surfaced Vendor

[1] This can be done by comparing current vs prior version of the GVL.

claims a previously undisclosed Purpose or changes its declared Legal Basis for a previously disclosed Purpose before signalling that the Vendor's Legal Bases have been established.[2]

8. Publishers should remind users, or instruct their CMPs to do so, of their right to object to processing or 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 established a Vendor's Purposes and Legal Bases 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 accord with the Specifications that changes to the Framework are of such a nature as to require re-establishing Legal Bases.

11. A Publisher may use the Specification to manage and store, or instruct its CMP to do so, its own Legal Bases, including Legal Bases for purposes that are not supported by the Framework. A Publisher must not use Publisher-specific custom Legal Bases Signals to formally or informally agree signalling with any Vendor for Purposes that the Framework covers. Such management of Legal Bases 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 Legal Bases Signals in conjunction with its own processing or for processing conducted on its behalf by a Vendor who is acting as a processor under the law and only for purposes not standardized by the Framework.

# 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 wilful 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.

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.

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

# 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.

# Appendix A: Purposes and Features Definitions

## A. Purposes

### Purpose 1 - Store and/or access information on a device

| | |
|---|---|
| **Number** | 1 |
| **Name** | Store and/or access information on a device |
| **Legal text** | Vendors can:<br>● Store and access information on the device such as cookies and device identifiers for the purposes presented to a user. |
| **User-friendly text** | Cookies, device identifiers, or other information can be stored or accessed on your device for the purposes presented to you. |
| **Vendor guidance** | ● Allowable Lawful Basis: Consent.<br>● Purpose 1 is meant to signal whether the condition for lawful storing and/or accessing information on a user's device is met where this is required. It is not a purpose for personal data processing in itself, unlike all other Purposes the Framework covers. Purpose 1 corresponds to the obligation of Article 5(3) of the ePrivacy Directive. While Purpose 1 is not a data processing purpose, is technically treated the same way for signalling purposes.<br>● Purpose 1 does not apply to processing identifiers or client information, etc. that is not accessed on a user device. For example, reading a device's IDFA falls within Purpose 1, however processing an IDFA outside of reading it from a device, e.g. when receiving it as part of information sent through an ad request is not covered by Purpose 1.<br>● If information stored or accessed falls within the information covered by Special Feature 2 or Feature 3, Vendors must make sure to adhere to the opt in requirement of Special Feature 2 and the disclosure requirement of Feature 3 respectively in addition to the consent requirement of Purpose 1.<br>● Controllers may register for Purpose 1 only in conjunction with another Purpose, Feature, Special Purpose, and/or Special Feature. Any personal data stored and/or accessed via Purpose 1 still requires another Purpose to actually be processed. For example, |

| | |
|---|---|
| | reading a user identifier from a stored cookie cannot be used to create a personalised ads profile without having obtained consent or met requirements for processing under a legitimate interest for the Purpose 3.<br>● Personal data stored and/or accessed via Purpose 1 may not require another Purpose to be processed where a Vendor is acting as a data processor for purposes for which the data controller responsible for the processing has established a legal basis. In such cases, processors of Vendors on the GVL or publishers using the Publisher TC String should only process data in accordance with the Signals of their controller. |

## Purpose 2 - Select basic ads

| | |
|---|---|
| **Number** | 2 |
| **Name** | Select basic ads |
| **Legal text** | To select basic ads vendors can:<br>● 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<br>● Use a user's non-precise geolocation data<br>● Control the frequency of ads shown to a user.<br>● Sequence the order in which ads are shown to a user.<br>● Prevent an ad from serving in an unsuitable editorial (brand-unsafe) context<br>Vendors cannot:<br>● Create a personalised ads profile using this information for the selection of future ads without a separate legal basis to create a personalised ads profile.<br>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** | ● Allowable Lawful Bases: Consent, Legitimate Interests |

| | |
|---|---|
| **guidance** | ● Vendors cannot:<br>● 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 processing under a legitimate interest for Purpose 3.<br>● 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 demographic information) without having obtained consent or met requirements for processing under a legitimate interest for Purpose 4.<br>● 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.)<br>● Real time data, as referenced above, may be used for positive or negative targeting<br>● *Note*: This purpose allows processing of non-precise geolocation data to select and deliver an ad. However, processing precise geolocation data for this purpose requires the user's opt-in to Special Feature 1 in addition to having obtained consent or met requirements for processing under a legitimate interest for this Purpose.<br>● [with Feature 1] Combine data obtained offline with data available in the moment, about the user, to select an ad.<br>● [with Feature 2] Link different devices in order to select an ad.<br>● [with Feature 3] Identify a device by receiving and using automatically sent device characteristics in order to select an ad in the moment.<br>● [with opt-in for Special Feature 1] Use precise geolocation data to select and deliver an ad in the moment, without storing it.<br>● [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 personalised ads profile

| | |
|---|---|
| **Number** | 3 |
| **Name** | Create a personalised ads profile |
| **Legal text** | To create a personalised 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 personalised advertising.<br>● Combine this information with other information previously collected, including from across websites and apps, to create or edit a user profile for use in personalised advertising. |
| **User-friendly text** | A profile can be built about you and your interests to show you personalised ads that are relevant to you. |
| **Vendor guidance** | ● Allowable Lawful Bases: Consent, Legitimate Interests<br>● 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.<br>● When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis.<br>● Establish retargeting criteria<br>● Establish negative targeting criteria<br>● For offline data collection, a legal basis for Purpose 3 (Create a personalised profile) needs to be achieved out of band - the TCF signal will take precedence for collection of data online (see Policies)<br>● 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 legal basis<br>● Keeping track of ad frequency and ad sequence may be done on the basis of Purpose 2, and do not require Purpose 3.<br>● Other purposes, including ad measurement, are not included in this purpose<br>● If a vendor uses a shared profile for personalised ads and personalised content, the vendor should only create and/or update that profile with the appropriate established legal bases for both Purpose 3 and 5.<br>● [with Feature 1] Associate data obtained offline with an online user to create or edit a user profile for use in advertising.<br>● [with Feature 2] Store a user identifier, obtained by actively scanning device characteristics, in a profile for use in advertising.<br>● [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 personalised ad, based on a personalised ads profile, by processing precise geolocation previously stored or made available in the moment.<br>● [with opt-in for Special Feature 2] Associate an identifier obtained by actively scanning device characteristics with a profile for use in advertising |

## Purpose 4 - Select personalised ads

| | |
|---|---|
| **Number** | 4 |
| **Name** | Select personalised ads |
| **Legal text** | To select personalised ads vendors can:<br>● Select personalised 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** | Personalised ads can be shown to you based on a profile about you. |
| **Vendor guidance** | ● Allowable Lawful Bases: Consent, Legitimate Interests<br>● Requires having obtained consent or met requirements for processing under a legitimate interest for Purpose 2 (Basic ads) to be used<br>● This purpose is intended to enable these processing activities:<br>○ Select ads based on a personalised ads profile<br>○ Select an ad based on retargeting criteria<br>○ Select an ad based on negative targeting criteria tied to a profile<br>○ Select dynamic creative based on an ad profile, or other historical information<br>● 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.<br>● [with Feature 1] Select a personalised ad, based on a personalised ads profile, by matching and combining data obtained offline with the data stored in an online profile.<br>● [with Feature 2] Select a personalised ad, based on a personalised ads profile, by linking different devices. |

| | |
|---|---|
| | ● [with Feature 3] Select an ad based on a personalised profile associated with an identifier obtained by receiving and using automatically sent device characteristics<br>● [with opt-in for Special Feature 1] Select an ad based on precise geolocation previously stored<br>● [with opt-in for Special Feature 2] Select an ad based on a personalised profile associated with an identifier obtained by actively scanning device characteristics.<br>● If you use a single profile for **both** personalised ads and personalised content, users will need to grant the appropriate legal bases for **both** purpose 4 and purpose 6. |

## Purpose 5 - Create a personalised content profile

| | |
|---|---|
| **Number** | 5 |
| **Name** | Create a personalised content profile |
| **Legal text** | To create a personalised content profile vendors can:<br>● 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 personalising content.<br>● Combine this information with other information previously collected, including from across websites and apps, to create or edit a user profile for use in personalising content. |
| **User-friendly text** | A profile can be built about you and your interests to show you personalised content that is relevant to you. |
| **Vendor guidance** | ● Allowable Lawful Bases: Consent, Legitimate Interests<br>● **Content** refers to non-advertising content. Creating a profile for advertising personalisation, such as, paid cross-site content promotion and native advertising is *not* included in Purpose 5, but the corresponding ad-related Purpose 3<br>● When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis.<br>● This purpose is intended to enable these processing activities:<br>○ Associate data collected, including information about the content and the device, such as: device type and capabilities, |

| | |
|---|---|
| | user When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis.agent, URL, IP address  with a new or existing content profile based on user interests or personal characteristics of the user<br>○ Establish negative targeting criteria<br>○ If a vendor uses a shared profile for personalised ads and personalised content, the vendor should only create and/or update that profile with the appropriate established legal bases for both purpose 3 and 5.<br>● [with Feature 1]  Associate offline data with an online user to create or edit a user profile for use in content personalisation<br>● [with Feature 2] Link different devices and store that data point in a profile for use in content personalisation.<br>● [with Feature 3] Associate an identifier obtained by receiving and using automatically sent device characteristics, with a profile for use in content personalisation<br>● [with opt-in for Special Feature 1] Store precise geolocation data in a profile for use in content personalisation.<br>● [with opt-in for Special Feature 2] Associate an identifier obtained by actively scanning device characteristics with a profile for use in content personalisation |

## Purpose 6 -  Select personalised content

| | |
|---|---|
| **Number** | 6 |
| **Name** | Select personalised content |
| **Legal text** | To select personalised content vendors can:<br>● Select personalised 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** | Personalised content can be shown to you based on a profile about you. |
| **Vendor guidance** | ● Allowable Lawful Bases: Consent, Legitimate Interests<br>● **Content** refers to non-advertising content. Personalising 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.<br>● This purpose is intended to enable these processing activities:<br>○ Select content based on a personalised content profile<br>○ [with Feature 1] Select personalised content, based on a personalised content profile, by matching and combining data obtained offline with the data stored in an online profile.<br>○ [with Feature 2] Select personalised content, based on a personalised content profile, by linking different devices.<br>○ [with Feature 3] Select personalised content based on a personalised profile associated with an identifier obtained by receiving and using automatically sent device characteristics<br>○ [with opt-in for Special Feature 1] Select personalised content, based on a content profile, by processing precise geolocation previously stored or made available in the moment.<br>○ [with opt-in for Special Feature 2] Select personalised content, based on a personalised content profile by using an identified obtained by actively scanning device characteristics.<br>○ If you use a single profile for **both** personalised ads and personalised content, users will need to grant the appropriate legal bases 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:<br>● Measure whether and how ads were delivered to and interacted with by a user<br>● Provide reporting about ads including their effectiveness and performance<br>● Provide reporting about users who interacted with ads using data observed during the course of the user's interaction with that ad<br>● Provide reporting to publishers about the ads displayed on their property<br>● 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<br>● Combine this information with other information previously collected, including from across websites and apps<br><br>Vendors cannot:<br><br>● Apply panel- or similarly-derived audience insights data to ad measurement data without a separate legal basis to apply market research to generate audience insights. |
| **User-friendly text** | The performance and effectiveness of ads that you see or interact with can be measured. |
| **Vendor guidance** | ● Allowable Lawful Bases: Consent, Legitimate Interests<br>● This purpose is intended to enable processing activities such as:<br>  ● Measure how brand suitable or safe the content of the digital property where the ad was served was<br>  ● Measure the percentage of the ad that had the opportunity to be seen and for how long<br>  ● Measure how many users engaged with an ad, for how long and what was the nature of that engagement (click, tap, hover, scroll etc.)<br>  ● Determine how many unique users or devices an ad was served to<br>  ● Measure the time when users saw the ad<br>  ● Measure/ analyse 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)<br>  ● Measure ad attribution, conversions, sales lift<br>  ● Data collected and/or processed for ad measurement must not be used to improve individual profile or segment data for other purposes<br>● When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis.<br>● This purpose permits reporting on an individual and aggregate level<br>● This purpose does not permit applying panel-derived demographic information to the measurement data unless the user has also granted the appropriate legal basis for Purpose 9.<br>● [with Feature 1] Measure ad performance by matching and combining data obtained offline with the data obtained online.<br>● [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<br>● [with opt-in for Special Feature 1] Measure ad performance by processing precise geolocation previously stored or made available in the moment.<br>● [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 |
| **Name** | Measure content performance |
| **Legal text** | To measure content performance vendors can:<br>● Measure and report on how content was delivered to and interacted with by users.<br>● Provide reporting, using directly measurable or known information,about users who interacted with the content.<br>● Combine this information with other information previously collected, including from across websites and apps.<br>Vendors cannot:<br>● Measure whether and how ads (including native ads) were delivered to and interacted with by a user without a separate legal basis.<br>● Apply panel- or similarly derived audience insights data to ad measurement data without a separate legal bases 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** | ● Allowable Lawful Bases: Consent, Legitimate Interests<br>● **Content** refers to non-advertising content. Ad measurement should be conducted under Purpose 7.<br>● This purpose does not permit applying panel-derived demographic information to the measurement data, this requires Purpose 9.<br>● This purpose is intended to enable processing activities such as: |

| | |
|---|---|
| | ○ Measure how many users engaged with content, for how long and what was the nature of that engagement (click, tap, hover, scroll etc.)<br>○ Determine how many unique users or devices content was served to<br>○ Measure the time when users saw content<br>○ Measure/ analyse 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)<br>○ Measure user referrals<br>● When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis without an appropriate legal basis for these purposes.<br>● Data collected and/or processed for measuring content must not be used to improve individual profiles and segment data for other purposes<br>● [with Feature 1] Measure content performance by matching and combining data obtained offline with the data obtained online.<br>● [with Feature 2] Measure content performance by linking different devices.<br>● [with Feature 3] Measure content performance by using an identifier obtained by receiving and using automatically sent device characteristics.<br>● [with opt-in for Special Feature 1] Measure content performance by processing precise geolocation previously stored or made available in the moment.<br>● [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.<br>● 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.<br>● 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<br>● Combine this information with other information previously collected, including from across websites and apps<br><br>Vendors cannot:<br>● Measure the performance and effectiveness of ads that a specific user was served or interacted with, without a separate legal basis to measure ad performance.<br>● Measure which content a specific user was served and how they interacted with it, without a separate legal basis 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** | ● Allowable Lawful Bases: Consent, Legitimate Interests<br>● Unique Reach<br>● Audience segmentation (Demographic attributes of the users)<br>○ Website/Apps KPIs across ads and contents<br>○ usually panel-derived:<br>○ Age<br>○ Gender<br>○ interests / affinity / in-market categories: what else are users interested in<br>● When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis.<br>● Data collected and/or processed for audience measurement must not be used to improve individual profiles for Purposes 3 and 5 without an appropriate legal bases for these purposes<br>● Audience Measurement reports include only aggregate data |

| | |
|---|---|
| | • Those are data related to market research and "currency" data eg.: Syndicated data from JICs, Ad Audience certifications, etc.<br>• Vendors cannot provide reporting about the audiences using methods covered in Purposes 7 and 8.<br>• [with Feature 1] This purpose serves to match offline obtained data (panel data) to online obtained data (through Purpose 7 or 8).<br>• [with Feature 2] Apply market research to generate audience insights by linking different devices.<br>• [with Feature 3] Use identifiers generated by receiving and using automatically sent device characteristics.<br>• [with opt-in for Special Feature 1] Use precise geolocation data to apply market research data in order to generate audience insights.<br>• [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<br>• This purpose does not permit applying measurement data to the panel-derived demographic information unless the user has also granted the appropriate legal basis 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:<br>• Use information to improve their existing products with new features and to develop new products<br>• Create new models and algorithms through machine learning<br>Vendors cannot:<br>• Conduct any other data processing operation allowed under a different purpose under this purpose |
| **User-friendly text** | Your data can be used to improve existing systems and software, and to develop new products. |

| | |
|---|---|
| **Vendor guidance** | • Allowable Lawful Bases: Consent, Legitimate Interests<br>• You may only process information here for the explicit purpose of product improvement or new product development.<br>• Do not conduct any other data processing operation, such as improving individual user profiles, allowed under a different purpose under this purpose - you must obtain a lawful basis for that purpose.<br>• [with Feature 1] Develop and improve products by matching and combining data obtained offline with the data obtained online.<br>• [with Feature 2] Develop and improve products by linking different devices.<br>• [with Feature 3] Develop and improve products by using an identifier obtained by receiving and using automatically sent device characteristics.<br>• [with opt-in for Special Feature 1] Develop and improve products by processing precise geolocation previously stored or made available in the moment.<br>• [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:<br>• Ensure data are securely transmitted<br>• Detect and prevent malicious, fraudulent, invalid, or illegal activity.<br>• Ensure correct and efficient operation of systems and processes, including to monitor and enhance the performance of systems and processes engaged in permitted purposes<br>Vendors cannot:<br>• Conduct any other data processing operation allowed under a different purpose under 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 and processes work properly and securely. |
| **Vendor guidance** | • Special Purpose: No right-to-object to processing under legitimate interests via the Framework.<br>• Allowable Lawful Bases: Legitimate Interests<br>• 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.<br>• This purpose is intended to enable processing activities such as:<br>  ○ Monitoring, preventing ex and post ante:<br>  ■ General Invalid Traffic Detection and Blocking<br>  ■ Sophisticated Invalid Traffic Detection and Blocking<br>  • Automated Browsing, Dedicated Device<br>  • Automated Browsing, Non-Dedicated Device<br>  • Incentivized Human Activity<br>  • Manipulated Human activity<br>  • Falsified Measurement Events<br>  • Domain Misrepresentation<br>  • Hidden Ads<br>  ○ Process of identifying product errors - making products work (not improving them)<br>  ○ 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:<br>• Use a user's IP address to deliver an ad over the internet<br>• Respond to a user's interaction with an ad by sending the user to a landing page<br>• 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<br>• 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<br>Vendors cannot:<br>• Conduct any other data processing operation allowed under a different purpose under 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 processing under legitimate interests via the Framework.<br>• Allowable Lawful Bases: Legitimate Interests<br>• This purpose covers both ads and content<br>• This purpose is intended to enable processing activities such as:<br>  ○ Receiving and responding to ad requests<br>  ○ Delivery of ad-files to an IP address<br>  ○ Receiving and responding to content requests<br>  ○ Delivery of content files to an IP address<br>  ○ Logging that an ad was delivered, without recording any personal data about the user<br>  ○ Logging that content was delivered, without recording any personal data 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 legal bases.<br>● As the TCF only works online, , “appropriate legal bases” in the preceding bullet refers to legal bases established offline at the point of data collection. |

## Feature 2 - Link different devices

| | |
|---|---|
| **Number** | 2 |
| **Name** | Link different devices |
| **Legal text** | Vendors can:<br>● Deterministically determine that two or more devices belong to the same user or household<br>● Probabilistically determine that two or more devices belong to the same user or household<br>● 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 of purposes. |
| **Vendor guidance** | ● Use cross-device matching for one or more Purposes or Special Purposes, for which you have established appropriate legal bases. |

## 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:<br>● Create an identifier using data collected automatically from a device for specific characteristics, e.g. IP address, user-agent string.<br>● Use such an identifier to attempt to re-identify a device.<br>Vendors cannot:<br>● 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.<br>● Use such an identifier to re-identify a device. |
| **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:<br>● Collect and process precise geolocation data in support of one or more purposes.<br><br>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.<br>• 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 legal bases.<br>• Any uses of precise geolocation for security & fraud fall under that purpose and do NOT require this feature.<br>• The use of the special feature will depend on the context and the language of the purpose for which the legal bases 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 personalised ads) |

## Special Feature 2 - Actively scan device characteristics for identification

| | |
|---|---|
| **Number** | 2 |
| **Name** | Actively scan device characteristics for identification |
| **Legal text** | Vendors can:<br>• Create an identifier using data collected via actively scanning a device for specific characteristics, e.g. installed fonts or screen resolution.<br>• 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.<br>• 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.<br>● Not in scope: IP address, user agent; information that does not require access via JavaScript or API<br>● 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.

### 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<br>● 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<br>● Purpose 7: Measure ad performance |

### Stack 3 - Personalised ads

| | |
|---|---|
| **Number** | 3 |
| **Name** | Personalised ads |
| **Description** | Ads can be personalised based on a profile. More data can be added to better personalise ads. |
| **Purposes included** | ● Purpose 2: Select basic ads<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised 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. |
| **Purposes included** | ● Purpose 2: Select basic ads<br>● Purpose 7: Measure ad performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 5 - Basic ads, personalised ads profile, and ad measurement

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

### Stack 6 - Personalised ads display and ad measurement

| | |
|---|---|
| **Number** | 6 |

| | |
|---|---|
| **Name** | Personalised ads display and measurement |
| **Description** | Ads can be personalised based on a profile. Ad performance can be measured. |
| **Purposes included** | ● Purpose 2: Select basic ads<br>● Purpose 4: Select personalised ads<br>● Purpose 7: Measure ad performance |

### Stack 7 - Personalised ads display, ad measurement, and audience insights

| | |
|---|---|
| **Number** | 7 |
| **Name** | Personalised ads display, ad measurement, and audience insights |
| **Description** | Ads can be personalised based on a profile. 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<br>● Purpose 4: Select personalised ads<br>● Purpose 7: Measure ad performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 8 - Personalised ads and ad measurement

| | |
|---|---|
| **Number** | 8 |
| **Name** | Personalised ads and ad measurement |
| **Description** | Ads can be personalised based on a profile. More data can be added to better personalise ads. Ad performance can be measured. |
| **Purposes included** | ● Purpose 2: Select basic ads<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 7: Measure ad performance |

### Stack 9 - Personalised ads, ad measurement, and audience insights

| | |
|---|---|
| **Number** | 9 |

| | |
|---|---|
| **Name** | Personalised ads, ad measurement, and audience insights |
| **Description** | Ads can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 7: Measure ad performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 10 - Personalised ads profile and display

| | |
|---|---|
| **Number** | 10 |
| **Name** | Personalised ads profile and display |
| **Description** | Ads can be personalised based on a profile. More data can be added to better personalise ads. |
| **Purposes included** | ● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads |

### Stack 11 - Personalised content

| | |
|---|---|
| **Number** | 11 |
| **Name** | Personalised content |
| **Description** | Content can be personalised based on a profile. More data can be added to better personalise content. |
| **Purposes included** | ● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content |

### Stack 12 - Personalised content display and content measurement

| | |
|---|---|
| **Number** | 12 |
| **Name** | Personalised content display and content measurement |

| | |
|---|---|
| **Description** | Content can be personalised based on a profile. Content performance can be measured. |
| **Purposes included** | ● Purpose 6: Select personalised content<br>● Purpose 8: Measure content performance |

### Stack 13 - Personalised content display, content measurement and audience insights

| | |
|---|---|
| **Number** | 13 |
| **Name** | Personalised content display, content measurement and audience insights |
| **Description** | Content can be personalised 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 personalised content<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 14 - Personalised content and content measurement

| | |
|---|---|
| **Number** | 14 |
| **Name** | Personalised content and content measurement |
| **Description** | Content can be personalised based on a profile. More data can be added to better personalise content. Content performance can be measured. |
| **Purposes included** | ● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 8: Measure content performance |

### Stack 15 - Personalised content, content measurement and audience insights

| | |
|---|---|
| **Number** | 15 |
| **Name** | Personalised content, content measurement and audience insights |
| **Description** | Content can be personalised based on a profile. More data can be added to better personalise 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 personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

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

| | |
|---|---|
| **Number** | 16 |
| **Name** | Personalised content, content measurement, audience insights, and product development |
| **Description** | Content can be personalised based on a profile. More data can be added to better personalise 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 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights<br>● 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** | ● Purpose 7: Measure ad performance |

| | |
|---|---|
| **included** | ● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 18 - Ad and content measurement

| | |
|---|---|
| **Number** | 18 |
| **Name** | A and content measurement |
| **Description** | Ad and content performance can be measured. |
| **Purposes included** | ● Purpose 7: Measure ad performance<br>● 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<br>● Purpose 9: Apply market research to generate audience insights |

### 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<br>● Purpose 8: Measure content performance<br>● 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<br>● Purpose 9: Audience measurement<br>● 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<br>● Purpose 10: Develop and improve products |

### Stack 23 - Personalised ads and content display, ad and content measurement

| | |
|---|---|
| **Number** | 23 |
| **Name** | Personalised ads and content display, ad and content measurement |
| **Description** | Ads and content can be personalised based on a profile. Ad and content performance can be measured. |
| **Purposes included** | ● Purpose 2: Select basic ads<br>● Purpose 4: Select personalised ads<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance |

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

| **Number** | 24 |
|---|---|
| Name | Personalised ads and content display, ad and content measurement, and audien insights |
| **Description** | Ads and content can be personalised 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<br>● Purpose 4: Select personalised ads<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 25 - Personalised ads and content, ad and content measurement

| **Number** | 25 |
|---|---|
| Name | Personalised ads and content, ad and content measurement |
| **Description** | Ads and content can be personalised based on a profile. More data can be added to better personalise ads and content. Ad and content performance can be measured. |
| **Purposes included** | ● Purpose 2: Select basic ads<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance |

### Stack 26 - Personalised ads and content, ad and content measurement, and audience insights

| | |
|---|---|
| **Number** | 26 |
| Name | Personalised ads and content, ad and content measurement, and audience insights |
| **Description** | Ads and content can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 27 - Personalised ads and content profile

| | |
|---|---|
| **Number** | 27 |
| **Name** | Personalised ads and content profile |
| **Description** | More data can be added to personalise ads and content. |
| **Purposes included** | ● Purpose 3: Create a personalised ads profile<br>● Purpose 5: Create a personalised content profile |

### Stack 28 - Personalised ads and content display

| | |
|---|---|
| **Number** | 28 |
| **Name** | Personalised ads and content display |
| **Description** | Ads and content can be personalised based on a profile. |
| **Purposes included** | ● Purpose 2: Select basic ads<br>● Purpose 4: Select personalised ads |

| | |
|---|---|
| | ● Purpose 6: Select personalised 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<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 30 - Personalised ads display, personalised content, ad and content measurement, and audience insights

| | |
|---|---|
| **Number** | 30 |
| **Name** | Personalised ads display, personalised content, ad and content measurement, a audience insights |
| **Description** | Ads and content can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 4: Select personalised ads<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

### Stack 31 - Personalised ads display, personalised content, ad and content measurement, audience insights, and product development

| | |
|---|---|
| **Number** | 31 |

| | |
|---|---|
| **Name** | Personalised ads display, personalised content, ad and content measurement, audience insights, and product development |
| **Description** | Ads and content can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 4: Select personalised ads<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights<br>● Purpose 10: Develop and improve products |

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

| | |
|---|---|
| **Number** | 32 |
| **Name** | **Basic ads, personalised content, ad and content measurement, and audien insights** |
| **Description** | Basic ads can be served. Content can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

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

| | |
|---|---|
| **Number** | 33 |

| | |
|---|---|
| **Name** | Basic ads, personalised content, ad and content measurement, audience insight and product development |
| **Description** | Basic ads can be served. Content can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights<br>● Purpose 10: Develop and improve products |

### Stack 34 - Basic ads, personalised content, content measurement, and audience insights

| | |
|---|---|
| **Number** | 34 |
| **Name** | Basic ads, personalised content, content measurement, and audience insights |
| **Description** | Basic ads can be served. Content can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights |

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

| | |
|---|---|
| **Number** | 35 |
| **Name** | **Basic ads, personalised content, content measurement, audience insights, and product development** |

| | |
|---|---|
| **Description** | Basic ads can be served. Content can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights<br>● Purpose 10: Develop and improve products |

### Stack 36 - Basic ads, personalised content, and ad measurement

| | |
|---|---|
| **Number** | 36 |
| **Name** | Basic ads, personalised content, and ad measurement |
| **Description** | Basic ads can be served. Content can be personalised based on a profile. More data can be added to better personalise content. Ad performance can be measured. |
| **Purposes included** | ● Purpose 2: Select basic ads<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance |

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

| | |
|---|---|
| **Number** | 37 |
| **Name** | Basic ads, personalised content, ad measurement, and product development |
| **Description** | Basic ads can be served. Content can be personalised based on a profile. More data can be added to better personalise 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<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 10: Develop and improve products |

### Stack 38 - Personalised ads, ad measurement, and product development

| | |
|---|---|
| **Number** | 38 |
| **Name** | Personalised ads, ad measurement, and product development |
| **Description** | Ads can be personalised based on a profile. More data can be added to better personalise ads. 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<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 7: Measure ad performance<br>● Purpose 10: Develop and improve products |

### Stack 39 - Personalised ads, ad measurement, audience insights and product development

| | |
|---|---|
| **Number** | 39 |
| **Name** | Personalised ads, ad measurement, audience insights and product development |
| **Description** | Ads can be personalised based on a profile. More data can be added to better personalise ads. Ad 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<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 7: Measure ad performance<br>● Purpose 9: Apply market research to generate audience insights<br>● Purpose 10: Develop and improve products |

### Stack 40 - Personalised ads, ad and content measurement, audience insights and product development

| | |
|---|---|
| **Number** | 40 |
| **Name** | Personalised ads, ad and content measurement, audience insights and product development |
| **Description** | Ads can be personalised based on a profile. More data can be added to better personalise ads. Ad and content performance can be measured. Insights about 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<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights<br>● Purpose 10: Develop and improve products |

### Stack 41 - Personalised ads, personalised content display, ad and content measurement, audience insights and product development

| | |
|---|---|
| **Number** | 41 |
| **Name** | Personalised ads, personalised content display, ad and content measurement, audience insights and product development |
| **Description** | Ads and content can be personalised based on a profile. More data can be added to better personalise ads. Ad and content performance can be measured. Insights about 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<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights<br>● Purpose 10: Develop and improve products |

### Stack 42 - Personalised ads and content, ad and content measurement, audience insights and product development

| | |
|---|---|
| **Number** | 42 |
| **Name** | Personalised ads and content, ad and content measurement, audience insights and product development |
| **Description** | Ads and content can be personalised based on a profile. More data can be added to better personalise ads and content. Ad and content performance can be measured. Insights about 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<br>● Purpose 3: Create a personalised ads profile<br>● Purpose 4: Select personalised ads<br>● Purpose 5: Create a personalised content profile<br>● Purpose 6: Select personalised content<br>● Purpose 7: Measure ad performance<br>● Purpose 8: Measure content performance<br>● Purpose 9: Apply market research to generate audience insights<br>● Purpose 10: Develop and improve products |

# F. Example Stack Combinations

## Example Stack Combination 1

- **Purpose 1: Store and/or access information on a device**
- **Special Feature 1: Use precise geolocation data**
- **Stack 3: Personalised ads**
    - Purpose 2: Select basic ads
    - Purpose 3: Create a personalised ads profile
    - Purpose 4: Select personalised ads
- **Stack 11: Personalised content**
    - Purpose 5: Create a personalised content profile
    - Purpose 6: Select personalised 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**

## Example Stack Combination 2

- **Purpose 1: Store and/or access information on a device**
- **Special Feature 1: Use precise geolocation data**
- **Stack 8:** Personalised ads, and ad measurement
    - Purpose 2: Select basic ads
    - Purpose 3: Create a personalised ads profile
    - Purpose 4: Select personalised ads
    - Purpose 7: Measure ad performance
- **Stack 14: Personalised content, and content measurement**
    - Purpose 5: Create a personalised content profile
    - Purpose 6: Select personalised 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)

- **Purpose 1: Store and/or access information on a device**
- **Special Feature 1: Use precise geolocation data**
- **Stack 3: Personalised ads**
    - Purpose 2: Select basic ads
    - Purpose 3: Create a personalised ads profile
    - Purpose 4: Select personalised 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**

# 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 accord with the Framework Policies and the Specifications, consistent with legal requirements to support the transparent and lawful storing and/or accessing of information on user devices and/or processing of users' personal data by Vendors. The Framework UI may be used to support the Publisher's own transparent and lawful storing and/or accessing of information on user devices and/or processing of users' personal data.

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 EU privacy and data protection law. In the event of a conflict between applicable EU 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 and 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.

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 process users' personal data for one or more Purposes, Special Purposes, and/or using one or more Special Features disclosed by the Publisher in line with a OOB legal basis 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 object to disclosed Vendors processing personal data 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.

## 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 covers all or substantially all of the content of the website or app.

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:

I. Must include information about the fact that information is stored on and/or accessed from the user's device (e.g. use of cookies, device identifiers, or other device data);
II. Must include information about the fact that personal data is processed, and the nature of the personal data processed (e.g. unique identifiers, browsing data);

III. Must include information about the fact that third party Vendors will be storing and/or accessing information from the user's device and processing their personal data; and a link to the list of named third parties;
IV. Must include the list of the distinct and separate Purposes for which the Vendors are processing data, using at least the standardized names and/or Stack names as defined in Appendix A;
V. Must include information about the Special Features used by the Vendors when processing data;
VI. Should include information about the consequences (if any) of consenting or not consenting (including withdrawing consent);
VII. Must include information about the scope of the consent choice, i.e. global consent, service-specific consent, or group-specific consent. If group-specific consent, a link with information about the group;
VIII. Must include information about the fact that the user can withdraw their consent at any time, and how to resurface the Framework UI in order to do so;
IX. Should include information about the fact that some Vendors (if any) are not requesting consent, but processing the user's data on the basis of their legitimate interest; the fact that the user has a right to object to such processing; and a link to the relevant layer of the Framework UI dealing with processing on the basis of legitimate interests where more information can be found;
X. Must include a call to action for the user to express their consent (for example "Accept", "Okay", "Approve", etc.);
XI. Must include a call to action for the user to customise their choices (for example "Advanced Settings", "Customise Choices", etc.).

c. When making use of a so-called layered approach, a secondary layer must be provided that allows the user to:

I. review the list of named Vendors, their Purposes, Special Purposes, Features, Special Features, associated Legal Bases, and a link to each Vendor's privacy policy, their maximum device storage duration as well as, where available, any additional purpose-specific storage and access information provided by a Vendor in accordance with the Specifications;
II. review the list of Purposes, Special Purposes, Features, and Special Features including their standard name and their full standard description, as defined in Appendix A, and a way to see which Vendors are seeking consent for each of the Purposes;
III. make granular and specific consent choices with respect to each Vendor, and, separately, each Purpose for which the Publisher chooses to obtain consent on behalf of or more Vendors;
IV. make granular and specific opt-in choices with respect to each Special Feature for which the Publisher chooses to obtain opt-ins on behalf of one or more Vendors;
V. where applicable and not disclosed in a 1st layer, view information about the fact that some Vendors (if any) are not requesting consent, but processing the user's data on the basis of their legitimate interest; the fact that the user has a right to object to such processing; and a link to the relevant layer of the Framework UI dealing with processing

on the basis of legitimate interests where more information could be found and the right to object exercised;

VI. Where not disclosed in a 1st layer, view information about the consequences (if any) of consenting or not consenting (including withdrawing consent).

d. When a user accesses a layer, which will be a secondary layer when using a layered approach, allowing them to make granular and specific consent choices with respect to each Purpose, under Policy C(c)(III), and/or to make granular and specific opt-in choices with respect to each Special Feature under Policy C(c)(IV) the default choice must be “no consent”, “no opt-in” or “off”.

e. If a UI displays Vendors who are not registered with IAB Europe 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.

f. A user must be able to resurface the Framework UI from an easily accessible link, such as a Privacy Policy available on the Publisher’s website or app as to allow them to withdraw their consent 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”).

g. 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.

h. By way of derogation from Appendix B, Policies C(c)(iii) and (iv) and C(d), a Publisher shall not be required to allow a user to make granular and specific consent or opt-in choices if the Publisher implements a way for the user to access its content without consenting through other means, for example by offering paid access that does not require consenting to any Purposes. For the avoidance of doubt, all other Policies remain applicable.

# D. Specific Requirements for Framework UIs in Connection with Legitimate Interests

a. When providing transparency about Purposes, Special Purposes, Features, Special Features, and Vendors in connection with a legitimate interest for the same, transparency must be provided at least through an easily accessible link to the relevant layer of the Framework UI dealing with processing on the basis of legitimate interests.

b. When providing transparency about Purposes, Special Purposes, Features, Special Features, and Vendors in connection with both requesting a user’s consent for the same and a legitimate interest, Policy C(a) applies, and the easily accessible link to the relevant layer of the

Framework UI dealing with processing on the basis of legitimate interests required under Policy D(a) must be included in the Initial Layer of the Framework UI presented in line with Policy C(a).

c. When providing transparency about Purposes, Special Purposes, Features, Special Features and Vendors in connection with a legitimate interest for the same, a single secondary layer must be provided that allows the user to:

I. see information about the fact that personal data is processed, and the nature of the personal data processed (e.g. unique identifiers, browsing data);
II. see information about the scope of the legitimate interest processing and scope of any objection to such processing, i.e. global scope, service-specific scope, or group-specific scope. If group-specific scope, a link with information about the group.
III. access controls within the Framework UI to object to processing of their personal data on the basis of a legitimate interest;
IV. review the list of Purposes and Special Purposes including their standard name and their full standard description, as defined in Appendix A, and a way to see which Vendors are processing their data for each of the Purposes and Special Purposes on the basis of a legitimate interest;
V. exercise their right to object with respect to processing under a legitimate interest for each Vendor, and, separately, each Purpose for which the Publisher chooses to help establish Vendors transparency;
VI. review the list of named Vendors, their Purposes, Special, Purposes, Features, Special Features, and Legal Bases, and find a link to each Vendor's privacy policy.

# Version History and Changelog

- Version 2018-04-10.1 – Initial Framework Policies.
- Version 2018-04-25.2 – Added Purpose and Feature Definitions to Appendix A, and UI/UX Guidelines and Requirements to Appendix B.
- Version 2018-10-02.2a – Removed a provision stating CMPs must only work with Vendors registered with the MO. Clarified conditions for providing services to Vendors not registered with the MO.
- **Version 2019-08-21.3** – Framework Policies for Version 2.0. Major changes have been made to the Policies, including Appendix A, and Appendix B.
- Version 2020-04-06.3a – Added Stacks 38-42. Removed requirement to disclose Special Purposes and Feature in initial UI layer.
- Version 2020-06-30.3.1 – Added CTA prominence requirement in Appendix B, Policy C and storage duration disclosure requirements in Policy 16(2*bis*) and Appendix B, Policy C(c)(I).
- Version 2020-08-24.3.2 – Removed non-essential 1st layer requirements and updated 2nd layer requirements in Appendix B, Policy C. Added Appendix B, Policy C(h) introducing a derogation from Appendix B, Policy C(c)(iii),(iv) and (d) on not providing granular choices in certain situations.
- Version 2020-11-18.3.2a – Updated Vendor guidance for Purpose 1 to clarify it must be declared in conjunction with another Purpose, Feature, Special Purpose and/or Special Feature except where processors register for Purpose 1. Added new policy 13(7) to clarify that Vendors should verify signals have been obtained using API.