UNOFFICIAL GOOGLE TRANSLATE OF THE ORIGINAL TEXT

PRESS RELEASE

Recommendations for the compliance of data controllers with the specific legislation on electronic communications

The Authority has found to a sufficient extent that information society service providers have failed to comply with the specific requirements of electronic communications data processing legislation and the General Data Protection Regulation regarding the management of cookies and related technologies.

In order to provide practical guidance to editors and to inform users of Greek sites, the Authority issues text with specific recommendations for compliance in this area. This includes, in the form of points, guidance on the proper use of such technologies as well as practices to be avoided.

It should be noted that the codification of these requirements does not constitute a change in the existing institutional framework and the jurisprudence of the Authority, to which data controllers are required to comply. However, recognizing that it may take some time to adjust the management mechanisms used by the websites, the Authority invites all editors to adapt within two months at the latest.

Compliance Tips for Editors Who Maintain Web Sites

The following settings apply to HTTP / S cookies, to flash cookies, to "local storage" that applies to HTML 5, in recognition by calculating the terminal's digital fingerprint, to IDs generated by operating systems (whether intended for advertising purposes or not: IDFA, IDFV, Android ID, etc.), in hardware identifiers (MAC address, serial number, or other device identifier), etc.

The following text uses the term "tracker" as the most appropriate way to capture these techniques.

A. Obligation and exceptions

1. Putting a tracker on a terminal requires first the consent of the user, regardless of whether personal data is eventually processed.

2. Trackers exempted from consent are those deemed technically necessary to make the connection to the Website or to provide the Internet service requested by the user himself.

Indicative categories of trackers (cookies and related technologies) that fall under the above exception are those that are necessary:

- to identify and / or maintain content that the subscriber or user uploads during a session on a website throughout the specified connection, such as a "shopping cart"
- to connect the subscriber or user to services that require authentication
- for the safety of the user
- to perform the load balancing technique on a web site link

- to maintain the user's choice of website presentation, e.g. language selection, save search history

3. Tracers installed for online advertising are not an exception, so they are allowed only after the prior consent of the user has been obtained with appropriate information.

4. The use of third-party crawlers, such as the Google Analytics service for web analytics, can only be done with the consent of the website user.

Bad practices

1. Cursors are needed to operate the site, but no updates are provided to the user.

2. Use of Google Analytics for statistical analysis (web analytics) is done only by informing the user without the possibility of rejection or even updating.

B. Method and content of information

1. Updating and consent may be provided through the Internet Service Provider's website using appropriate mechanisms (e.g. pop-ups or banners).

2. It is legitimate to provide information using a layered approach, provided that the consent of the user is sought after the user has been specifically informed, at least of the categories of trackers used.

3. The information message (whether it is a pop-up window or otherwise) should provide specific information for the purpose of each tracker used, not general information on the use of trackers.

4. For each tracker or category of trackers of the same purpose, the duration of operation, the identity of the controller, the recipients or categories of recipients of the data shall be indicated.

5. The content of the update should be legible regardless of the terminal device from which it is accessed (portable or fixed device).

Bad practices

1. Only general information on the use of tracers is provided within a general privacy policy.

2. Information on the use of tracers at the first level of the pop-up window is limited to a general text which states that such techniques are used, e.g. cookies for better experience, better presentation, etc.

3. The text of the update is not readable due to the non-adaptation to the type of terminal device from which it is accessed (portable or fixed device).

C. How to obtain consent

1. Consent requires clear positive action. Pre-filled boxes, simple scrolling, or scrolling are not acceptable ways of obtaining consent.

2. It is not considered that there is consent from the user if the browser chooses to accept cookies.

3. In the absence of any manifestation of selection (neither acceptance nor rejection), no unnecessary tracer shall be used.

4. The user must be able, with the same number of actions ('clicks') and from the same level, to either accept the use of trackers (those with which consent is required) or to reject it, or all or any category Separately.

5. The user must be able to withdraw his consent in the same manner and with the same ease with which he has granted it.

6. Failure to consent to the use of crawlers should not result in access to the content of the site [being denied?] (avoiding a "cookie wall").

7. To ensure that the user is not influenced by design options in favour of the acceptance option over the rejection option, it is recommended to use buttons of the same size, accent and colour, providing the same ease of reading.

8. Regardless of whether or not the trackers are accepted, the pop-up window reappears to ask the user again after the same time. That is, the "compliance" period of the user's choice is the same whether the user rejects or accepts the trackers. It goes without saying that using a tracker to store this user's choice is technically necessary.

<u>Bad practices</u>

1. To obtain consent there is simply a choice of "OK, I was informed" or "OK, I agree" without the option of continuing navigation (by removing this message) if the user does not select the above.

2. It is not possible to reject the use of tracers in the pop-up window only to accept them all.

3. The possibility of rejecting the use of tracers is given only at a second level of information, that is, after clicking on a link to "more information", "settings".

4. Closing the popup / popup window leads to the use of unnecessary trackers.

5. Continuous navigation or scrolling after the pop-up window results in the installation of unnecessary trackers.

6. The size and color of the "accept" or "consent" button strongly predetermines the user to choose, e.g. is very large and in bold and / or default.

7. The pop-up window only allows unnecessary trackers to be accepted by reference to a general data protection or privacy policy.

8. After acceptance or rejection by the user, there is no way to change their preferences.

9. After acceptance or rejection by the user, his preferences can only be changed by changing the web browser settings.

10. In case the trackers are rejected, the user is constantly called through the popup to make a new selection. It is not the same when it is accepted, as this option is maintained for a longer period.