Report of the work undertaken by the Cookie Banner Taskforce

Adopted on 17 January 2023

[
Nicholas Vollmer: Dieser Report wird sehr kritisch kommentiert unter

https://netzpolitik.org/2023/europaeische-datenschutzbehoerden-schon-wieder-keine-klaren-regeln-fuer-cookie-banner/]
]

Table of Contents

DISCLAIMER 3
1. APPLICABLE LEGAL FRAMEWORK 4
2. APPLICATION OF THE OSS 4
3. TYPE A PRACTICE – "NO REJECT BUTTON ON THE FIRST LAYER" 4
4. TYPE B PRACTICE – "PRE-TICKED BOXES" 5
5. TYPE C PRACTICE 5
6. TYPE D & E PRACTICES : "DECEPTIVE BUTTON COLOURS" & "DECEPTIVE BUTTON CONTRAST" 6
7. TYPE H PRACTICE: "LEGITIMATE INTEREST CLAIMED, LIST OF PURPOSES" 6
8. TYPE I PRACTICE: "INACCURATELY CLASSIFIED « ESSENTIAL » COOKIES" 7
9. TYPE K PRACTICE: "NO WITHDRAW ICON" 8

DISCLAIMER

The positions presented in this document result from the coordination of the members of the TF with a view to handling the "cookies banner" complaints received from NOYB. They reflect the common denominator agreed by the SAs in their interpretation of the applicable provisions of the ePrivacy Directive, and of the applicable provisions of the GDPR, for the analysis to be led when handling these complaints. These positions reflect a minimum threshold in this multi-layered legal framework to assess the placement/reading of cookies and subsequent processing of the data collected. They do not constitute stand-alone recommendations or findings to obtain a greenlight from a competent authority. The positions do not prejudge the analysis that will have to be made by the authorities of each complaint and each website concerned. These positions have to be combined with the application of additional national requirements stemming from the national laws transposing the ePrivacy Directive in the Member States, as well as to further clarifications and guidance provided by the national competent authorities to enforce the law transposing the ePrivacy Directive at national level, which remain fully applicable.

Following thirteen meetings of the taskforce members to coordinate their actions in handling the complaints received from NOYB, the following points were noted:

1. APPLICABLE LEGAL FRAMEWORK

1. Where the complaints concern the placement or reading of cookies the delegations confirmed that the applicable framework is only the national law transposing the ePrivacy Directive to the placement of cookies[1].

2. Concerning the subsequent processing activities undertaken by the controller of data, meaning the processing which takes place after storing or gaining access to information stored in the terminal equipment of a user in accordance with Article 5(3) Directive 2002/58/EC (for example, the placement or reading of cookies), the delegations confirmed that the applicable framework is the GDPR (including to consent, even if given at the same moment of the placement of cookies, as far as this consent constitutes the legal basis of the subsequent processing), in line with the conclusions of EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR[2].

3. In accordance with the ePrivacy framework, it was recalled that certain concepts from the GDPR (e.g. the conditions for valid consent3 and the right to information) are indispensable to assess whether there is an infringement of the national law transposing the ePrivacy Directive or not.

2. APPLICATION OF THE OSS [Nicholas Vollmer: "One Stop Shop"]

4. Delegations recalled that the OSS mechanism does not apply to issues that fall under the ePrivacy Directive.

5. When the GDPR applies, the taskforce members favoured the position that article 4(23)(b) may apply but does not per se apply to complaints against website owners just because you can access the respective website from all Member States. The CSAs will be identified based on the factual elements to conclude on cross-border cases.

3. TYPE A PRACTICE – "NO REJECT BUTTON ON THE FIRST LAYER"4

6. It appears that some cookie banners displayed by several controllers contain a button to accept the storage of cookies and a button that allows the data subject to access further options, but without containing a button to reject the cookies.

[1] In accordance with article 15.3 of ePrivacy directive, and as it has been done in the context of these works, the EDPB shall also carry out its tasks with regard to matters covered by the ePrivacy Directive
[2] See also the EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications.
[3] By taking into consideration the EDPB Guidelines 05/2020 on consent under Regulation 2016/679
[4] The names of the violations used in the complaints have been kept.

7. As a preliminary remark, the task force members recalled that by default, no cookies which require consent can be set without a consent and that consent must be expressed by a positive action on the part of the user.

8. When authorities were asked whether they would consider that a banner which does not provide for accept and refuse/reject/not consent options on any layer with a consent button is an infringement of the ePrivacy Directive, a vast majority of authorities considered that the absence of refuse/reject/not consent options on any layer with a consent button of the cookie consent banner is not in line with the requirements for a valid consent and thus constitutes an infringement. Few authorities considered that they cannot retain an infringement in this case as article 5(3) of the ePrivacy Directive does not explicitly mentioned a "reject option" to the deposit of cookies.

4. TYPE B PRACTICE – "PRE-TICKED BOXES"

9. It appears that several controllers provide users with several options (typically, representing each category of cookies the controller wishes to store) with pre-ticked boxes on the second layer of the cookie banner (after the user clicked on the "Settings" button of the first layer).

10. The taskforce members confirmed that pre-ticked boxes to opt-in do not lead to valid consent as referred to either in the GDPR (see in particular recital 32 "Silence, pre-ticked boxes or inactivity should not therefore constitute consent.") or in Article 5(3) of the ePrivacy Directive.

5. TYPE C PRACTICE

11. Deceptive "Link Design"It appears that some cookie banners displayed by several controllers contain a link, not a button, as an option to reject the deposit of cookies (direct link to reject or link to a second layer where a user can reject the deposit of cookies).

12. The taskforce members agreed that in any case, there should be a clear indication on what the banner is about, on the purpose of the consent being sought and on how to consent to cookies.

13. The members agreed that for the consent to be valid, the user should be able to understand what they consent to and how to do so. In order for a valid consent to be freely given, the taskforce members agreed that in any case a website owner must not design cookie banners in a way that gives users the impression that they have to give a consent to access the website content, nor that clearly pushes the user to give consent (one way could be on the contrary to allow the continuation of the navigation without cookies from the first level in particular for example).

14. The taskforce members agreed that the following examples do not lead to valid consents (non-exhaustive list):
    - the only alternative action offered (other than granting consent) consists of a link behind wording such as 'refuse' or 'continue without accepting' embedded in a paragraph of text in

the cookie banner, in the absence of sufficient visual support to draw an average user's attention to this alternative action;
- the only alternative action offered (other than granting consent) consists of a link behind wording such as 'refuse' or 'continue without accepting' **placed outside the cookie banner** where the buttons to accept cookies are presented, in the absence of sufficient visual support to draw the users' attention to this alternative action outside the frame;

6. TYPE D & E PRACTICES : "DECEPTIVE BUTTON COLOURS" & "DECEPTIVE BUTTON CONTRAST"

15. It appears that the configuration of some cookie banners in terms of colours and contrasts of the buttons ("contrast ratio between the accept button and the background" – type D practice) could lead to a clear highlight of the "accept all" button over the available options.

16. The taskforce members agreed to examine type D and E practices together as the issues are linked and raise similar points of discussion.

17. The taskforce members agreed that a general banner standard concerning colour and/or contrast cannot be imposed on data controllers. In order to assess the conformity of a banner, a case-by-case verification must be carried out in order to check that the contrast and colours used are not obviously misleading for the users and do not result in an unintended and, as such, invalid consent from them. As a result, it was also agreed that a case-by-case analysis would be necessary to address specific cases, although some examples of features manifestly contrary to the ePrivacy Directive provisions have been identified.

18. Based on concrete examples, the taskforce members took the view that at least this practice could be manifestly misleading for users:
    - an alternative action is offered (other than granting consent) in the form of a button where the contrast between the text and the button background is so minimal that the text is **unreadable** to virtually any user.

19. While the design choices above are considered problematic, the taskforce members reiterated that each specific cookie banner needs to be assessed on a case-by-case basis.

7. TYPE H PRACTICE: "LEGITIMATE INTEREST CLAIMED, LIST OF PURPOSES"

20. It appears that some controllers put in place a banner which highlights the possibility of accepting the read/write operation at the first level (of the banner) but does not include an option to refuse at this level, which can lead the average user to believe that he has no possibility of objection to the deposit of cookies at all, and, incidentally, to the subsequent processing that results from them.

21. In addition, at the second level (of the banner), a distinction is made between the refusal given to read/write operations and the potential objection to further processing presented as falling within the legitimate interest of the data controller.

22. In those cases, it appears that:
    - The controller relied on legitimate interests under article 6(1)(f) GDPR for different processing activities as, for example, "Create a personalised content profile" or "Select personalised ads" whereas it could be considered that no overriding legitimate interest would exist for such processing activities.
    - The integration of this notion of legitimate interest for the subsequent processing "in the deeper layers of the banner" could be considered as confusing for users who might think they have to refuse twice in order not to have their personal data processed.

23. The taskforce members agreed that whether the subsequent processing based on cookies is lawful requires to determine if:
    - the storage/gaining of access to information through cookies or similar technologies is done in compliance with Article 5(3) ePrivacy directive (and the national implementing rules).
    - any subsequent processing is done in compliance with the GDPR.

24. In this regard, the taskforce members took the view that non-compliance found concerning Art. 5 (3) in the ePrivacy directive (in particular when no valid consent is obtained where required), means that the subsequent processing cannot be compliant with the GDPR5. Also, the TF members confirmed that the legal basis for the placement/reading of cookies pursuant to Article 5 (3) cannot be the legitimate interests of the controller.

25. The TF members agreed to resume discussions on this type of practice should they encounter concrete cases where further discussion would be necessary to ensure a consistent approach.

8. TYPE I PRACTICE: "INACCURATELY CLASSIFIED « ESSENTIAL » COOKIES"

26. It appears that some controllers classify as "essential" or "strictly necessary" cookies and processing operations which use personal data and serve purposes which would not be considered as "strictly necessary" within the meaning of Article 5(3) ePrivacy Directive or the ordinary meaning of "strictly necessary" or "essential" under the GDPR.

27. Taskforce members agreed that the assessment of cookies to determine which ones are essential raises practical difficulties, in particular due to the fact that the features of cookies change regularly, which prevents the establishment of a stable and reliable list of such essential cookies.

28. The existence of tools to establish the list of cookies used by a website has been discussed, as well as the responsibility of website owners to maintain such lists, and to provide them to the competent authorities where requested and to demonstrate the « essentiality » of the cookies listed.

[5] See EDPB guidelines on connected vehicles; also see ECJ C-597/19 para. 118.

29. On that point, it has been mentioned that specific tools exist and may be used to analyse a website and create a report that shows all the cookies that were placed when visiting the website. However, the only available tools do not allow to check the nature of the cookies but only to list the cookies placed in order to ask the website owner to provide documentation on their purposes. These tools are thus an additional help for the competent authorities to seek further clarifications and information from the website owners in addition to the information also provided on the website.

30. The opinion n°04/2012 on Cookie Consent Exemption of WP 29 has also been recalled in relation to the criteria mentioned to assess which cookies are essential, and in particular the fact that cookies allowing website owners to retain the preferences expressed by users, regarding a service, should be deemed essential.

9. TYPE K PRACTICE: "NO WITHDRAW ICON"

31. It appears that where controllers provide an option allowing to withdraw consent, different forms of options are displayed. In particular, some controllers have not chosen to use the possibility to show a small hovering and permanently visible icon on all pages of the website that allows data subjects to return to their privacy settings, where they can withdraw their consent.

32. Website owners should put in place easily accessible solutions allowing users to withdraw their consent at any time, such as an icon (small hovering and permanently visible icon) or a link placed on a visible and standardized place.

33. The ePrivacy Directive's reference to consent in the GDPR includes both a reference to the definition of consent (article 4 of the GDPR) as well as to the conditions of it (article 7 of the GDPR).

34. In addition to the requirements for the collection of consent to be valid in accordance with the GDPR and under Article 5(3) ePrivacy Directive, three additional cumulative conditions are mandatory (i) the possibility to withdraw consent, (ii) the ability to withdraw consent at any time, (iii) withdrawal of consent must be as easy as to give consent.

35. However, website owners can only be imposed that easily accessible solutions are implemented and displayed once consent has been collected, but they cannot be imposed a specific withdrawal solution, and in particular to set up a hovering solution for the withdrawal of consent to the deposit of cookies and other trackers. A case-by-case analysis of the solution displayed to withdraw consent will always be necessary. In this analysis, it must be examined whether, as a result, the legal requirement that it is as easy to withdraw as to give consent is fulfilled.