DRAFT RECOMMENDATION

concerning session replay tools

This content is a courtesy translation of the original publication in French. In the event of any inconsistencies between the French version and this English translation, please note that the French version shall prevail.

Document submitted for public consultation ***until 22 April 2026***

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Table of Contents

1. Introduction

1. Session replay tools are technologies that capture and visualise the user end-to-end journey on a website or mobile application user. In addition to collecting information about the pages or screens visited, they allow you to view all browsing actions, such as mouse movements, clicks or touch interactions, page scrolling, user input and other interactions.
2. These tools are used by website and mobile application publishers as they enable detailed analysis of user navigation. By replaying users' navigation journeys, operators obtain detailed data that helps explains browsing paths. This data is used to adress specific use cases (e.g. detecting and understanding errors or technical problems) as an alternative to more traditional measures (e.g. audience measurement or "*analytics*" tools).
3. **The use of these tools may present certain risks**. On the one hand, they can lead to permanent tracking of browsing, providing accurate information about people's private lives (habits, interests, sensitive data in some cases, etc.). On the other hand, they can lead to excessive data collection that does not meet the requirement of proportionality with regard to the initially intended purpose. The level of risk generally depends on the nature of the website or mobile application visited.
4. These risks are all the more significant given the wide range of business models involving the marketing of session replay tools offering a variety of features and settings. This diversity increases the choices available to website and mobile application publishers and contributes to sustaining a rapid pace of technical evolution for these tools. As a result, publishers may be incentivised to make use of features and settings that would enable them to access more information about users' navigation journeys.
5. The CNIL therefore considers it necessary to regulate the growing use of session replay solutions. The draft recommendation sets out practical recommendations to providers offering these tools and to publishers using them in order to ensure compliance with applicable regulations. This draft recommendation is not exhaustive and does not have a binding or regulatory nature. Its sole purpose is to assist the professionals concerned in their compliance efforts. It was developed following a consultation phase with representatives of the professions concerned by the use of these tools, on the one hand, and representatives of civil society, on the other.

2. Applicable legal framework

6. Firstly, session replay tools involve trackers that enable the reading and writing of information, to which the principles and obligations set out in Article 82 of Law No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties ("Data Protection Act"), which transposes Article 5.3 of Directive No. 2002/58/EC, known as the "Privacy and Electronic Communications Directive".
7. **Secondly**, these tools reconstruct individual browsing sessions: they enable the collection of data that directly or indirectly identifies users, regardless of their configuration and settings. Such processing operations, based on data produced or collected via a tracker (also known as "subsequent processing"), must comply **with the General Data Protection Regulation (GDPR) and the Data Protection Act.**

3. Scope of the draft recommendation

3.1 Technological environments concerned

8. Session replay tools make it possible to track users' navigation on a website or mobile application. These tools rely on trackers (which may be cookies in the context of the web, or other technologies such as mobile identifiers within mobile applications). They enable the visualisation of **reconstructed sessions,** either from data on interactions with a website or mobile application, or through the playback of recordings **of** browsing **sessions**.

3.2 The qualifications of the parties concerned under the GDPR

9. This recommendation applies to website and mobile application publishers and providers of session replay tools established in France or within the territory of European Union, or to those processing personal data relating to individuals located within the European Union in accordance with Article 3(1) and (2) of the GDPR and the relevant provisions of the French Data Protection Act. Each of these parties must determine their role in relation to the processing carried out.

The provider of session replay tools

10. This is the company that provides the **technical solution** for session replay. It defines the settings available within the tool provided to publishers. The qualification of this actor depends on the purposes it pursues in conjunction with the nature of the data generated by the tool:

    - when it provides the tool to the publisher without reusing the data collected for its own purposes, the supplier acts as **a processor**;
    - **if the provider, with the publisher's consent, uses the data collected by the tool for its own purposes** (e.g. to improve the solution provided), it is solely **responsible for the processing within the meaning of the GDPR** with regard **to such subsequent processing**. The supplier is also a joint controller **with the publisher** for the reading and writing operations that give rise to such processing[1] .

      In accordance with Article 26 of the GDPR, this relationship requires a clear and transparent allocation of obligations, particularly with regard to informing data subjects and respecting their rights.

The website or mobile application publisher

11. The publisher refers to the entity (company, public body, etc.) that chooses to use a session replay tool on its website or mobile application. **They are generally considered to be the data controller** because they decide to use a tool that is designed to meet their own specific needs. They therefore determine the purpose(s) of the processing and, by configuring the tool, they participate in determining the essential means of processing.
12. The publisher is solely responsible for the reading and writing operations carried out exclusively on its behalf, i.e. those enabling the collection of data that is then processed solely for its purposes.

[1] This joint responsibility is in line with the Fashion ID case law (§101 and 102) and the guidelines on the application of Article 82 of the amended Act of 6 January 1978 to read and write operations on a user's terminal (§38).

Example

Company A (the solution provider) provides a session replay solution as software as *a service* (SaaS) to Company B (the publisher) so that the latter can detect technical problems on its website. Company A plans, with the contractual agreement of Company B, to use the browsing data collected to improve the functioning of its tool. The respective qualifications are distributed as follows:

- **With regard to the processing carried out by company B for the purpose of detecting technical problems on its website :** the publisher is the data controller and company A is the data processor ;
- **With regard to the processing carried out by company A to improve its services :** company A is responsible for independent processing because it is processing for its own purposes ;
- **With regard to the reading and writing operations carried out for data collection**: given that the data collected in this way serves the purposes of both companies, they act as joint controllers for these operations.

4. Purpose(s) of the processing

13. Session replay tools can be used for different purposes, which must be **determined, explicit and legitimate**.
14. They must be defined by the data controller (publishers or suppliers) **prior to the deployment of the tool**. They cannot be determined after the data has been collected, nor **can they depend on what the data controller** is able to view using the tool.
15. The tool may be deployed by publishers on their websites or mobile applications for the following purposes:
    - **detecting and understanding errors or technical problems:** viewing individual navigation sessions makes it possible to identify technical errors and resolve them using browsing data obtained in real-life situations that cannot be detected using conventional analysis metrics;
    - **improving the user experience (UX)**: viewing individual navigation sessions refines knowledge of the user journey by revealing behaviours that cannot be detected trough conventional analysis metrics and enables the identification of friction points (rage clicks, misclicks, etc.), smoother navigation and improved ergonomics of the website or application;
    - **support and assistance in managing customer requests (or issues with services provided)**: replaying sessions specific to a user who has encountered a problem during navigation enables the data controller to better respond to requests they are likely to receive (for example, when a user who is unable to validate their order contacts customer service).
16. Depending on the purpose(s) pursued, particular attention must be paid to **the configuration of the tool:** the choice of features depends on each purpose.
17. The data controller who uses a session replay tool for purposes other than those identified in this recommendation must ensure that such use complies with the regulations.

In accordance with the principle of minimisation (Article 5.1.b of the GDPR), and in view of the risks inherent in session replay, the data controller should favour the use of alternative tools that process less data, if they enable the same objectives to be achieved. For example, a session replay tool should not be used for retargeting advertising purposes, given the existence of more privacy-friendly solutions (e.g. "shopping basket" reminder cookies).

5. Information and consent

18. Information is one of the conditions for the lawfulness of informed consent (Articles 4.11 and 6.1.a of the GDPR). Data controllers must be particularly vigilant on this point, especially since the functioning of cookie and tracker technologies is often little known to the general public, who cannot always detect their use.

5.1 The need for consent in accordance with Article 82 of the French Data Protection Act

19. Unless exempted, the reading and writing of any information stored or accessed in terminal equipment requires the collection of consent. The purposes pursued by the deployment of session replay tools are subject to the prior consent of users. Indeed, reading and writing operations:
    - are not exclusively intended to enable or facilitate electronic communication;
    - are not strictly necessary for the provision of the services offered by publishers, as these services could be provided without them.
20. This consent must be obtained under the conditions set out in Article 2 of the Guidelines[2] and Article 2 of the Recommendation on cookies and other trackers[3], subject to the specific recommendations set out below.

5.2 Practical methods for obtaining consent

Use of tools already deployed to obtain consent

21. User consent can be obtained through consent management platforms (CMPs) deployed by publishers on their websites or applications. Where necessary, these platforms must be updated to comply with the requirements of applicable positive law, as set out in the following recommendations.
22. Data controllers must ensure that the information and consent collection documents they make available to data subjects (cookie management module, dedicated information notices, CMP, etc.) are updated, in accordance with their obligations under Articles 13 and 14 of the GDPR. By way of reminder, where none of the exemptions provided for in Article 82 of the French Data Protection Act are applicable, users must receive information in accordance with this article, supplemented where relevant by the requirements of the GDPR (data recipients, retention periods, etc.).

[2] Deliberation No. 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978 and on read and write operations on a user's terminal (in particular "cookies and other trackers") and repealing deliberation no. 2019-093 of 4 July 2019.

[3] Deliberation No. 2019-093 of 4 July 2019 and in deliberation No. 2020-092 of 17 September 2020 adopting a recommendation proposing practical compliance measures in the event of the use of "cookies and other trackers".

Information required to obtain informed consent

23. Each purpose for which the tool is deployed must be presented to users, before they are asked to give or withhold their consent, in a short label accompanied by a brief description that enables them to understand the scope of their choice. For example, for the purposes presented above, the second level of information in the CMPs, in accordance with the requirements governing the collection of consent, is intended to include the following information:

    - **Detection and understanding of errors or technical problems:** *[Publisher name] uses trackers (user journey recording tools) to identify technical errors and resolve them.*
    - **Improvement of the user experience ("UX"):** *[Publisher name] uses trackers (user journeys recording tools) to identify areas of friction in the browsing journey in order to streamline navigation and improve the ergonomics of the website [or application].*
    - **Support and assistance in managing customer requests (or issues with the services offered):** *[Publisher name] uses trackers (user journey recording tools) to reproduce the session(s) of certain users who have encountered a problem while browsing [the site] / [the application], in order to respond to requests that the [Publisher name] teams may receive.*

Specific information about session replay tools

24. As a good practice, the CNIL encourages data controllers to provide specific information about session replay tools on the first level of the CMPs.

25. These tools present certain risks, and users of websites or mobile applications have little knowledge of their existence and how they operate. Each data controller therefore assesses, in light of their own situation, whether to implement this good practice so that the consent given is fully informed. The decision on whether or not to display this information on the first level of the CMPs must take into account the extent of the navigation tracking carried out, the impact on users, and the settings and minimisation measures implemented.

26. This information should present the tool and explain how it works (e.g. the data that is collected and processed, the settings applied to it, etc.), so that users are truly able to understand why their consent is required when they visit a website or use a mobile application.

5.3 Implementation of subsequent processing by the publisher

27. "Subsequent processing" refers to the processing that results from the data generated by cookies and other trackers.

28. While the principle is that consent must be obtain prior to any reading or writing of information on a terminal, the processing of personal data collected from these trackers must be based on one of the legal grounds provided for in Article 6 of the GDPR.

29. Consent is generally the most appropriate legal basis for this subsequent processing, but each data controller must determine, based on the context and its specific characteristics, which legal basis is appropriate to use. Where the legal basis for subsequent processing is also users' consent, the data controller may collect it at the same time as it collects consent for storage and/or reading operations, for example by means of a single checkbox for each of the purposes.

5.4 Further processing of data

30. "Further processing" refers to the processing defined in Article 6.4 of the GDPR.

31. Data collected through reading and writing operations subject to user consent may only be reused for another purpose if the user has given their consent to this new purpose.

32. However, reuse by the data controller does not require consent if the data has been anonymised beforehand. Indeed, the reuse of anonymised data is not considered to constitute an additional infringement of individuals' privacy, in view of the protection afforded by Article 82 of the Data Protection Act.

Proof of consent

A data controller must be able to demonstrate at any time that users have given their consent. To do so, it must put in place mechanisms to demonstrate that users' consent has been validly obtained.

For "cookies and other trackers", the CNIL considers that actors who rely on the consent given by the user may limit themselves to providing proof of the process, given the specificities of the environment.

Paragraph 48 of the "cookies and other trackers" recommendation provides examples of mechanisms that operators can adopt.

These various consents may be obtained via the CMP deployed on the publisher's website, regardless of the purposes (those pursued by the publisher or those pursued by the provider).

When stakeholders are jointly responsible for collecting these consents, they cannot be satisfied with the presence of a contractual clause that solely imposes on the publisher the obligation to collect valid consent on behalf of the other party.

The contract should therefore specify:

- The mechanisms put in place to demonstrate that valid consent has been obtained and who is responsible for this.
- The provision of evidence to the organisation wishing to rely on the consent.
- Where relevant, the conditions under which this evidence must be stored, in particular in order to preserve its probative value.
- The terms and conditions for regular audits of the consent collection mechanisms.

6. Exercise of individual rights

6.1 General

33. Users benefit from rights that are guaranteed in particular by Articles 15 to 20 of the GDPR: right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability, etc. Data controllers must facilitate the exercise of these rights by providing users with user-friendly and comprehensible mechanisms, such as a rights management centre (see the CNIL's design recommendations).

6.2 Consequences of withdrawing consent

34. Users must be able to withdraw their consent at any time (Article 7 of the GDPR). Withdrawing consent must be as easy for them as giving it was.

35. Data controllers must ensure that withdrawal of consent is effective: reading and writing operations may no longer take place after the user withdraws consent. It may be necessary to implement specific solutions to ensure that previously used trackers are not read so that the withdrawal of consent is considered effective (e.g. modifying the lifetime of cookies to indicate that they have expired by returning an appropriate "set cookie" header in an HTTP response specifying an expiry date in the past, or, in the case of cookies that do not have the "httpOnly" attribute, ensuring their deletion using a script executed locally on the terminal, etc.).

7. Implementation of data protection principles

36. **The configuration of session replay tools must enable publishers to comply with the principles of minimisation, storage limitation and security of personal data processing.**

37. Publishers **must choose providers whose session replay tools enable them to comply with their obligations.**

38. Providers must offer a configurable tool that allows their customers to take into account regulatory requirements and the diversity of purposes for which they may be used.

39. The CNIL therefore recommends that providers implement a series of measures which, when made available to publishers, support compliant deployment.

40. These measures are not mandatory, and alternative actions may be implemented insofar as they enable data controllers to comply with the regulations. In such cases, data controllers must be able to document, with the help of their provider, how the alternative actions meet their obligations.

Selection of relevant measures according to the purposes pursued

To guide stakeholders, the CNIL provides a table in the appendix indicating the technical measures recommended.

For each purpose covered by the recommendation, the tablesets out a series of measures to be applied cumulatively or alternatively (described below) to ensure the use of session replay tools is consistent with regulatory principles. It is also the role of the solution provider, acting as a processor**, to advise the data controller on the selection of relevant measures.**

7.1 Ensuring compliance with the principle of minimisation

41. Data **must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Article 5.1.c of the GDPR).**

42. In this regard, the CNIL recommends **limiting the sessions collected** according to the purpose pursued using the following features:

- Random sampling of sessions collected to limit the amount of data collected (*L1*).

- Limiting collection to situations where a defined triggering event occurs. In situations where a session history is necessary, and cannot be obtain by other means, it is possible to recording all sessions may be envisaged, provided that recordings are deleted shortly thereafter if no predefined triggering event has occurred (*L2*).
- Analysis of recorded sessions and prompt deletion of sessions that are not necessary for the purpose of the processing (e.g. deletion of sessions if it is established that the user did not encounter any navigation difficulties) (*L3*).

43. In addition, the CNIL recommends that **a masking tool** be made available systematically **in order to limit the nature of the data made available to the publisher** to what is necessary for the intended purpose: the provider should supply appropriate tools to automatically and manually select the data that should not be made available, in particular images, forms, text fields and dynamically filled fields (e.g. containing account information). In the absence of configuration, masking should apply by default to all categories considered (*M0*). In addition, the publisher should be able to choose the consequences of masking:
    - Data collection, with the option to request unmasking only accessible to a limited number of authorised users and an internal request validation process (*M1*).
    - Collection of data by the tool but not made available to the publisher (e.g. via provider-side encryption). Any access request must be justified (*M2*).
    - No data collection (*M3*).

44. Finally, the CNIL recommends that **the use of identifiers be limited** according to the purpose pursued. The publisher should therefore have the following features at its disposal:
    - Randomly generated session identifiers, to prevent linking different sessions of the same user or linking these sessions with a specific user account. These identifiers may have a short lifespan, allowing long sessions to be fragmented (*I1*).
    - A pseudonymous identifier specific to each user but which does not directly identify the corresponding user. Such an identifier can be created using hash functions, for example (*I2*).
    - Identifier limited to a domain to restrict the ability to match sessions from the same user across multiple domains (*I3*)

7.2 Ensuring compliance with the principle of storage limitation

45. Data must be retained for **no longer than is necessary for the purposes for which it is processed (Article 5.1.e of the GDPR).**

46. The solution provider should therefore allow the publisher to configure retention periods and deletion rules according to the purposes pursued.

47. The CNIL recommends that the provider implement a technical architecture that allows individual sessions to be deleted, particularly in cases where the retention period depends on user actions (e.g. deletion of the session following the closure of a support request) and, in any event, to comply with requests for data deletion. In the table below, the CNIL recommends retention periods based on the purposes pursued.

7.3 Ensuring compliance with the principle of processing security

48. The publisher and its subcontractors must implement **appropriate technical and organisational measures to ensure a level of security appropriate to the risk**

(Article 32 of the GDPR). In the context of session replay tools, the CNIL recommends that the publisher have the following features at its disposal:

- Blocking the collection of any passwords, banking information, or other data subject to special conditions of collection and storage due to their sensitivity and the risks associated with malicious use (*S1*).
- A tool enabling the implementation of an authorisation policy (with distinct profiles/roles/rights depending on the data concerned) and the verification of their relevance over time, as with any internal measure (periodic review, update in the event of departure/internal mobility) (*S2*).

When implementing all of these features, it is recommended that the provider always offer the most protective default settings possible, in accordance with "Data protection by default" (Article 25 of the GDPR).

8. Appendix 1

Explanation: *the purpose of this table is to enable publishers to identify, purpose by purpose, the technical measures that are recommended (and therefore that providers should offer). For each purpose covered by the recommendation, there is a series of cumulative or alternative measures (described below) that enable the tools to be used in accordance with the regulations.*

Purpose	Business need	Risk mitigation measure	Comment
Support and assistance in managing customer requests (or issues with the services offered)	Need to be able to identify the session associated with a specific identifier (provided by the customer or associated with their account) for use in the context of support.	-L2 and (M3 or M2 or M1) and (I2 or I3) and S1 and S2 -Retention period limited to a few hours after the end of the session.	-Unmasking validation: as the situation arises following contact with the user, the CNIL recommends having a validation process with the user prior to any unmasking. -The retention period should be justified in a documented manner with regard to the occurrence of support situations over time.
Improvement of the user experience ("UX")	Identification of areas of friction (rage clicks, false clicks, etc.) in order to streamline navigation and correct any UX difficulties. The visualisation of individual browsing sessions complements the aggregated analysis data because it reveals behaviours that cannot be detected using conventional analysis metrics. Requires a significant volume of data and historical depth.	-(L1 or L3) and (M2 or M3) and I1 and S1 and S2 -Retention period of a few months to focus on issues relating to the current version of the site.	-The intended purpose does not require linking a session to a user ID. -Unmasking can only be of very marginal use, which explains why the process is more complex.
Detection and understanding of errors or technical issues	Identifying errors allows us to understand the context leading to them based on navigation data obtained in real situations and not detectable using conventional analysis metrics. This requires a significant volume and average historical depth, but for a specific type of situation (occurrence of an error).	-(L2 or L3) and (M1 or M2 or M3) and I1 and S1 and S2 -retention period of a few months in order to focus on issues relating to the current version of the site.	-For this purpose, there is no justification for associating a session with a user ID. -Unmasking can be used on an ad hoc basis to identify issues caused by a specific user entry.