

Deliberation No. 2020-091 of 17 September 2020 adopting 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 (in particular "cookies and other tracers") and repealing Deliberation No. 2019-093 of 4 July 2019

The National Commission for Information Technology and Civil Liberties,

Having regard to Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Having regard to Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of 25 November 2009;

Having regard to Directive 2008/63/EC of 20 June 2008 on competition in the markets for telecommunications terminal equipment, and in particular Article 1 thereof

Having regard to Law No. 78-17 of 6 January 1978, as amended, relating to information technology, files and freedoms, in particular Articles 8-I-2°-b) and 82 ;

Having regard to Decree No. 2019-536 of 29 May 2019, as amended, taken for the application of Law No. 78- 17 of 6 January 1978 on information technology, files and freedoms;

Having regard to the decision of the Council of State n° 434684 of 19 June 2020;

Having regard to the guidelines on consent under Regulation (EU) 2016/679 adopted on 4 May 2020 by the European Data Protection Committee;

After having heard Mr François PELLEGRINI, Commissioner, in his report, and Mr Benjamin TOUZANNE, Government Commissioner, in his observations,

Adopts the following guidelines:

1. The National Commission for Information Technology and Civil Liberties (hereinafter "the Commission") is responsible for ensuring compliance with Article 82 of the aforementioned Act of 6 January 1978 (hereinafter the "Information Technology and Civil Liberties" Act).

2. In this context, the main purpose of these guidelines is to recall and explain the law applicable to the reading and/or writing of information (hereinafter "tracers") in the subscriber's or user's electronic communications terminal equipment, and in particular to the use of cookies. The legal framework results in particular from the applicable provisions of the aforementioned Directive of 12 July 2002 (hereinafter "ePrivacy Directive"),

transposed into national law in Article 82 of the "Informatique et Libertés" law, and the definition of consent established in Article 4 of the above-mentioned Regulation (EU) of 27 April 2016 (hereinafter "RGPD"), which the above-mentioned guidelines of the European Data Protection Committee (EDPS) are intended to clarify.

3. Article 82 of the French Data Protection Act states:

"Any subscriber or user of an electronic communications service must be informed in a clear and comprehensive manner, unless previously informed, by the controller or his representative:

1° The purpose of any action to access, by electronic transmission, information already stored in his or her electronic communications terminal equipment, or to write information into that equipment;

2° The means at his disposal to oppose it.

Such access or registration may only take place on condition that the subscriber or user has expressed, after having received this information, his or her consent, which may result from appropriate settings on his or her connection device or any other device under his or her control.

These provisions shall not apply if access to information stored in the user's terminal equipment or the recording of information in the terminal equipment of the user :

1° Or, has the exclusive purpose of enabling or facilitating communication by electronic means ;

2° Or, is strictly necessary for the provision of an online communication service at the express request of the user.

4. These provisions thus require consent to be obtained before any action is taken to store or access information stored in a subscriber's or user's terminal equipment, apart from the applicable exceptions.

5. The Commission recalls that the consent provided for in these provisions, read in the light of Article 5 of the ePrivacy Directive and Article 94 of the GDPR, refers to the definition and conditions provided for in Articles 4(11) and 7 of the GDPR.

6. The RGPD has clarified the conditions for obtaining consent and the need to demonstrate that it has been obtained.

7. The entry into force of the RGPD has thus led the Commission to repeal, by its deliberation No. 2019-093 of 4 July 2019, its 2013 recommendation on *cookies* and other tracers, replacing it with guidelines. The present deliberation draws the consequences of the above-mentioned decision of the Council of State of 19 June 2020 and updates these guidelines.

8. These guidelines are supplemented by non-prescriptive and non-exhaustive recommendations, including examples and good practice of how to obtain consent and how to implement tracers not subject to consent.

Article 1 - On the scope of the guidelines

9. The guidelines concern all operations aimed at accessing, by electronic transmission, information already stored in the terminal equipment of the subscriber or user of an electronic communications service or at writing information into it.

10. Article 1 of Directive 2008/63/EC of 20 June 2008 defines terminal equipment as *"any equipment which is connected directly or indirectly to the interface of a public telecommunications network for the purpose of transmitting, processing or receiving information; in both cases, direct or indirect, the connection may be established by wire, fibre optic or electromagnetic means; a connection is indirect if an apparatus is interposed between the terminal equipment and the interface of the public network"*.

11. This definition encompasses many commonly used devices, such as a tablet, a *smartphone*, a fixed or mobile computer, a video game console, a connected TV, a connected car, a voice assistant, as well as any other terminal equipment connected to a telecommunications network open to the public.

12. These guidelines apply to all terminal equipment covered by this definition, regardless of the operating systems or application software (such as web browsers) used.

13. They concern, in particular, the use of HTTP *cookies*, through which these read or write actions are most often carried out, but also other technologies such as *"local shared objects"*, sometimes called *"Flash cookies"*, *"local storage"* implemented within the HTML 5 standard, identifications by calculation of the terminal's fingerprint or *"fingerprinting"*, identifiers generated by operating systems (whether advertising or not: IDFA, IDFV, Android ID, etc.), hardware identifiers (MAC address, serial number or any other device identifier), etc. For the purposes of these guidelines, the word

"Tracer" means any device that may be covered by section 82 of the Act.

14. Finally, these guidelines concern the above-mentioned operations of reading and writing any information stored or consulted in a terminal equipment in the predefined sense, whether or not it is personal data within the meaning of the GDPR. The provisions of Article 5(3) of the ePrivacy Directive and, consequently, of Article 82 of the Data Protection Act, are indeed

applicable to such operations regardless of whether the data concerned are personal or not.

15. The Commission recalls that any processing of data produced or collected *via* a tracker, as long as they fall within the category of personal data - sometimes directly identifying (e.g. an e-mail address) and often indirectly identifying (e.g. the unique identifier associated with a *cookie*, an IP address, an identifier of the user's terminal or a component of the terminal, the result of a fingerprint calculation in the case of a "*fingerprinting*" technique, or an identifier generated by a software or an operating system) - must comply with the provisions of the RGPD and the relevant provisions of the "Informatique et Libertés" law. These processing operations are not covered by these guidelines.

Article 2 - On the modalities for obtaining consent

16. Pursuant to the combined provisions of Article 82 of the French Data Protection Act and Article 4 of the RGPD, the tracers requiring consent may, subject to the exceptions provided for by these provisions, only be used by writing or reading if the user has expressed his or her will to this end, in a free, specific, informed and unambiguous manner, by means of a declaration or by a clear positive act.

With regard to the free nature of consent

17. In order to determine whether consent is freely given, the GDPR requires *"In this regard, it is important to take the utmost account of the question whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data which is not necessary for the performance of that contract.* According to Recital 42 of the GDPR, which clarifies the requirement of freedom of consent laid down in Article 4 of the GDPR, *"consent should not be regarded as freely given if the data subject does not have a genuine choice or is not able to refuse or withdraw consent without suffering prejudice.* In these circumstances, the Commission considers that making the provision of a service or access to a website conditional on the acceptance of write or read operations on the user's terminal (the so-called "*cookie wall*" practice) is likely to infringe the freedom of consent in certain cases.

18. In the event of a "*cookie wall*", and subject to the lawfulness of this practice, which must be assessed on a case-by-case basis, the information provided to the user should clearly indicate the consequences of his or her choices, and in particular the impossibility of accessing the content or service without consent.

19. Finally, according to Recital 43 of the GDPR, *"consent shall be presumed not to have been freely given if separate consent cannot be given to different personal data processing operations even though this*

is appropriate in the case in question". In this respect, the Commission considers that the simultaneous collection of a single consent for several processing operations for different purposes (purpose matching), without the possibility of accepting or refusing purpose by purpose, is also likely to affect, in some cases, the user's freedom of choice and therefore the validity of his consent.

With regard to the specific nature of consent

20. The Commission recalls that consent to read and write operations must be specific. As such, consent to these operations cannot be validly obtained *through* a global acceptance of general terms of use.

With regard to the informed nature of consent

21. The Commission recalls that the consent of individuals must be informed in accordance, on the one hand, with the provisions of Articles 4(11), 7, 13 of the RGPD and, on the other hand, with the provisions of Article 82 of the "Informatique et Libertés" law.

22. The Commission recalls that the information must be drafted in simple and comprehensible terms and that it must enable users to be duly informed of the different purposes of the data loggers used. It considers that the use of overly complex legal or technical terminology is likely to make this information incomprehensible to users.

23. The Commission recalls that the information must be complete, visible and prominent. A simple reference to the general conditions of use is not sufficient.

24. At a minimum, the provision of the following information to users prior to the collection of their consent is necessary to ensure that consent is informed:

- the identity of the person(s) responsible for processing the read or write operations;
- the purpose of the data reading or writing operations;
- how to accept or reject the trackers;
- the consequences of refusing or accepting the tracers;
- the existence of the right to withdraw consent.

25. The Commission recalls that in order for consent to be informed, the user must be able to identify the controller(s) and all joint controllers before being able to express his or her choice. Thus, the exhaustive and up-to-date list of these entities must be made easily accessible to users.

With regard to the unambiguous nature of consent

26. The Commission stresses that, in accordance with Article 4(11) of the GDPR, consent must be given through a positive action by the person who has been informed of the consequences of his or her choice and has the means to express it.

27. It therefore considers that continuing to browse a website, use a mobile app or scroll down the page of a website or mobile app do not constitute clear positive actions amounting to valid consent. The Commission recalls that the Court of Justice of the European Union (CJEU) ruled in its *Planet 49* decision of 1 October 2019 (CJEU, 1 Oct 2019, C-673/17) that the use of pre-ticked boxes cannot be considered a clear positive act of giving consent. In the absence of consent expressed by a clear positive act, the user must be considered to have refused access to their terminal or the recording of information in it.

28. Appropriate systems should be put in place to collect consent in a practical way that allows users to benefit from user-friendly solutions. The Commission refers on this point to its Recommendation No 2020- 092 of 17 September 2020.

On proof of consent

29. Article 7.1 of the RGPD requires that the organisations operating the tracers, responsible for the processing operation(s), be able to provide, at any time, proof of the valid collection of the user's free, informed, specific and unambiguous consent.

On refusal and withdrawal of consent

30. The Commission notes that while consent must be expressed by a positive action on the part of the user, the latter's refusal may be inferred from his silence. The expression of the user's refusal must therefore not require any action on his part or must be able to be translated into an action with the same degree of simplicity as that used to express his consent.

31. Furthermore, the Commission recalls that, in accordance with Article 7.3 of the GDPR, it must be as easy to withdraw consent as to give it. Users who have given their consent to the use of trackers must be able to withdraw it simply and at any time.

Article 3 - On the qualification of actors

32. The trackers concerned by the consent requirement do not systematically involve the processing of personal data. However, in a large number of cases, the reading or writing operations will concern

personal data, the processing of which will be subject to the other provisions of the "Informatique et Libertés" law and the RGPD.

33. While in some cases the use of trackers involves a single entity which is therefore fully responsible for the obligation to obtain consent (e.g. a website publisher using trackers to personalise the editorial content offered to the Internet user), in other cases several actors contribute to the performance of the reading or writing operations referred to in these guidelines (e.g. a website publisher and an advertising agency depositing trackers when the website is visited). In the latter cases, these entities must determine their status with regard to the processing carried out.

3.1 Joint responsibility and obligations of the controller(s)

34. The Commission recalls that the publisher of a site that deposits trackers must be considered as a controller, even when it subcontracts to third parties the management of these trackers set up on its own behalf.

35. Third parties who use tracers on a service published by another organisation must also be considered as data controllers, for example by depositing tracers when visiting a publisher's site, provided that they are acting on their own behalf. In this case, the Conseil d'Etat ruled, in its decision of 6 June 2018, that the obligations of the site publisher include ensuring that its partners do not use the publisher's site to transmit data that does not comply with the regulations applicable in France, and that it must take all necessary steps to put an end to any breaches.

36. Therefore, the organisation that authorises the use of trackers, including by third parties, from its website or mobile application, must ensure that a mechanism is in place to obtain users' consent.

37. In general, the Commission notes that publishers of websites or mobile applications, because of the direct contact they have with the user, are often in the best position to inform the user about the trackers deposited and to collect his consent.

38. For Article 82 operations, as the CJEU also held in a similar case (CJEU, 29 Jul 2019, Case C-40/17, Fashion ID GmbH & Co KG v. / Verbraucherzentrale NRW eV), the publisher of the website or mobile application and the third party depositing the trackers are deemed to be jointly responsible for the processing insofar as they jointly determine the purposes and means of the read and write operations on the users' terminal equipment.

39. In the case of joint responsibility, where the controllers jointly determine the purposes and means of the processing, the Commission recalls that, in accordance with the provisions of Article 26 of the RGPD, they must define in a transparent manner their respective obligations in order to ensure

compliance with the requirements of the GDPR, in particular with regard to the collection and demonstration, where applicable, of valid consent.

3.2. Subcontracting

40. The Commission recalls that an actor who stores and/or accesses information stored in a user's terminal equipment exclusively on behalf of a third party must be considered as a processor. In this respect, it recalls that if a processing relationship is established, the controller and the processor must draw up a contract or other legal act specifying the obligations of each party, in compliance with the provisions of Article 28 of the GDPR.

41. The Commission also recalls that, in accordance with Article 28(3) of the RGPD, the processor must assist the controller in complying with certain of its obligations and in particular those relating to requests to exercise the rights of individuals.

42. Finally, the processor must inform the latter in particular if any of its instructions constitute a breach of the applicable texts on the protection of personal data.

Article 4 - On terminal settings

43. Section 82 of the Act specifies that consent may result from appropriate settings on the person's connection device or any other device under his or her control.

44. Nevertheless, at the date of adoption of these guidelines, the Commission considers, in the light of the knowledge available to it and without prejudice to possible technical developments, that the parameterisation possibilities of browsers and operating systems cannot, on their own, enable the user to express valid consent. Indeed, although web browsers offer numerous settings allowing users to express choices regarding the management of cookies and other tracers, these are generally expressed today in conditions that do not ensure a sufficient level of prior information for individuals to respect the principles recalled in these guidelines.

45. Furthermore, browsers do not currently allow for a distinction to be made between trackers according to their purpose, even though such a distinction may be necessary to ensure freedom of consent.

Article 5 - On consent-exempt trackers

46. As a reminder, the consent requirement does not apply to operations whose sole purpose is to enable or facilitate communication by electronic means or are strictly necessary for the provision of an online communication service at the express request of users.

47. Tracers only fall outside the scope of the consent requirement if they are used exclusively for one or more purposes that can be linked to the exceptions provided for in Article 82 of the French Data Protection Act.

48. In this respect, the Commission specifies that the use of the same tracer for several purposes, some of which do not fall within the scope of these exemptions, requires the prior consent of the persons concerned, under the conditions set out in these guidelines. For example, in the case of a service offered *via* a platform requiring user authentication ("*logged-in universe*"), the service provider may use a *cookie* to authenticate users without asking for their consent (because this *cookie* is strictly necessary for the provision of the online communication service). On the other hand, the service provider may only use the same *cookie* for advertising purposes if the users have given their prior consent to this specific purpose.

Tracers exempt from consent

49. On the basis of the practices brought to its attention, the Commission considers that the following tracers in particular can be regarded as exempted

- Tracers retaining the choice expressed by users on the deposit of tracers;
- Tracers for authentication to a service, including those for ensuring the security of the authentication mechanism, e.g. by limiting robotic or unexpected access attempts;
- tracers intended to keep track of the contents of a shopping basket on a commercial site or to invoice the user for the product(s) and/or service(s) purchased;
- user interface customisation trackers (e.g. for the choice of language or presentation of a service), where such customisation is an intrinsic and expected feature of the service;
- tracers for load balancing of equipment involved in a communication service;
- Tracers allowing paying sites to limit free access to a sample of content requested by users (predefined quantity and/or over a limited period);
- certain audience measurement tracers, subject to the reservations mentioned below.

Specific case of audience measurement tracers

50. The management of a website or an application almost systematically requires the use of traffic and/or performance statistics. In many cases, these measurements are essential for the proper functioning of the website or application and therefore for the provision of the service. Consequently, the Commission considers that tracers whose purpose is limited to measuring the audience of the site or application, in order to meet various needs (performance measurement, detection of navigation problems, optimisation of technical performance or

The data collected (e.g. ergonomics, estimation of the power of the servers required, analysis of the content consulted, etc.) are strictly necessary for the functioning and current administration of a website or an application and are therefore not subject, pursuant to Article 82 of the French "Informatique et Libertés" law, to the legal obligation to obtain the prior consent of the Internet user.

51. In order to limit itself to what is strictly necessary for the provision of the service, the Commission stresses that the purpose of these tracers must be strictly limited to the sole measurement of the audience on the website or application on behalf of the publisher. In particular, these cookies must not allow the overall tracking of the person's browsing using different applications or browsing different websites. Similarly, these tracers must only be used to produce anonymous statistical data, and the personal data collected may not be cross-checked with other processing or transmitted to third parties, nor are these operations necessary for the functioning of the service.

52. More generally, the Commission recalls that audience measurement processing operations are personal data processing operations that are subject to all the relevant provisions of the GDPR.

Article 6 - Repeal of deliberation no. 2019-093 of 4 July 2019

53. This resolution repeals resolution no. 2019-093 of 4 July 2019 adopting 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.

54. This decision will be published in the Official Journal of the French Republic.

The President

Marie-Laure DENIS