Policies & Technical Specifications Controls Catalogue

1. Introduction **2**
2. Enforcement procedures **2**
Procedure n°1: Tampering of TC Strings by CMPs & Vendors' live installations 2
Procedure n°2: Other material breach of the TCF Policies by CMPs & Vendors' live installations 3
Procedure n°3: Vendors' information required for inclusion in the GVL is incomplete or inaccurate 3
3. CMP Checklist **4**
Technical Checks 4
Policies Checks 8
Initial layer checks 8
Secondary layers checks 12
Resurfacing of the UI 20
4. Vendor Checklist **21**
Technical checks 21
Registration checks 23
Version History and Changelog **26**

1. Introduction

The Controls Catalogue maps requirements of the Transparency & Consent Framework Policies and the corresponding Technical Specifications to auditable elements that can help participants in assessing and reviewing the compliance of their TCF implementations.

The Controls Catalogue also includes the description of the applicable enforcement procedures in case of non-compliance with the TCF Policies or Technical Specifications under the TCF Compliance programmes. Please note that while the Controls Catalogue describes the primary checks IAB Europe performs to verify compliance of TCF participants in the context of the TCF Compliance Programmes, IAB Europe will continue monitoring compliance with all TCF Policies and adopting enforcement measures where non-compliance is identified, in line with its prerogatives under the TCF Policies and Terms and Conditions.

2. Enforcement procedures

The TCF Compliance Programmes set forth differentiated enforcement procedures according to the nature of the non-compliance with the TCF Policies or Technical Specifications. The Controls Catalogue below indicates which procedure is applicable in the case of a particular breach.

Procedure n°1: Tampering of TC Strings by CMPs & Vendors' live installations

Where a live CMP or Vendor installation is found to be tampering with TC Strings, the following process applies:

- Participant receives a formal suspension notice via email;
- Immediate suspension from the GVL or CMP list for a minimum of 4 weeks and until the issue is resolved;
- Public notification of non-compliance to the TCF Community, including facts and reasoning;

- If this is the fourth time within a twelve-month period that the participant has been found tampering with TC Strings, it will be notified and permanently suspended from the GVL or CMP list.

<u>Procedure n°2:</u> Other material breach of the TCF Policies by CMPs & Vendors' live installations

Where a live CMP or Vendor installation is found in breach of the TCF Policies (except in cases of TC String tampering), the following process applies:

- Participant receives a formal suspension warning via email;
- **Web-deployed environments** (web pages and mobile applications using a mobile web view):
  - CMPs are given 10 business days to remedy the issues.
  - Vendors are given 20 business days to remedy the issues.
- **Mobile applications** (fully native):
  - CMPs and Vendors have 10 business days to correct the issue within their SDKs or code snippets.
  - Once these updates are made available, the publisher of the affected application has an additional 30 business days to integrate the changes and republish the updated application(s) if necessary."
-
- If, following the expiration of the delay, the issues have not been resolved, the participant will receive a suspension notice via email and will be suspended from the GVL or CMP list until the issues have been remedied;
- If this is the fourth time within a twelve-month period that the participant has been found in breach of the TCF Policies, it will be notified via email and suspended from the GVL or CMP list with immediate effect <u>for a minimum of 2 weeks</u> and until all issues are resolved.

<u>Procedure n°3:</u> Vendors' information required for inclusion in the GVL is incomplete or inaccurate

Where a Vendor has provided inaccurate or incomplete information requested to register to the GVL, or if a Vendor has not appropriately completed their Vendor Compliance Questionnaire, the following process applies:

- Vendor receives a formal suspension warning via email;

- Vendor is given 5 business days to remedy the issues;
- If, following the expiration of the delay, the issues have not been resolved, the Vendor will receive a suspension notice via email and will be suspended from the GVL until the issues have been remedied;
- If this is the fourth time within a twelve-month period that the Vendor has been found in breach of the TCF Policies, it will be notified via email and suspended from the GVL with immediate effect for a minimum of 1 week and until all issues are resolved.

3. CMP Checklist

Number	Audited element	TCF policies references	Applicable enforcement procedure
Technical Checks			
1.	**Are consent signals in the TC String created after affirmative action by the user?** *For this check to pass, there must be either a) no TC String or b) all purpose and vendor consent signals must be set to 'no'.*	**Chapter II: Policies for CMPs; 5(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.*	**1**
2.	**If a 'Reject All' option is provided in the user interface, when the user clicks on it, are all consent signals for purposes and vendors set to 'off'?** *This check fails if there are any*	**Chapter II: Policies for CMPs; 5(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.*	**1**

	positive purpose or vendor consent signals after the user clicks 'Rejects All'.		
3.	**Does the API return an updated TC string after a change of users' choices made in the CMP UI?** *This check fails if the purpose and vendor consent or LI signals do not map the disclosures provided and choices made in the CMP UI.*	**Chapter II: Policies for CMPs; 5(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.* **Chapter II: Policies for CMPs; 5(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.* **Chapter II: Policies for CMPs; 5(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.*	**1**
4.	**Did all CMP API required commands return a correct response?** *This check fails if any of the following mandatory CMP API commands does not return an expected response: ping, addEventListener, removeEventListener.*	**CMP API v2.1 technical specifications.** *All CMPs must support three required API commands: 'ping', 'addEventListener' and 'removeEventListener'.*	**2**

5.	**Is the CMP registered?** *CMP is registered as a participant of a Transparency and Consent Framework and included in the CMP List.*	**Chapter II: Policies for CMPs; 2(1). Applying and registering.** *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**
6.	**Is the GVL version format correct?** *This check fails if the GVL version number is 0 or a number higher than the latest version of the GVL.*	**Chapter II: Policies for CMPs; 4(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.*	**2**
7.	**Is the current or penultimate version of the GVL being used?** *This checks fails if the version of the GVL being used is not the current or last version of the GVL (the last version of the GVL is acceptable as the GVL may be cached for up to one week meaning that the cached version could be 1 version out-of-date).*	**Chapter II: Policies for CMPs; 4(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.*	**2**
8.	**Is the max vendor ID less than or equal to the highest id in the GVL?** *This check fails if the max vendor id for consent or legitimate interest is not less than or equal to the highest*	**Chapter II: Policies for CMPs; 4(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**

	vendor id in the GVL being used by the CMP.		
9.	**Are purposes 1, 3, 4, 5 and 6 set to 'no' for legitimate interest?** *Vendors cannot base processing for Purposes 1, 3, 4, 5 and 6 on Legitimate Interest.*	**Chapter II: Policies for CMPs; 5(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*.	**2**
10.	**Do the Created and LastUpdated fields have the same value?** *As a result of the limited relevance of the Created field for publishers and their CMPs to remind users of their choices, the Created and LastUpdated fields have been updated to have the same value.*	**Chapter II: Policies for CMPs; 4(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**
11.	**Are the Created and LastUpdated timestamps imprecise?** *This check fails if the Created and LastUpdated timestamps do not have hours, minutes and seconds properly zeroed out.*	**Chapter II: Policies for CMPs; 4(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**
12.	**Are all vendor signals for deleted vendors set to 0?** *This check fails if there are any positive vendor consent or LI signals for vendors that are marked as deleted in the version of the GVL being used.*	**Chapter II: Policies for CMPs; 5(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*.	**2**

13.	**Does the TC String include the disclosedVendors segment?** *This check fails if the TC String does not include the disclosedVendors segment after the Core String.*	**Chapter II: Policies for CMPs; 4(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**
Policies Checks			
Initial layer checks			
1.	**Is the UI prominently displayed, covering most of the website content?**	**Appendix B, Policy C(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.*	**2**
2.	**Is the UI displayed separately from other information such as terms and conditions or the privacy policy?**	**Appendix B, Policy C(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.*	**2**
3.	**Does the 1st layer of the UI provide information about the**	**Appendix B, Policy C(b)(I).**	**2**

	storage and access of information from the user's device by third-party vendors?	*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);* **Appendix B, Policy C(b)(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, the number of third party Vendors (which may also include Vendors not participating in the Framework), and a link to the list of named third parties.*	
4.	**Does the 1st layer of the UI provide information about the processing of personal data by third party Vendors?**	**Appendix B, Policy C(b)(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);* **Appendix B, Policy C(b)(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, the number of third party Vendors (which may also include Vendors not participating in the Framework), and a link to the list of named third parties.*	**2**
5.	**Does the 1st layer of the UI provide an example of personal data processed?**	**Appendix B, Policy C(b)(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);*	**2**
6.	**Is there a direct link to the list of third parties in the 1st layer of the UI?**	**Appendix B, Policy C(b)(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 , the number of third*	**2**

		party Vendors (which may also include Vendors not participating in the Framework), and a link to the list of named third parties.	
7.	**Does the 1st layer of the UI provide information about the Purposes and/or Stacks and Special Features used by third parties?**	**Appendix B, Policy C(b)(IV)**. *Must include the list of the distinct and separate Purposes for which the Vendors are processing data, using at least the standardised names and/or Stack names as defined in Appendix A.* **Appendix B, Policy C(b)(V)**. *Must include information about the Special Features used by the Vendors when processing data.*	**2**
8.	**Does the 1st layer of the UI provide information about the scope of the consent choice, i.e. service-specific consent or group-specific consent?**	**Appendix B, Policy C(b)(VII).** *Must include information about the scope of the consent choice, i.e. service-specific consent, or group-specific consent. If group-specific consent, a link with information about the group.*	**2**
9.	**Does the 1st layer of the UI inform the user that they can withdraw their consent at any time and how to do so?**	**Appendix B, Policy C(b)(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.*	**2**
10.	**Are there calls to action in the 1st layer for users to express consent (e.g. "accept") and customise their choices (e.g. 'manage options')?**	**Appendix B, Policy C(b)(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).* **Appendix B, Policy C(b)(X).** *Must include a call to action for the user to express their consent (for example "Accept", "Okay", "Approve", etc.).*	**2**

		Appendix B, Policy C(b)(XI). *Must include a call to action for the user to customise their choices (for example "Advanced Settings", "Customise Choices", etc.).*	
11.	**Do the two primary calls to action on the 1st layer have matching text treatment and, for each, a minimum contrast ratio of 5:1?**	**Appendix B, Policy C(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.*	**2**
12.	**Does the 1st layer of the UI show the number of the third party Vendors?**	**Appendix B: Policy C(b)(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, the number of third party Vendors (which may also include Vendors not participating in the Framework), and a link to the list of named third parties.*	**2**
13.	**If the 1st layer of the UI provides information about the Purposes and Special Features used by Vendors using modified Stack descriptions, is the UseNonStandardTexts flag set to 1?**	**Chapter IV: Policy for Publishers; 21(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.*	

Secondary layers checks			
14.	**Does the UI show Purposes and Features with their standard names or Stacks, and, where Features are presented, provide the standard Feature explanation without associating Features with controls?**	**Appendix B, Policy B(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 user-friendly text, and where applicable the standard illustrations for each Purpose, Special Purpose, Feature, Special Feature and Category of data of Appendix A* **Appendix B, Policy B(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, Special Feature and Category of data names and definitions of Appendix A as they are published on the Global Vendor List.* **Appendix B, Policy C(b)(IV).** *Must include the list of the distinct and separate Purposes for which the Vendors are processing data, using at least the standardised names and/or Stack names as defined in Appendix A.* **Appendix B, Policy C(c)(II).** *review the list of Purposes, Special Purposes, Features, and Special Features including their standard name, their full standard user-friendly text and where applicable their illustrations, as defined in Appendix A, the number of Vendors seeking consent for each of the Purposes (which may also*	**2**

		include Vendors not participating in the Framework), and have a way to see those Vendors; **Appendix B, Policy B(f).** *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 and detect fraud, and fix errors) regardless of the user's choice about Special Features. When a user accesses a layer, which will be a secondary layer when using a layered approach, allowing them to review Features (including their standard name, their full standard user-friendly text and illustrations), the standard feature explanations text should be provided, and Features should not be associated with controls, so as to not mislead users.*	
15.	**Can users review the standard user-friendly texts and illustrations, for both Purposes and Features?**	**Appendix B, Policy B(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 user-friendly text, and where applicable the standard illustrations for each of Purpose, Special Purpose, Feature, Special Feature and Category of data of Appendix A.*	**2**
16.	**If the UI includes non-TCF Vendors, are they presented separately?**	**Appendix B, Policy B(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*	**2**

		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. **Appendix B, Policy C(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.*	
17.	**Does the UI provide information about third party Vendors processing personal data based on legitimate interest (if any)?**	**Appendix B, Policy C(b)(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.* **Appendix B, Policy D(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.* **Appendix B, Policy D(b).**	**2**

		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).	
18.	**Does the UI advise the user of their right to object to their personal data being processed on the basis of legitimate interest (if any)?**	**Appendix B, Policy C(b)(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.*	**2**
19.	**Is the user able to review the list of Vendors, their Purposes, Special Purposes, Features, Special Features, associated Legal Bases and a link to their privacy policy, as well as make granular choices per Purpose and per Vendor (when applicable)?**	**Appendix B, Policy C(c)(I).** *review:* ○ *the list of named Vendors and a link to each Vendor's privacy policy,* ○ *their Purposes, Special Purposes, associated Legal Bases and corresponding retention period,* ○ *their Features and, Special Features, and* ○ *the categories of data collected and processed;* **Appendix B, Policy C(c)(II).** *review the list of Purposes, Special Purposes, Features, and Special Features including their standard name, their full standard user-friendly text and where applicable their illustrations, as defined in Appendix A, the number of Vendors seeking consent for each of the Purposes (which may also*	**2**

		include Vendors not participating in the Framework), and have a way to see those Vendors; **Appendix B, Policy C(c)(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.* **Appendix B, Policy C(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.*	
20.	**Does the 2nd layer allow users to make granular and specific opt-in choices with respect to each Special Feature (when applicable)?**	**Appendix B, Policy C(c)(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.*	**2**
21.	**Are user choices set to 'off' by default?**	**Appendix B, Policy C(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".*	**2**
22.	**If legitimate interest is used by**	**Appendix B, Policy D(c)(I).**	**2**

	any Vendors as a legal basis, does the information in the 2nd layer specify the nature of processed information and its scope?	*See information about the fact that personal data is processed, and the nature of the personal data processed (e.g. unique identifiers, browsing data).* **Appendix B, Policy D(c)(II).** *See information about the scope of the legitimate interest processing and scope of any objection to such processing, i.e. service-specific scope, or group-specific scope. If group-specific scope, a link with information about the group.*	
23.	**If legitimate interest is used by any Vendors as a legal basis, does the 2nd layer allow users to object to the processing of their personal data, per Purpose and per Vendor?**	**Appendix B, Policy D(c)(III).** *Access controls within the Framework UI to object to processing of their personal data on the basis of a legitimate interest.* **Appendix B, Policy D(c)(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.*	**2**
24.	**Does the 2nd UI layer provide information about Vendors' maximum device storage duration including whether such duration may be refreshed and, where applicable, additional purpose-specific storage?**	**Appendix B, Policy C(c)(VII).** *Where applicable, review Vendors' maximum device storage duration and whether Vendors refresh such duration (by stating, for example, that "duration may expire [n] months/days from your last interaction with the property", where [n] represents the maximum duration for which the Vendor considers the user consent as valid) as well as, where available, review any additional purpose specific storage and access information provided by a Vendor in accordance with the Specifications.*	**2**
25.	**Does the secondary layer show the number of Vendors seeking consent or relying on legitimate**	**Appendix B: Policy C(c)(II).** *Review the list of Purposes, Special Purposes, Features, and Special Features including their standard name and their full*	**2**

	interest for each Purpose?	*standard user-friendly text, as defined in Appendix A, the number of Vendors seeking consent for each of the Purposes (which may also include Vendors not participating in the Framework), and have a way to see those Vendors;* **Appendix B: Policy D(c)(IV).** *Review the list of Purposes and Special Purposes including their standard name, their full standard user-friendly text and where applicable their illustrations, as defined in Appendix A, the number of Vendors processing their data for each of the Purposes on the basis of legitimate interest (which may also include Vendors not participating in the Framework), and have a way to see those Vendors;*	
26.	**Does the secondary layer allow users to access Vendors' information about their legitimate interest at stake, where applicable?**	**Appendix B: Policy D(c)(VI)** *review:* ○ *the list of named Vendors, and a link to each Vendor's privacy policy,* ○ *their Purposes, Special, Purposes, associated Legal Bases (and a link to each Vendor's explanation of its legitimate interest(s) at stake) and corresponding retention period,* ○ *their Features, Special Features and* ○ *the categories of data collected and processed*	**2**
27.	**Does the secondary layer provide information about Vendors' retention periods?**	**Appendix B, Policy C(c)(I).** *review:* ○ *the list of named Vendors and a link to each Vendor's privacy policy,* ○ *their Purposes, Special Purposes, associated Legal Bases and corresponding retention period,* ○ *their Features and, Special Features, and* ○ *the categories of data collected and processed;*	**2**

		Appendix B: Policy D(c)(VI) *review:* ○ *the list of named Vendors, and a link to each Vendor's privacy policy,* ○ *their Purposes, Special, Purposes, associated Legal Bases (and a link to each Vendor's explanation of its legitimate interest(s) at stake) and corresponding retention period,* ○ *their Features, Special Features and* ○ *the categories of data collected and processed*	
28.	**Does the secondary layer disclose the categories of data collected and/or already held by Vendors?**	**Appendix B, Policy C(c)(I).** *review:* ○ *the list of named Vendors and a link to each Vendor's privacy policy,* ○ *their Purposes, Special Purposes, associated Legal Bases and corresponding retention period,* ○ *their Features and, Special Features, and* ○ *the categories of data collected and processed;* **Appendix B: Policy D(c)(VI)** *review:* ○ *the list of named Vendors, and a link to each Vendor's privacy policy,* ○ *their Purposes, Special, Purposes, associated Legal Bases (and a link to each Vendor's explanation of its legitimate interest(s) at stake) and corresponding retention period,* ○ *their Features, Special Features and* ○ *the categories of data collected and processed*	**2**
29.	**If the secondary layer of the UI**	**Chapter IV: Policy for Publishers; 21(7).**	**2**

	provides modified or additional illustrations about the Purposes and Special Purposes used by Vendors, is the UseNonStandardStacks flag set to 1?	*A publisher must not modify or supplement, or instruct its CMP to modify or supplement, standard illustrations and/or their translations unless: (a) the Publisher follows any guidance that may be disseminated or updated by the MO so that the modified or additional illustrations provide accurate examples of data processing operations performed by Vendors under the Purposes; (b) the Publisher can modify only one of the two standard illustrations presented for each Purpose. Modifying the standard illustrations for Special Purposes and Purpose 1 (store and/or access information on a device) is not permitted; (c) Vendors are alerted to the fact of a Publisher using custom illustrations through the appropriate Signal in accordance with the Specification.*	
30.	**Does the secondary layer of the UI disclose the storage and access information relating to the CMP's recording of signals, including the maximum device storage duration where applicable?** *CMPs should at a minimum disclose on the secondary layer of their UIs how the TC String is stored and for how long if it is stored on the user's device.*	**Appendix B: Policy D (c) (VII)** *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: (...)* *VII. review where applicable the storage and access information relating to the CMP's recording of Signals, including the maximum device storage duration.*	**2**
Resurfacing of the UI			
31.	**Is the user able to resurface the CMP UI easily?**	**Appendix B: Policy (C)(f).** *A user must be able to resurface the Framework UI from an easily accessible link or call to action, such as a floating icon or a*	**2**

		footer link available on each webpage of the Publisher's website, or from the top-level settings of the Publisher's app as to allow them to withdraw their consent as easily as it was to give it.	
32.	**Is the user able to withdraw their consent as easily as they were able to give consent?**	**Appendix B: Policy (C)(f)** *If a call to action for the user to express their consent for all Purposes and Vendors was provided in the Initial Layer of the Framework UIs used to request the user's consent (for example "Consent to all"), an equivalent call to action for the user to withdraw their consent for all Purposes and Vendors must be provided in the Framework UI that the user resurfaces (for example "Withdraw consent to all").*	**2**

4. Vendor Checklist

Number	Audited elements	TCF Policies references	Applicable enforcement procedure
Technical checks			
1.	**Writing of cookies** *This check passes when there is no setting of cookies by the Vendor when there is no consent signal for purpose 1 or no consent signal for the vendor.*	**Chapter III: Policies for Vendors (14)(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**
2.	**Cookie duration**	**Chapter III: Policies for Vendors (14)(2bis);** *A Vendor shall indicate on the GVL the maximum duration of*	**2**

	This check passes when the Vendors' cookies have a max-age less or equal to the max-age registered in the GVL.	*information stored on a user's device, including whether such duration may be refreshed. A Vendor must, in addition, provide more detailed and purpose-specific storage and access information in accordance with the Specifications.*	
3.	**Integrity of TCF signals** *This check passes if no TC String is found in request URLs when no TC String is returned by the CMP API.* *This check passes if when the GDPR_CONSENT macro is present, its content is the same as the TC string returned by the CMP API.*	**Chapter III: Policies for Vendors (12)(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.*	**1**
4.	**Passing of personal data from a Vendor to another** *This check passes if the Vendor only initiates another Vendor's redirect that includes a UID when the receiving Vendor has a legal basis for processing.*	**Chapter III: Policies for Vendors (14)(15);** *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.*	**2**
5.	**Use of the addEventListener" CMP command** *Applicable where the Vendor is able to execute Javascript. This check passes if the Vendor has registered a listener function via addEventListener to retrieve changed TC Strings in real-time.*	**Chapter III: Policies for Vendors (12)(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*	**2**

		Feature where a Signal has been received more recently by that Vendor.	
6.	**Reliance on TCF signals returned by CMPs** *This check fails if the Vendor stores the TC String in proprietary storage mechanism instead of retrieving the TC String according to the Technical Specifications.*	**Chapter III: Policies for Vendors (12)(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 Signal has been received more recently by that Vendor.*	**2**
Registration checks			
1.	**Availability and language of Privacy Policy URLs** *The URLs to the Vendor's Privacy Policy are available and in the language indicated when registering to the GVL.*	**Chapter III: Policies for Vendors (9)(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 for each Purpose and Special Purpose and, where applicable, a link to an explanation of its legitimate interest(s) at stake, the retention period of data processed for each Purpose and Special Purpose, the Features and Special Features it relies on in pursuit of such Purposes and Special Purposes, the categories of data it collects and processes in pursuit of the Purposes and Special Purposes it has declared, and its requirements regarding storing and/or accessing information on users' devices. It will ensure its Purposes, Legal Bases, and access to a user's device, are completely and accurately included in the GVL. It will notify the MO of any changes in a timely manner.*	**3**

2.	**Availability and language of Legitimate Interest at stake URLs** *The URLs to the Vendor's explanation of its Legitimate Interest(s) at stake are available and in the language indicated when registering to the GVL.*	**Chapter III: Policies for Vendors (9)(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 for each Purpose and Special Purpose and, where applicable, a link to an explanation of its legitimate interest(s) at stake, the retention period of data processed for each Purpose and Special Purpose, the Features and Special Features it relies on in pursuit of such Purposes and Special Purposes, the categories of data it collects and processes in pursuit of the Purposes and Special Purposes it has declared, and its requirements regarding storing and/or accessing information on users' devices. It will ensure its Purposes, Legal Bases, and access to a user's device, are completely and accurately included in the GVL. It will notify the MO of any changes in a timely manner.*	**3**
3.	**Availability of the deviceStorage.json URL** *This check passes if the Vendor has provided a secure URL to a JSON resource that conforms to the containing disclosures related to the TCF Technical Specifications here and contains purpose-specific storage and access information and web domains used for collecting and processing personal data.*	**Chapter III: Policies for Vendors (9)(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 for each Purpose and Special Purpose and, where applicable, a link to an explanation of its legitimate interest(s) at stake, the retention period of data processed for each Purpose and Special Purpose, the Features and Special Features it relies on in pursuit of such Purposes and Special Purposes, the categories of data it collects and processes in pursuit of the Purposes and Special Purposes it has declared, and its requirements regarding storing and/or accessing information on users' devices. It will ensure its Purposes,*	**3**

		Legal Bases, and access to a user's device, are completely and accurately included in the GVL. It will notify the MO of any changes in a timely manner.	
4.	**The information required when registering on the Global Vendor List (GVL) is not missing, partly missing or incorrect** *This includes the additional information that does not appear in the GVL JSON file but is made available in a separate JSON file as per the TCF Technical Specification here, and the Vendor Compliance Form.*	**Chapter III: Policies for Vendors (9) (2);** *Vendors must provide all information requested by the MO that is reasonably required to fulfil the MO's application and approval procedures.* **Chapter III: Policies for Vendors (9) (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 for each Purpose and Special Purpose and, where applicable, a link to an explanation of its legitimate interest(s) at stake, the retention period of data processed for each Purpose and Special Purpose, the Features and Special Features it relies on in pursuit of such Purposes and Special Purposes, the categories of data it collects and processes in pursuit of the Purposes and Special Purposes it has declared, and its requirements regarding storing and/or accessing information on users' devices. It will ensure its Purposes, Legal Bases, and access to a user's device, are completely and accurately included in the GVL. It will notify the MO of any changes in a timely manner.*	**3**

Version History and Changelog

- Controls Catalogue for TCF Policies version 4.0 - Initial Control Catalogue
- Controls Catalogue for TCF Policies version 5.0 - Added CMP Secondary layers check n°30
- Controls Catalogue for TCF Policies version 5.0.a - Extended Enforcement Procedure n°3 for Vendors that have not appropriately completed their Vendor Compliance Questionnaires
- Controls Catalogue for TCF Policies version 5.0.a - New CMP technical check n°13
- Controls Catalogue for TCF Policies version 5.0.b - Differentiated deadlines under Enforcement Procedure n°2 for Web-Deployed and Native Mobile CMPs & Vendors, and updated Policy Checks n°14 and n°15