DRAFT RECOMMENDATION

ON THE PRACTICAL PROCEDURES FOR COLLECTING THE CONSENT PROVIDED FOR IN ARTICLE 82 OF THE FRENCH DATA PROTECTION ACT, CONCERNING OPERATIONS OF STORING OR GAINING ACCESS TO INFORMATION IN THE TERMINAL EQUIPMENT OF A USER (RECOMMENDATION "*COOKIES* AND OTHER TRACKERS")

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

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

January 14th, 2020

Makes the following observations:

1. On 4 July 2019, the Commission Nationale Informatique et Libertés (hereinafter "the Commission") adopted guidelines for the application of Article 82 of the French Data Protection Act (hereinafter the "French data protection Act"). The purpose of these guidelines was to present the legal framework applicable to storing or the gaining of access to information already stored (hereinafter "trackers") in the terminal of a user or subscriber of an electronic communications service (hereinafter "the user").

2. In order to support the professionals concerned, both from the public and private sector, the Commission has decided to supplement these guidelines with a recommendation. The purpose of this document is to describe the practical modalities for obtaining consent in accordance with the applicable rules, to propose concrete examples of user interface, and to present best practices that go beyond the legal requirements.

3. This recommendation, including the examples proposed therein, is neither prescriptive nor exhaustive, and its sole purpose is to guide the professionals concerned in their efforts to comply. Other methods of collecting consent may be used by professionals, provided that they allow consent to be obtained in compliance with the applicable law, as explained in the previously released guidelines on *cookies* and other tracking devices.

4. Moreover, as a tool to support professionals and a practical guide, this recommendation is likely to be updated and enriched in order to take into account, over time, technological developments and responses to questions expressed by both professionals and data subjects.

5. This recommendation was drawn up following a consultation with representatives of the digital advertising ecosystem as well as with representatives of the civil society.

Article 1

Scope of the recommendation

1.1 - Environments concerned

6. This recommendation takes particular account of configurations specific to web environments and mobile applications. The examples of compliant practices can however inspire and guide the development of interface in other contexts where the consent provided for in Article 82 of the "French data protection act" must be collected (connected television, video game console, voice assistant, etc.).

7. The recommendation concerns both environments in which the user is authenticated (sometimes called "*logged-in* environment") as well as "*unlogged*" ones. Indeed, the fact that the user is authenticated does not dispense with the need to obtain his or her consent in accordance with Article 82 of the “French Data Protection Act”, as long as trackers subject to consent are used.

1.2 – Concerned trackers

8. The main purpose of the recommendation is to guide professionals in the application of the rules applicable to the read or write operations subject to consent, and not those for which consent is not required. As a reminder, the consent requirement does not apply to operations whose exclusive purpose is to carry out the transmission of a communication over an electronic communications network or which are strictly necessary for the provision of an online communication service explicitly requested by the user.

9. In the light of the practices brought to the Commission's attention, the following trackers may, in particular, be regarded as exempted:

- the trackers keeping the choice expressed by the user on the use of trackers or the will of the user not to express a choice ;
- trackers intended for authentication to a service ;
- Trackers designed to keep track of the content of a shopping cart on a merchant site;
- user interface customization trackers (e.g. for the choice of language or presentation of a service), where such customization is an intrinsic and expected element of the service user;
- trackers allowing load balancing of equipment contributing to a communication service;
- Trackers allowing paying sites to limit free access to their content to a predefined quantity and/or over a limited period of time;
- trackers enabling audience measurement, within the framework specified by Article 5 of the Guidelines on *cookies* and other trackers.

10. Trackers only fall outside the scope of the consent requirement if they are used exclusively for one of the purposes set out above. A tracker loses the benefit of the exemption if it is also used for another purpose subject to consent.

11. For example, in the case of a service offered *via* a *logged-on* universe, the service provider may use a *cookie* to authenticate the user without asking for his consent (as this *cookie* is necessary for the provision of the online electronic communication service). On the other hand, it will only be able to use this same *cookie* for advertising purposes if the user has effectively consented in advance to this specific purpose under the conditions described in the guidelines on *cookies* and other trackers.

1.3- Actors concerned

12. This recommendation concerns both the trackers used by the publisher of a website or mobile application and those used by third parties. In the case of a website, the fact that the trackers are deposited *via the* domain to which the site in question belongs, or *via a* sub-domain of the same publisher, or *via the* domain of a third party, has no effect on the obligations arising from Article 82 of the "French Data Protection Act" law. The obligation to obtain consent is attached to the purpose of the tracker and not to the technical characteristics of its implementation.

13. Both publishers and third parties can be regarded as responsible for the read or write operations. The Commission points out that the controller of the processing operation(s) is the natural or legal person who alone or jointly decides on the purpose and determines the means of the read and/or write operation. This qualification is therefore likely to apply to both:

- to the publisher wishing to meet a need it has defined (e.g. to measure its audience) and appealing for this purpose:
    - to third parties who issues trackers, acting solely on his instructions and on his behalf. In this case, third parties act as subcontractors of the publisher;
    - to trackers that the publisher issues and which it manages on its own;
- to the third party to the site or application consulted by the user, which uses trackers in order to collect data for a purpose it has determined (for example, the third party offers several publishers a service to enrich the data it collects from trackers implemented on different sites or applications).

14. The Commission stresses out that the publisher of the site or mobile application whose visit triggers the deposit of trackers, and who therefore authorizes the deposit and use of trackers, including by third parties, from its site or mobile application, should ensure that a mechanism is in place to obtain the free, specific, informed and unambiguous consent of users for the operations of reading and/or writing information in the terminal, in accordance with Article 82 of the Law.

15. In general, the Commission observes that, in many cases, publishers of mobile sites or applications are in the best position to inform users of the information on deposited trackers and to collect their consent, because of the control they exercise over the interface for collecting choices and the direct contact they have with the user.

Article 2

The requirement for informed consent

16. The user must receive information in compliance with article 82 of the French Data Protection Law and where applicable, by the requirements of the GDPR, under the conditions described in the guidelines. The Commission intends to focus its practical recommendations, in particular, on the information required for the purposes, the identity of the controller(s) and the scope of consent.

2.1 - Information on the purpose of trackers

17. The purpose of the trackers must be presented to the user before he or she is given the opportunity to consent or not to consent to their use.

Practical arrangements for implementation

18. Purposes must be formulated in an intelligible manner, in a sufficiently clear and appropriate language to enable the user to understand precisely what he or she is consenting to. In order to facilitate the reading for the user, the Commission recommends that each purpose be highlighted in a short and prominent title, which would be accompanied by a brief description.

Examples of how to comply with the applicable rules

19.

- If the tracker(s) is (are) used to display targeted advertisement, this purpose can be described as follows: "**Behavioural advertising**: *[name of the site / application]*

*[and **third party companies / our partners]** use / use tracking devices to display advertisement that is customized according to your browsing behaviour and profile*".

- If the tracker(s) are only used to display the advertisement and measure its audience, without customizing it on the basis of personal data, the controller may use the following wording: "**Displaying of advertisement**: *[name of **the** site / application] [and **third party companies / our partners]** uses / use trackers to display advertisement [on the site or application], without profiling you*".

- If the advertisement is customized according to the precise location of the user (with an accuracy greater than the scale of a city or more than one decimal unit in terms of latitude/longitude), this purpose can be described as follows: "**Geolocation advertisement**: *[name of site/app] [and **third party companies/our partners]** use/use trackers to send you advertisement based on your location*".

- If the trackers are used to customize the editorial content or the products and services that are provided and displayed by the publisher, one of the following formulations may be displayed: *"**Content customization**: Our website/application [and **third party companies]** use/use trackers to customize the editorial content [of our website/application] based on your use of our website/application"*, or *"Our website/application [and **third party companies]** use/use trackers to customize the display of our products and services based on what you have previously viewed [on our website/application]*").

- If trackers are used to share data on social networks, their purposes can be described as follows: *"**Sharing on social networks**: Our website/application uses trackers to allow you to share content on social networks or platforms present [on our website/application]*". If the publisher has put in place a mechanism to trigger these trackers only at a time when the user actually wishes to share the data with the relevant social networks (and interacts with the feature or button allowing this interaction), the information and the collection of consent may appear once the user decides to trigger the said sharing feature.

- If trackers are used for audience measurement, and if their characteristics make them subject to consent, where such trackers do not meet all the conditions set out in Article 5 of the Guidelines on *cookies* and other trackers, the purpose may be described as follows: ***"Audience measurement**: Our website/application [and **third party companies/our partners]** use/use trackers to measure the audience [of our website/application]*".

20. In order to enable the user to understand more precisely what he or she is consenting to, the Commission recommends that, in addition to the list of purposes presented on the first screen, a more detailed description of these purposes is included in an easily accessible way in the consent collection interface. In practice, this information can be displayed under a scroll button that the user can activate directly at the first level of information. It can also be made available by clicking on a hyperlink at the first level of information.

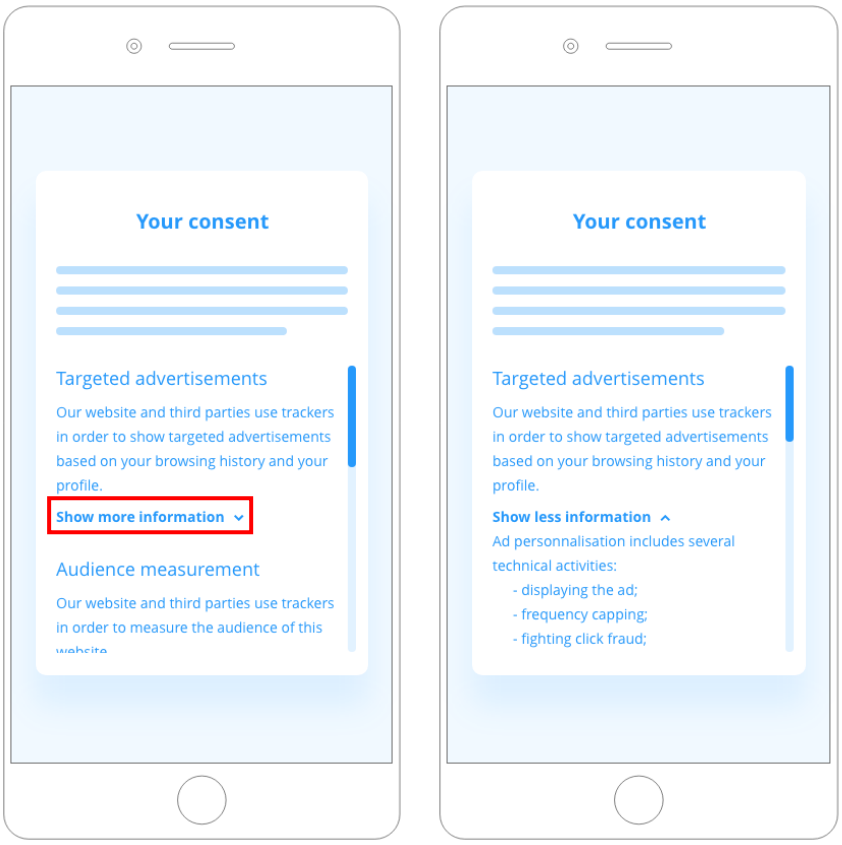

Figure 1 - The details of the purposes are available under a drop-down button that the user can activate on the first level of information.

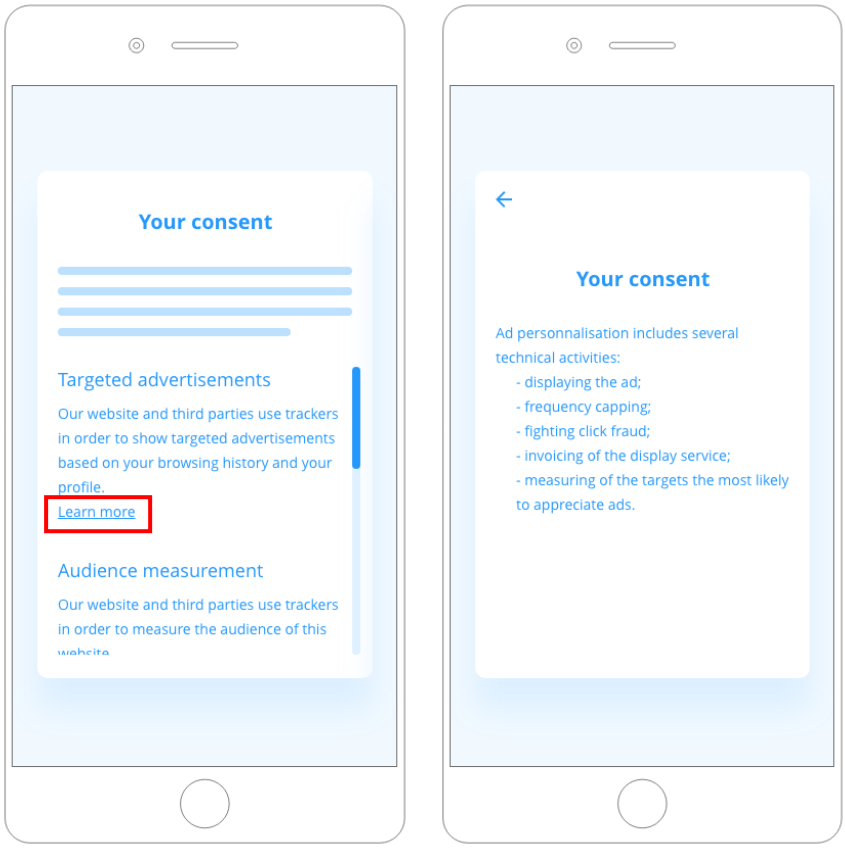

Figure 2 - Details of the purposes are available by clicking on a hyperlink on the first level of information.

21. Regarding the content of this additional information and, as an example, with regard to the display of advertisement (personalized or not), it can be specified that this purpose encompasses various technical operations such as the display of advertising, the *capping* of the display (sometimes called "advertising *capping*"), aiming at not presenting the same advertisement to a user in a repetitive manner, fighting against click fraud (detection of publishers claiming to have a larger advertising audience than they actually do), billing the display services, measurement of the size of the targeted audience, better understanding the audience, etc.

22. With regard to audience measurement, it may be specified that the trackers will be used to enable the person responsible for the processing(s) to understand how visitors access the website or mobile application, as well as the paths taken.

Best practices

23. Finally, as a good practice, the categories of data collected through trackers could be specified for each purpose in a way that is easily accessible to the user.

2.2 - Information on data controllers and the scope of consent

24. The user must be able to find out the identity of all those responsible for the processing operation(s) before being able to give consent or refuse to give his or her consent. He or she must therefore be fully aware of the effective scope of his or her consent.

Practical arrangements for implementation

25. Pursuant to this requirement, the exhaustive list of controllers of the processing operation(s) should be made available to the user upon obtaining consent and permanently made easily accessible.

26. In addition, this list should be regularly updated. In order to avoid overburdening the user, the Commission considers that in case of additions that are qualitatively non-substantial, it is sufficient that the updated list of controllers of the processing operation(s) is made available to the user via a permanent and easily accessible link on the service, e.g. through the consent removal mechanism. On the other hand, in the case of a substantial addition, the user's consent should be sought again before continuing with the reading and/or writing of information on his terminal equipment.

27. Finally, for the user to be fully aware of the scope of his or her consent, he or she should particularly know whether the consent is valid for the tracking of his or her navigation on sites or applications other than those on which his or her consent is collected. Information on the extent of navigational tracking permitted by the trackers, indicating the different web sites and applications concerned, should be made available to the user before he or she expresses a choice.

Examples of how to comply with the applicable rules

28. In practice, in order to reconcile the requirements of clarity and conciseness of information with the need to identify all those responsible for the processing operation(s), specific information on these entities (identity, link to their privacy policy) may be given on a second level of information. They can be made available on the first level *via*, for example, a hyperlink or a button accessible from this level. The Commission recommends using a descriptive name and using clear terms such as "list of companies using trackers on our website/application".

29. The Commission also recommends that the mechanism for viewing the updated list of data controllers should be placed in areas of the screen that attract the attention of users or in areas where they expect to find it, throughout its navigation. As an example, the editor of a website can provide the user with a parameterization module accessible on all the pages of the site by means of a static icon "*cookie*" or a hypertext link located at the bottom of the page.

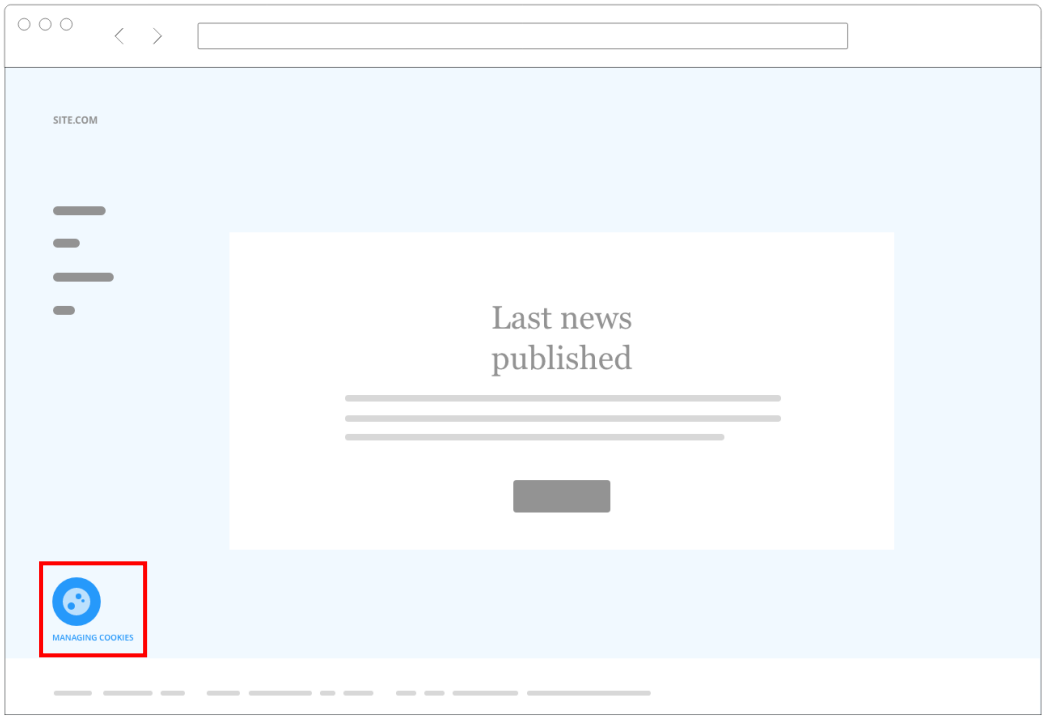

Figure 3 - Example of parameters accessible on all the pages of the site by means of a static "cookie" icon located at the bottom of the screen allowing the user to view the updated list of those responsible for the processing operation(s).

30. Finally, for a consent (which is collected on one site or mobile application) to also be valid on other sites or mobile applications, the list of all the websites or mobile applications concerned can be made accessible *via* a hypertext link or a button located on the first level of the consent collection mechanism.

Best practices

31. As a good practice, the number of persons responsible for the processing operation(s) could be indicated at the first level of information. Similarly, in order to ensure better understanding and readability for the user, the role of the controllers of the processing operation(s) could be highlighted by grouping them into categories, which would be defined according to their activity and the purpose of the trackers used.

32. With regard to the modification of the list, the fact that the list has been modified could be usefully highlighted, for example by a change of colour of the link leading to it, or a particular animation of that link. Within the list, it is possible to draw the user's attention to the controllers of the processing operation(s) that have joined the list since the last expression of consent, so that the user can maintain consent in full knowledge of the facts.

Article 3

The requirement for free consent

33. Consent can only be valid if the user is able to exercise his or her choice freely, under the conditions described in the guidelines.

Practical arrangements for implementation

34. In the first place, the person responsible for the processing operation(s) should offer the user both the possibility of accepting and not accepting (in other words, of refusing) the read and/or write operations.

35. Secondly, the same degree of simplicity should apply to the ability to consent or not to consent. The ability to express refusal as easily is indeed the counterpart of the ability to express free consent. Therefore, in order not to affect the user's freedom of choice, the mechanism for expressing consent should be presented at the same level and in the same technical manner as the mechanism for expressing refusal.

36. Thirdly, the user should not suffer any prejudice if he or she chooses to refuse. Thus, the choice expressed by the user, be it consent or refusal, should be recorded in such a way that the user's consent is not sought again for a certain period of time. Indeed, failure to register the refusal would prevent it from being taken into account in the long term, in particular during new visits. If the choice that the user has expressed is not registered, he or she would be asked again to consent. This continued pressure would be likely to cause the user to accept out of weariness. Failure to record the refusal to consent could therefore have the consequence of exerting pressure that could influence his or her choice, thus calling into question the freedom of the consent he or she expresses.

37. Moreover, in the light of the above, the Commission considers that for consent to be freely given, its counterpart, namely the refusal, should be registered (and therefore taken into account) for a duration which is at least identical to that for which consent is registered. In order to preserve the choices expressed by the Internet user, a tracker may be used, with the sole purpose of storing consent or refusal.

38. Moreover, nothing prohibits the person responsible for the processing operation(s) to provide the user with the possibility of not making any choice and delaying his or her decision, as long as the user is given the choice between acceptance and refusal. The situation in which the user does not express any positive choice must be distinguished from the situation of refusal. In the absence of any manifestation of choice (neither acceptance nor refusal), no trackers requiring consent should be written. The user could then be asked again as long as he or she does not express a choice.

39. Finally, these interfaces should not use potentially misleading design practices, such as the use of visual grammar that might lead the user to think that consent is required to continue browsing or that visually emphasizes the possibility of accepting rather than refusing.

Examples of how to comply with the applicable rules

40. In practice, a request for consent could take the form of boxes that the user may choose to check to express his or her consent. The person responsible for the processing operation(s) may also use sliders *that* can be activated to express consent or refusal of the trackers. The user may also have the choice between two buttons presented at the same level and in the same format, with "accept" and "refuse", "allow" and "forbid", or "consent" and "do not consent", or any other equivalent wording that is sufficiently clear to the user.

41. In addition, in order to allow the user not to make a choice, the person responsible for the processing(s) may integrate a closing cross on the interface for collecting consent, or allow the user to make it disappear by clicking outside the interface, for example.

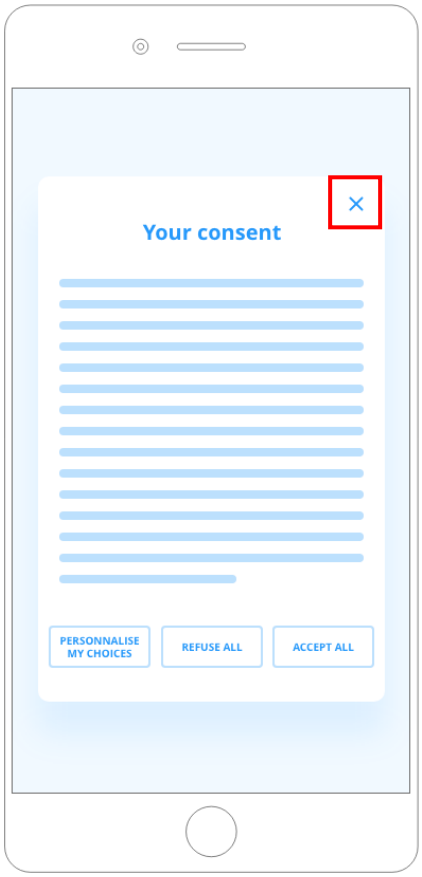

Figure 4 - A closing cross allows the user not to make a choice and to delay his decision.

Best practices

42. The development of standardised interfaces operating in the same way and using a standardised vocabulary would make it easier for users to understand when navigating from one site to another.

Article 4

The requirement for specific consent

43. The user must be given the opportunity to give independent and specific consent for each separate purpose.

Practical arrangements for implementation

44. Mere acceptance of general terms and conditions of use or of sale does not constitute specific consent.

45. The Commission considers that the obligation to obtain specific consent does not preclude the possibility of offering the user the ability to consent globally for a range of purposes, provided that:

- all the purposes have been presented to the user beforehand;
- the user is also allowed to consent purpose per purpose;
- the user is provided with the option to refuse globally at the same level and under the same conditions as the option to consent globally.

Examples of how to comply with the applicable rules

46. Thus, in order to facilitate the navigation of the Internet user, it is possible to propose global acceptance and refusal buttons *via, for* example, the presentation of buttons entitled "accept all" and "refuse all", "I authorise" and "I do not authorise", "I accept all" and "I do not accept anything" or "I agree to all purposes" and "I do not agree", allowing him to consent or refuse, in a single action, to several purposes. However, in order to ensure that the user has not been induced by design choices to accept rather than to refuse, it is recommended to use buttons and a font of the same size, offering the same ease of reading, and highlighted in the same way.

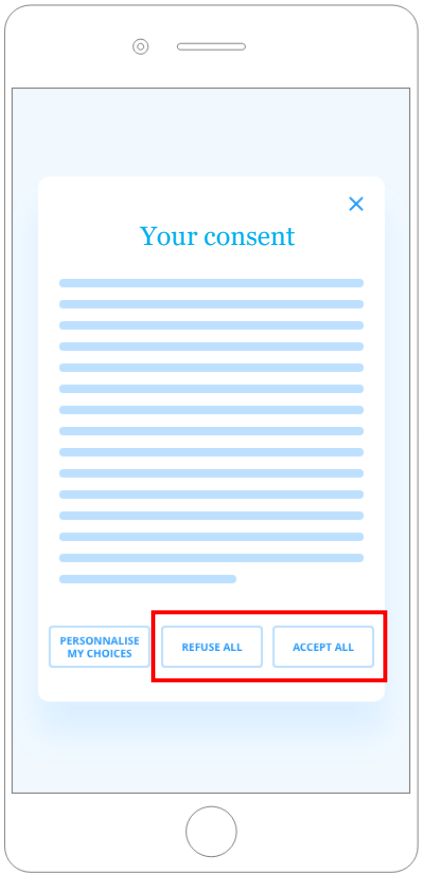

Figure 5 - It is possible to offer global accept and reject buttons, for example by presenting "accept all" and "reject all" buttons that are equally emphasized.

47. On the other hand, the possibility of granular consent or refusal can be offered in different ways.

48. For example, the user could be offered to accept or refuse purpose per purpose directly on the first level of information. He or she may also be asked to click on each purpose so that a drop-down menu offers him or her "accept" or "decline" buttons. It is also possible to include a button, on the same level of information as the links or buttons allowing to accept and refuse everything, and allowing to access the choice purpose per purpose. In this case, a descriptive and intuitive name should be used so that users can be fully aware of the possibility of exercising a choice by purpose. As an example, a button "customize my choices" or "decide by purpose" allows you to clearly indicate this possibility.

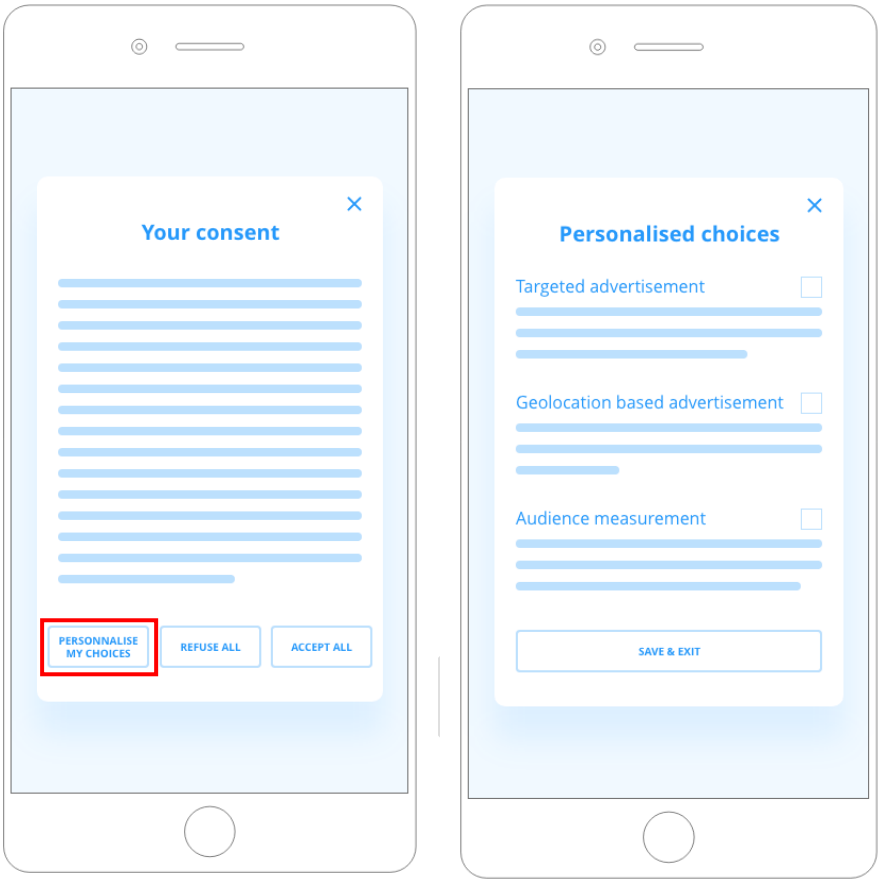

Figure 6 - The possibility of granular consent can be offered on a second level of information via a "customize my choices" button inserted on the same level of information as the links or buttons allowing "accept all" and "refuse all".

Best practices

49. The possibility for users to be able to choose specifically not only by purpose but also by data controller could contribute to strengthening the user's control over his/her data.

Article 5

The requirement for unambiguous consent

50. Consent must be manifested by a clear positive act of the user, meeting the conditions described in the guidelines.

Practical arrangements for implementation

51. By its presentation, the mechanism for obtaining consent must enable the data subject to be aware of the goal and scope of the act enabling him or her to signify his or her agreement or disagreement. Thus, this mechanism should not involve potentially misleading design practices, such as the use of visual grammar that impedes the user's understanding of the nature of his or her choice.

Examples of how to comply with the applicable rules

52. A consent request made using check boxes, unchecked by default, is easily understood by the user. The person responsible for the processing(s) may also use sliders, deactivated by default, if the choice expressed by the user is easily identifiable. The information accompanying each actionable element for expressing consent or refusal should be easily understandable and should not require any effort on the part of the user. Thus, it should not be written in such a way that a quick or careless reading might suggest that the selected option produces the opposite of what the user intended to choose.

Article 6

Withdrawal and duration of consent

53. Users who have given their consent to the use of trackers must be able to withdraw it at any time. The Commission reminds that it must be as simple to withdraw as it is to give consent.

Practical arrangements for implementation

54. Users must be informed in a simple and intelligible manner, even before giving their consent, of the options available to them for withdrawing their consent, or even of the period of validity of their consent if such a period has been defined.

55. In practice, the Commission recommends that solutions allowing the user to withdraw consent should be easily accessible throughout the use of the service. The simplicity of access can be measured by the time spent and the number of actions required to access the withdrawing mechanism.

Examples of how to comply with the applicable rules

56. The possibility of withdrawing consent may, for example, be offered *via* a link accessible at any time from the service concerned, in order to ensure that users can withdraw their consent with the same ease as they gave it. It is recommended to use a descriptive and intuitive name such as "*cookie* management module" or "manage my *cookies*" or "*cookies",* etc. The publisher of a website can also provide the user with a configuration module accessible on all the pages of the site by means of a "*cookie"* icon, located at the bottom left of the screen, enabling him to easily withdraw his consent.

57. In any event, the Commission recommends that the mechanism for withdrawing consent be placed in an area that attracts the attention of users or in areas where the user expects to find it, and that the visuals used be as explicit as possible.

Best practices

58. To the extent that the consent to be monitored may be forgotten by those who gave it at a given time, the Commission recommends that it be renewed at appropriate intervals without waiting for the user to withdraw consent. The length of time the consent is valid will depend on the context, the scope of the initial consent and the expectations of the user.

59. In general, the Commission considers that a period of validity of six months from the expression of the user's choice is appropriate.

Article 7

Proof of consent

Practical arrangements for implementation

60. The data controllers must be able to demonstrate that the user has given his consent. They must implement mechanisms that enable them to demonstrate that they have rightfully obtained the consent of the users concerned.

61. The controller of the processing operation(s) must therefore be able to:

- on the one hand, provide individual evidence of the collection of user consent; and
- on the other hand, demonstrate that the mechanism that collected the consent has all the characteristics that allows a valid consent to be collected (freely given, specific, informed and unambiguous), thus providing proof of the overall validity of the consent collection process.

62. The Commission reminds that data controllers must ensure that a suitable solution is put in place.

Examples of how to comply with the applicable rules

63. In practice, in order to provide individual proof of consent, the Commission recommends the following mechanisms:

- The recording of the information allowing the consent to be properly taken into account could be done at the level of the consent collection mechanism, i.e. the tracker in the case of a web browser, or the parameter used to store the consent information in the case of a mobile application, etc.
- The data thus recorded could include a timestamp of the consent, the context in which the consent was collected (identification of the website or mobile application), the type of consent collection mechanism used, and the purposes to which the user has consented.

64. The Commission reminds that if the obligation to prove consent leads to the collection of data on the context in which consent was given, it should not lead the controller of the processing operation(s) to collect more data on the user; only data necessary to prove consent should be collected.

65. With respect to proving the validity of the consent, the Commission recommends the following procedures:

- Proof of the validity of the consent may be obtained by placing the code used by the organization collecting the consent, for the different versions of its site or mobile application in an escrow managed by a third party; or
- A screenshot of the visual rendering displayed on a mobile or desktop device can be kept for each version of the site or application; or
- Regular audits of the consent collection mechanisms implemented by the sites or applications from which consent is collected may be implemented.

Article 8

How to use cookies: good practices

66. In order to ensure the greatest transparency in the use of *cookies*, the use of different *cookies* for each distinct purpose would allow the user to distinguish between them and to ensure that his consent is respected, but also to make reading or writing operations more transparent. In particular, trackers previously listed as exempt from consent should preferably be used for a single purpose only, so that the lack of user consent does not affect the use of trackers necessary for navigation.

67.The Commission also encourages against the use of entity identity masking techniques using trackers, such as CNAME cloaking.

68. The Commission also recommends, as a good practice, that the names of the trackers used should be explicit and, as far as possible, standardised regardless of the actor setting them.

69. The Commission also recommends, as a matter of good practice, that the tracker used to store the choice of the user is named "eu-consent", setting each purpose to a "true" or "false" boolean value reflecting the user choice. In the event that the user does not wish to express himself, the tracker can store the number of pages viewed by the user or a reference date in order to limit the resurfacing frequency of the consent collection interface.

70. Finally, standardised icons could be developed to enable users to be informed quickly and efficiently.

Article 9

Collection of consent via browsers: good practices

71. Article 82 of the French law Data Protection Act provides for obtaining consent through *"appropriate parameters of the user's connection device or any other device under his control"*. The Commission described in its guidelines that the browser settings cannot, in the state of the art, allow the user to express valid consent.

72. However, browsers and operating systems could eventually integrate consent collection mechanisms that would facilitate both the setting up of consent collection mechanisms for

mobile site and application publishers and the expression of users' choices, who could set their browsers to inform sites of their preferences.

73. Thus, as a good practice, where browser providers and operating systems decide to offer such mechanisms to the user, the Commission recommends that they:

- allow users to consent to, or refuse, read or write operations when first using the browser or terminal concerned, providing they received the information that allow them to make an informed choice;
- include a mechanism that allows mobile site and application publishers to request and obtain consent in accordance with regulations;
- where the user has explicitly consented through the above-mentioned mechanism, apply this consent by authorizing the recipient of this consent to perform the read and write operations.