Legitimate Interests Assessment: processing of the users' privacy choices in the form of TC Strings

Preamble

IAB Europe, the international online advertising industry association, has developed and published the Transparency and Consent Framework (TCF). Its goal is to standardize the consent process for cookies and provide information about user consent through transmitting a TC String. The TC String records and communicates the individual user's privacy choices.

At Gemius SA, we process the TC String based on our legitimate interest. According to the law, we must carry out a **legitimate interest assessment**. The following text, therefore, documents the performance of such an assessment. In it, we intend to demonstrate that the interests and fundamental rights of the data subjects are pursued precisely through the processing of TC String and that they do not override the legitimate interests we pursued as a TCF participant.

Part 1: Purpose test: Is there a legitimate interest in the processing?

The purpose test identifies the purpose of the processing and assesses whether there is a legitimate interest behind it.

Why do we want to process the data?

We need to process information about users' privacy choices in the form of TC Strings to ensure and demonstrate that users have consented to or not objected to processing their data for various purposes and vendors.

Who benefits from the processing?

In the context of this purpose, there may be several different interests that are of benefit to different categories of stakeholders:

- The processing ensures that **users'** privacy choices can be respected (i.e., the giving, refusing, or withdrawing of consent by users and the exercise of their right to object) and that they do not have to make those choices again on each subsequent use of the relevant digital property.
- The processing ensures that we (**Gemius**) can retrieve and observe those choices.
- The processing contributes to demonstrating compliance with the accountability principle under Article 5(2) of the GDPR by us (**Gemius**).
- The processing contributes to demonstrating our compliance with the Transparency and Consent Framework and its policies established by **IAB Europe** to respect the users' privacy choices
- The processing can support **Data Protection Authorities'** investigations and audits, particularly verifying that we appropriately respect users' privacy choices.

Such interests, in line with Recital 47 of the GDPR and also supported by Opinion 06/2014 of the Article 29 Working Party, may be considered to be legitimate[1].

What would the impact be if we couldn't proceed with the processing?

If we could not remember the users' privacy choices, we would not be able to conduct our business and demonstrate that we have obtained the appropriate users' consent.

Are we complying with any specific data protection rules applicable to our processing?

Yes. We comply with the GDPR's accountability requirement (Article 5(2)). We also refer to Recital 47 of the GDPR, supported by Opinion 06/2014 of the Article 29 Working Party and the APD decision mentioned in the footnote [1] below.

Would our use of the data be unethical or unlawful in any way?

No, we do not use the data to infringe anyone's rights. What is more, we process it precisely to respect these rights.

Accordingly, we process information about users' privacy choices in the form of TC Strings using the lawful basis of legitimate interest to save, communicate, and observe the user's privacy choices.

[1] Additionally, this assessment concords with the Belgian Data Protection Authority's (APD) reasoning in their decision of February 2022 against IAB Europe and the Transparency & Consent Framework (TCF) as stated in paragraphs 413, 414 and 415 and in particular "More specifically, the possibility of storing the preferences of users is an essential part of the TCF and the Litigation Chamber notes that this is done in the legitimate interest of the defendant as well as of third parties involved, such as the participating adtech vendors."

Part 2: Necessity test: Is the processing necessary?

In the necessity test, we demonstrate that the processing is necessary to achieve the purposes pursued and, in particular, that the same result cannot reasonably be achieved by other means without processing personal data and less personal data.

Will this processing help us to achieve our purpose?

We process data, so it is not just a help to further the interest; it is a requirement.

Is each element of the data processed necessary for the purpose?

Yes. In the context of the processing of TC String, it is essential to assess whether the information contained in the TC String is strictly necessary to achieve the intended purpose. In that respect, the TC String captures the following information:

- General metadata: standard markers that indicate details about the Publisher's implementation of the TCF (e.g., the ID of the Consent Management Platform ("CMP") that is used, the language of the user interfaces, whether the user interfaces use non-standard texts (such as custom stacks or illustrations) and a day-level timestamp of when users have made/updated their choices;
- The user's consent per purpose and vendor when the legal basis is Consent ("1" meaning user's consent and "0" meaning user's refusal or withdrawal of consent);
- The user's right-to-object per purpose and vendor when the legal basis is Legitimate interest ("1" meaning the user was informed and "0" meaning the user was not informed or the user's objection to processing);
- Publisher restrictions: metadata specific to the publisher's implementation of the TCF, e.g., indicating a general prohibition for certain vendors to pursue a given data processing purpose;
- Where applicable, the user's choices for purposes that are not covered by the TCF or for vendors that are not participating in the TCF ("1" meaning user's agreement and "0" no agreement).

Accordingly, the TC String contains only information that is strictly necessary to save, communicate, and observe users' privacy choices[2].

Can we achieve the same purpose without the processing?

No.

Can we achieve the same purpose by processing less data or in a less intrusive way?

[2] This part of the assessment is supported by the APD decision of February 2022, in particular in paragraphs 416, 417, and 418. The decision notably states the following: "The Litigation Chamber notes that the information processed in a TC String is limited to data that are strictly necessary to achieve the intended purpose. In addition, based on the documents in this file and the parties' defenses, the Litigation Chamber has not been able to establish that the TC String is retained indefinitely."
The method for capturing users' privacy choices using a TC String is also aligned with the French Data Protection Authority's (CNIL) recommendation on cookies and other trackers (https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf) Indeed, the regulator recommends that users' privacy choices be recorded as a boolean value for each purpose. The existence of non-binding guidance issued by Data Protection Authorities encouraging controllers to adopt the same processing method to achieve the intended purpose is an important consideration for the Legitimate Interest Assessment

Users' privacy choices can be delivered in any way that is agreed upon by the two communication parties; it does not have to be a TC string. However, the essence of this type of processing remains the same: the user's choices are saved and communicated for this purpose to ensure that the user's preferences are respected. Thus, it can be said that there is currently no other way to communicate the user's privacy choices to the different parties involved.

Is the set of operations performed on the data necessary for the purpose?

In Gemius, we do not save the TC String itself. We check that the Publisher has received the appropriate consent and record a note saying the permission has been appropriately given. A TCF-compliant Publisher asks the user about their privacy choices. Consents are checked before saving the data in our system, and if there is no consent, the saved data does not have user IDs. We do not forward TC String anywhere.

Technically speaking, we have access to the CMP API (and therefore can execute Javascript) and do not subsequently share personal data with other entities. We do not need to retrieve the entire TC String. Instead, we can use the relevant CMP API commands to check only parts of the TC String that are strictly necessary to observe users' choices.

We would argue that we have minimized the data to what is absolutely necessary to process it according to the user's choice and ensure that we follow their decisions.

Are the periods of retention for the data justified?

Our retention policy for storing TC Strings complies with the storage limitation principle. TC Strings are erased once they are no longer needed for the relevant purpose (e.g., a TC String might cease to be relevant if, beyond a certain period, it no longer reflects users' choices).

Part 3: Balancing test: What is the impact on individuals' interests? Does this override our legitimate interests?

The balancing test weighs the individual's rights and freedoms against the identified purpose and legitimate interests. The weighing must consider the entire context of the processing, precisely the nature of the legitimate interests and the impact on individuals. It should also factor in the safeguards the controller implements for the processing.

1) Nature of the personal data

The more sensitive the data, the more likely it is to intrude on the data subjects' interests or create risks to data subjects' fundamental rights and freedoms. Therefore, it weighs more against legitimate interests. Consequently, the nature of the personal data processed should be appropriately evaluated as part of the balancing test.

Do we process special categories or crime data?

In the present case, the TC String is a string of characters representing an abstract user's privacy choices without directly attributing these to any specific user.

Indeed, the combined state of these various privacy choices is not unique, as millions of users visit digital properties on the same day and can express the same preferences. The number of choices a user can make is always limited, and the other attributes of a TC String constitute stable, low-entropy metadata data laid out in a fixed order (e.g., the language in which the information was presented or the day where the user preferences were expressed/updated).

Finally, the TC String does not encapsulate any special categories of personal data or personal data relating to criminal convictions and offenses. Indeed, even if the TC String can be used for recording user's choices for purposes that are not covered by the TCF or for vendors that are not participating in the TCF, the TCF is not intended nor has it been designed to facilitate the lawful processing of special categories of personal data or data relating to criminal convictions, and should therefore never be used to engage in these more strictly regulated processing activities.

Therefore, the nature of the personal data in question is not sensitive in any way.

Is it data that people are likely to consider particularly 'private'?

No. Given the description provided in response to the previous question - no.

Are we processing children's data or data relating to other vulnerable people?

Not specifically, we cannot see if the individual expressing their choices in the form of TC string is a child. So, we have no means to determine if the TC String comes from a child; as webpages are visited (apps are used) by both children and adults, it is fair to assume that some of the visits will be from children. However, because of the nature of our processing, there is no reason to argue that any special processes should be adopted in those cases.

Is the data about people in their personal or professional capacity?

Not specifically, we cannot see if the person expressing their choices in the form of a TC string is doing so in

their personal or professional capacity. Thus, we cannot determine whether the TC string comes from a person acting in their personal or professional capacity; it is fair to assume that some visits will come from them. However, because of the nature of our processing, there is no reason to argue that special procedures should be adopted in these cases.

Is any of the data particularly sensitive or private?

No. The data relates to consent to process data for specific purposes and does not itself relate to "data particularly sensitive or private".

2) Reasonable expectations

The availability of privacy notice and transparency is an essential factor in determining the data subject's reasonable expectations.

In the context of this TC String processing, the TCF Policies prescribe a minimum amount of information that has to be disclosed in the CMP UI to the data subject:

1. Name of the purpose, description, and illustration

NAME	SAVE AND COMMUNICATE PRIVACY CHOICES
USER-FRIENDLY TEXT	The choices you make regarding the purposes and entities listed in this notice are saved and made available to those entities in the form of digital signals (such as a string of characters). This is necessary to enable both this service and those entities to respect such choices.
ILLUSTRATION(S)	When you visit a website and are offered a choice between consenting to the use of profiles for personalized advertising or not consenting, the choice you make is saved and made available to advertising providers so that advertising presented to you respects that choice.

2. Information about where the TC String is stored

In the files provided to publishers as required by the TCF, we provide the necessary data to explain how the TC String is stored and how long it is stored on the user's device in the CMP user interfaces they use. Such an explanation can include, for example, "the choices you make regarding the purposes and entities listed in this notice are saved in a cookie named [n] for a maximum duration of [x] months."

3. Information about the maximum retention period

We provide the maximum retention period for the data processing for each purpose so that this information can, in turn, be disclosed to end-users in CMP user interfaces.

4. Availability of an explanation of legitimate interest at stake

We provide a URL to a webpage that describes the legitimate interests we pursue when we rely on such a legal basis for at least one purpose. This information can then be provided to end-users in CMP user

interfaces. The URL directs individuals to a PDF file attached to our privacy policy page.

The four points above help us demonstrate that data subjects are adequately informed about how their data may be processed and that they might reasonably expect the processing that underlies TC String processing.

3) Likely impact

The potential impact of processing on the rights of data subjects must be assessed and balanced against the processing's interests. The notion of impact can encompass the various ways in which an individual may be affected, positively or negatively, by processing his or her personal data.

First, and as stated under "Part 1: Purpose test", the processing notably ensures that users' privacy choices can be respected (i.e., the giving, refusing, or withdrawing of consent by users and the exercise of their right to object) and that they do not have to make those choices again on each subsequent use of the relevant digital property. It is, therefore, evident that data subjects benefit positively from the processing first and foremost.

Second, it is crucial to identify the likelihood of any risk that could materialize due to the processing and the severity of its consequences. In the context of TC string processing, this processing does not pose any particular privacy risks to data subjects, as it merely reflects their privacy choices.

It is generally a service-specific and non-unique data point (as many users may make the same choices on any given day - see the section "Nature of the personal data" above). As a result, it does not introduce new vectors for cross-website tracking (such as fingerprinting). Therefore, the TC String processing does not entail any heightened privacy risks for data subjects; instead, it embodies the principle of data minimization, as confirmed by the APD decision of February 2022.

4) Additional safeguards for rights and freedoms protection

Particular attention should be given to additional safeguards to protect the interests or rights and freedoms of data subjects, prevent personal data from being misused, and limit undue impact on data subjects. For example, this has to be assessed on a case-by-case basis through technical and organizational measures.

TCF Compliance programs

IAB Europe operates Compliance Programs[3] for CMPs and Vendors to protect the integrity of the Transparency and Consent Framework ("TCF") and ensure that organizations that have signed up to the TCF comply with their commitments under the TCF Policies.

Although the businesses subject to the TCF are responsible for its correct implementation and, ultimately, compliance with the EU's data protection framework, the TCF Compliance Programs help us demonstrate that the dedicated procedures that apply to us effectively limit the possibility of misuse of TC Strings.

Indeed, IAB Europe regularly monitors our live installations and investigates reports of non-compliance from end-users or other third parties. This includes verifying that TC Strings are created adequately to faithfully represent the privacy choices made by end-users in the CMP user interfaces and are forwarded without any modification or falsification.

Where our live installation is found to be tampering with TC Strings, we receive a formal suspension notice via email and are immediately suspended from the TCF for a minimum of four weeks until the issue is

[3] https://iabeurope.eu/tcf-compliance-programmes/

resolved. A public notification of non-compliance is also sent to other TCF participants and published on IAB Europe's website[4].

Our own organizational and technical measures

We have considered appropriate safeguards and protection concerning the processing adapted to our specific circumstances. Such measures can include, but are not limited to:

1. Technical, administrative, and physical safeguards for securing the data (e.g., the use of encryption technologies for storing the data);
2. Internal policies and procedures that document such measures or at least the type of safeguards to be implemented in any project, initiative, or technical solution that relates to the collection and use of TC Strings, as well as any use of data based on privacy choices;
3. Equivalent external policies and procedures when working with a supplier;
4. Due diligence and audits performed internally and externally (e.g., assessment of partners to which we forward the data and live monitoring of our technical integration with them);
5. Appointment of the Gemius' Group Data Protection Officer to supervise GDPR compliance;
6. Implementation of an ISO 27001-compliant Information Security Management System (ISMS) to ensure systematic management of sensitive data and continuous improvement of security practices;
7. Regular risk assessments and threat modeling exercises to identify potential vulnerabilities in data processing activities and implement appropriate countermeasures;
8. Data access control measures, including role-based access controls (RBAC) and, where necessary, multi-factor authentication, to ensure that only authorized personnel can access sensitive data;
9. Employee training programs on GDPR and data protection best practices, ensuring that all staff members are aware of their responsibilities in safeguarding personal data;
10. Incident response and breach notification procedures, which include timely detection, reporting, and mitigation of data breaches, in compliance with GDPR Article 33;
11. Regular data retention and deletion reviews to ensure that personal data is not kept longer than necessary, aligning with GDPR's data minimization principle;
12. Contractual safeguards with third-party processors, including Data Processing Agreements (DPAs) that stipulate security obligations and ensure that all parties involved in data processing maintain compliance with GDPR requirements.

[4] See procedure n°1 in the controls catalogue: https://iabeurope.eu/wp-content/uploads/Controls-Catalogue-TCFv2.2.pdf

Compelling legitimate interest demonstration[5]

In the context of processing TC String, we justify, as described below, rejecting possible objection requests after a TC String has been created and received due to certain technical and practical imperatives that cannot be avoided.

Justification for Mandatory TC String Creation

First, creating a TC String without giving users the possibility to object is justified to ensure the appropriate recording of users' privacy choices. To illustrate, not creating a TC String would merely lead to permanent solicitations of user choices and requests to create a TC String each time a digital property is accessed. Such an approach would likely raise other issues, considering that the EDPB has taken a very negative view of "continuous prompting" in its "dark patterns" guidelines.

Accountability Principle and TC String Processing

Second, processing TC Strings without allowing users to object is justified under the controller's required compliance with the accountability principle in GDPR Art. 5(2). Indeed, information must be stored in relation to users' privacy choices to respect them, regardless of the user's specific choices, including their refusal of consent.

Minimized Privacy Risks in TC String Handling

Third, the processing of TC String does not create any heightened privacy risks for data subjects. The TC String embodies the principle of data minimization and cannot mechanically be used for purposes other than saving, communicating, and respecting users' privacy choices. Users can, moreover, always choose to delete any TC Strings saved on their device if they so desire - and then receive another prompt the next time they visit the relevant website, which further reinforces the validity of invoking such compelling legitimate grounds.

The three points above demonstrate that rejecting possible objection requests during a certain period after a TC String has been created and received is justified.

[5] Where legitimate interests are relied upon as legal ground for processing, Art. 21 GDPR provides for the right for data subjects to object. However, that same article then states that "[t]he controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims".

Our decision: Can we rely on legitimate interests for this processing?

Yes.

We believe processing the users' privacy choices in TC Strings is permitted under the lawful basis of legitimate interests. Moreover, in the context of the "Compelling legitimate interest demonstration" section, we believe it is justified to reject possible objection requests after a TC String has been created and received.

Date: July 1, 2024	Initial version (1.0)
Date: August 12, 2024	The document has been expanded to include additional questions, ordering corrections have been made (table of contents), communication style has been changed (1.1)