Practical guide to carrying out a Legitimate Interest Assessment (LIA) in connection with Special Purpose 3

About this guide

The purpose of this document is to provide a practical guide to carrying out a Legitimate Interest Assessment (LIA) for companies that may process TC Strings in the context of their implementation of the Transparency & Consent Framework (TCF). It is specifically aimed at vendors that intend to declare Special Purpose 3 ("Save and communicate privacy choices").

The CJEU ruling in the case C-604/22 (IAB Europe vs APD) establishes that the TC String may constitute personal data from the perspective of IAB Europe if it can be associated with other data points that may make it possible to identify the individual concerned and if IAB Europe has reasonable means allowing it to identify a particular natural person from a TC String. The reasoning from the CJEU can therefore be applied by TCF participants when assessing the nature of the information they collect and process, in particular to assess whether the TC String as well as other data points could be considered personal data from their perspective when associated with identifiable information.

For TCF participants that determine that the TC String under those circumstances constitutes personal data from their perspective, the TCF purposes taxonomy provides TCF participants with the ability to declare Special Purpose 3 ("Save and communicate privacy choices"). Such declaration is subject to the TCF participant having conducted and documented a legitimate interest assessment for their processing of personal data for this purpose, and that the assessment has shown that data subjects' interests and fundamental rights do not override the legitimate interests pursued by the TCF participant.

This document has therefore been elaborated to support TCF participants in conducting their own objective analysis when they intend to pursue this particular processing under the legitimate interest legal basis. It breaks down the various assessments that they should carry out for each part of the "three-part test" that is required to demonstrate and document that legitimate interests apply.

Each TCF participant remains responsible for ensuring that it complies with all the legal requirements associated with processing personal data on the basis of its legitimate interests, notably by conducting their own LIA based on the specific context and circumstances of their processing.

Indeed, the fact that the TCF policies cover the possibility for vendors to declare that they are relying on their legitimate interests for the TCF Special Purpose 3 should not be taken as an indication or guarantee that it is always lawful to do so in any particular instance.

Once a vendor has completed its LIA and if the outcome confirms that the legitimate interests basis applies, it should keep a written record of the LIA to help demonstrate compliance, in line with its accountability obligations under GDPR Articles 5(2) and 24. Each vendor should ensure that its LIA is sufficiently detailed and descriptive so that its reasoning is clear and comprehensible to others (for example the competent Supervisory Authority, should they need to review it).

The LIA must also be maintained, and should be reviewed periodically to ensure it remains current, and be updated when circumstances change.

Part 1: Purpose test

The purpose test serves to identify appropriately the purpose of the processing and assess whether there is a legitimate interest behind the processing.

The saving and communicating of users' privacy choices in the form of TC Strings is performed for the purpose of ensuring and being able to demonstrate that users have consented to or not objected to the processing of their personal data, for various purposes and/or vendors.

Although the concept of 'interest' is closely related to the concept of 'purpose', the 'purpose' constitutes the specific reason of the processing while the interest is the broader stake that a controller or other third parties may have in the processing (i.e. the benefit that the controller or other third parties derive from the processing)[1].

In the context of Special Purpose 3, various interests may be identified as benefiting several categories of stakeholders:

1) 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.
2) The processing ensures that TCF participants are able to retrieve and observe those choices.
3) The processing contributes to demonstrating compliance with the accountability principle pursuant to Article 5(2) of the GDPR by TCF participants.
4) The processing can support Data Protection Authorities in their investigations and audits of TCF participants, in particular to verify that users' privacy choices are appropriately respected.

Such interests, in line with Recital 47 of the GDPR and also supported by Opinion 06/2014 of the Article 29 Working Party[2], may be considered to be legitimate.

Additionally, this assessment concords with the Belgian Data Protection Authority's (APD) reasoning in their decision of February 2022 against IAB Europe and the 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.*"

[1] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[2] See footnote 1

Part 2: Necessity test

The necessity test serves to assess carefully whether the processing is actually necessary for the purpose you have identified in the first part (purpose test).

This implies demonstrating that the processing is necessary for the achievement of the purposes pursued, and in particular, that the same result cannot reasonably be achieved by other means without processing personal data and/or by processing less personal data.

1) Is each element of the data processed necessary for the purpose and interest?

In the context of the processing of TC String, it is as a first step important 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[3]:

1) General metadata: standard markers that indicate details about the Publisher's implementation of the TCF (e.g. the ID of the CMP that is used, the language of the UIs, whether the UIs use non-standard texts, such as custom stacks or illustrations) and a day-level timestamp of when users have made/updated their choices.
2) The user's consent per purpose and per vendor when the legal basis is Consent ("1" meaning user's consent and "0" meaning user's refusal or withdrawal of consent)
3) The user's right-to-object per purpose and per 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)
4) 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.
5) 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 achieve the intended purpose of saving, communicating and observing users' privacy choices.

[3]See:https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md

This 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' defences, the Litigation Chamber has not been able to establish that the TC String is retained indefinitely.*"

The method for capturing users' privacy choices in the form of a TC String is also aligned with the French Data Protection Authority's (CNIL) recommendation on cookies and other trackers[4]. Indeed, the regulator recommends that users' privacy choices be recorded in the form of a boolean value for each purpose. The existence of non-binding guidance issued by Data Protection Authorities encouraging controllers to adopt the same method of processing to achieve the intended purpose is an important consideration for the LIA.

2) Is the operation (or set of operations) performed on the data necessary for the purpose and interests?

As a second step, TCF participants should evaluate on a case-by-case basis their own method for retrieving and processing TC Strings, in light of the flexibility provided by the TCF Technical Specifications. This is to ensure that the various methods they may choose to adopt are strictly necessary for achieving the intended purpose. Elements that participants may want to consider when performing this assessment are:

- How does the participant retrieve the TC String?
- How does the participant verify that the TC String originates from a CMP participating in the Framework?
- How does the participant verify that it has established a legal basis, for each Purpose, on the basis of the TC String?
- How does the participant disclose/forward the TC String to another participant and/or entity?

For example, a TCF vendor that has access to the CMP API (and therefore is able to execute javascript) and that does not subsequently share personal data with other entities might not need to retrieve the entire TC String. Instead, such a vendor might be able to use the relevant CMP API commands to check only parts of the TC String that are strictly necessary to achieve the purpose of observing users' choices.

[4] https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf

3) Are the periods of retention for the data justified?

As a third step, TCF participants should carefully consider whether the retention policy they have in place for the storing of TC String complies with the storage limitation principle.

The keeping of TC Strings beyond the period during which they are actually needed increases the risk that the processing might be deemed excessive. For this reason, it is better to ensure that TC Strings are erased once they cease to be needed for the relevant purpose (a TC String might for instance cease to be relevant if beyond a certain period of time that TC String is considered to no longer reflect users' choices).

Part 3: Balancing test

The balancing test serves to weigh the individual's rights and freedoms against the purpose and legitimate interest identified. The balancing must consider the whole context of the processing, in particular the nature of the legitimate interests identified on the one hand and the impact on the individuals on the other hand. It should also take into account the safeguards implemented by the controller for the processing.

1) Nature of the personal data

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

In the present case, the TC String is a string of characters that represent 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 exact 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 offences. 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[5], and should therefore never be used to engage in these more strictly regulated processing activities.

The nature of the personal data in question is therefore not sensitive in any way.

2) Reasonable expectations

The availability of notice and transparency is an important factor that bears on the data subject's reasonable expectations.

In the context of Special Purpose 3, the TCF Policies prescribe a minimum amount of information that has do 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 in order 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 personalised 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

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. Such an explanation can include for

[5] See Preamble (iv) of the TCF Policies:
https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

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) For each vendor, information about their maximum retention period

As a reminder, a Vendor must provide for each purpose the maximum retention period for the data processing so that this information can in turn be disclosed to end-users in CMP UIs. Vendors that intend to declare Special Purpose 3 are advised to ensure that the information they provide is therefore accurate.

4) For each vendor, availability of an explanation of their legitimate interest at stake

As a reminder, a Vendor must provide a URL to a webpage that describes the legitimate interests they pursue when they rely on such a legal basis for at least one purpose so that it can in turn be provided to end-users in CMP UIs.

This URL can direct to a part of their privacy policy, accessed through a bookmark on that webpage. Vendors that intend to declare Special Purpose 3 are advised to review concomitantly the user-facing information about their legitimate interests at stake, in order to make sure that it includes a description of the legitimate interest relied upon when pursuing Special Purpose 3.

The four points above may help TCF participants demonstrate that data subjects are adequately informed about how their data may be processed and that they might reasonably expect the processing that underlies Special Purpose 3. Additionally, the TCF Policies always allow TCF participants to provide more information, for example directly in the various layers of the CMP or as part of their privacy policies.

3) Likely impact

The potential impact that the processing can have on data subjects' rights has to be evaluated and balanced against the interests of the processing. The notion of impact can encompass the various ways in which an individual may be affected - positively or negatively - by the processing of 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 important to identify the likelihood of any risk that could materialise as a result of the processing, as well as the severity of its consequences. In the context of the Special Purpose 3, the TC String itself does not present any particular privacy risks for data subjects, as it merely reflects their privacy choices.

It is moreover generally a service-specific and non-unique data point (as it is entirely possible that a multitude of users make the same choices on any given day - see "Nature of the personal data" above). It does not as a result introduce new vectors for cross-website tracking (such as fingerprinting). Additionally, Special Purpose 3 does not cover such processing activities, which are separately covered by Special Feature 2 and for which users are always given the choice to opt-in. Therefore, the processing does not entail any heightened privacy risks for data subjects; instead, it embodies the principle of data minimisation, as confirmed by the APD decision of February 2022.

4) Safeguards

Special attention should be given to additional safeguards aimed at protecting the interests or rights and freedoms of data subjects, preventing personal data from being misused and limiting undue impact on data subjects. This has to be assessed on a case-by-case basis for example through technical and organisational measures.

1) TCF Compliance programmes

IAB Europe operates Compliance Programmes[6] for CMPs and Vendors in order to protect the integrity of the Transparency and Consent Framework ("TCF") and ensure that organisations who have signed up to the TCF comply with their commitments under the TCF Policies.

Although the responsibility for correct implementation of the TCF, and ultimately compliance with the EU's data protection framework, lies with the businesses that are subject to it, the TCF Compliance Programmes can help TCF participants in demonstrating the dedicated procedures that apply to them effectively limit the possibility to misuse TC Strings.

Indeed, IAB Europe regularly monitors TCF participants' live installations and also investigates reports of non-compliance from end-users or TCF participants - including to verify that TC

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

Strings are created adequately to faithfully represent the privacy choices made by end-users in the CMP UIs, and are forwarded without any modification or falsification.

Where a TCF participants' live installation is found to be tampering with TC Strings, the participant receives a formal suspension notice via email and is immediately suspended from the GVL or CMP list for a minimum of 4 weeks and until the issue is resolved. Additionally, a public notification of non-compliance is sent to other TCF participants and published on IAB Europe's website[7].

2) TCF participants' own organisational and technical measures

Each TCF participant should ensure they have considered appropriate safeguards and protection in relation to the processing that are adapted to their specific circumstances.

Such measures can include, but are not limited to:

- Technical, administrative and physical safeguards for securing the data (e.g. the use of encryption technologies for storing the data);
- 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 on the basis of privacy choices;
- Equivalent external policies and procedures when working with a supplier;
- Due diligence and audits performed internally and externally (e.g. assessment of partners to which you forward the data and live monitoring of your technical integration with them)

Compelling legitimate interest demonstration

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".

In the context of the processing of TC String, it may be possible for participants to formalise the grounds that justify rejecting possible objection requests during a certain period of time after a

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

TC String has been created and/or received, due to certain technical and practical imperatives that cannot be avoided.

First, the necessity of creating a TC String without giving the 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 moreover likely raise other issues, given that the EDPB has taken a very negative view of "continuous prompting" in its guidelines on "dark patterns"[8].

Second, the necessity of processing TC Strings without giving the users the possibility to object is justified in the context of the controller's required compliance with the accountability principle pursuant to GDPR Art. 5(2). Indeed in practice, information must be stored in relation to users' privacy choices in order to respect them, irrespective of which choices precisely the user makes, including their refusal of consent.

Third, the processing of TC String does not create any heightened privacy risks for data subjects. The TC String embodies the principle of data minimisation and cannot mechanically be used for other purposes than saving, communicating and respecting users' privacy choices. Users can moreover always choose to delete any TC Strings saved on their own 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 may help TCF participants demonstrate that it is justified to reject possible objection requests during a certain period of time after a TC String has been created and/or received. However, nothing prevents a TCF participant from providing and exercising a data subject's right to object outside of the Framework taking into account their own imperatives.

[8] https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf