JustRelate

Is your consent banner genuinely GDPR-compliant, and are the consents you collect legally effective?

Only a small number of websites meet all the requirements set by supervisory authorities regarding the design and content of consent dialogs on websites and apps. The verdict is unequivocal: if even a single requirement is missing, the entire consent obtained becomes invalid. For this reason, we have summarized the authorities' requirements in a practical and concise guide.

According to Version 1.2 of the Guidance for Providers of Digital Services (OH Digital Services) issued by the supervisory authorities, the following requirements must be met to ensure that consent dialogs are designed in a legally compliant manner:

Design and functionality

☐ **Voluntary Consent:** The rejection of all consent-requiring data access must be possible directly on the first layer of the consent dialog if consent can also be granted there.

☐ **Avoidance of dark patterns:** The option not to give consent must be presented as an equivalent alternative to giving consent.

- The option to refuse consent must not be designed as a text link while the option to give consent is presented as a button.
- Buttons and text for both accepting and rejecting consent must have the same size, readability, and visual prominence.

☐ **Visibility:** all buttons must be clearly visible at a glance, regardless of screen size. This requirement also applies to mobile views.

☐ **Trigger exception:** access to the legal notice (Imprint) and the privacy policy must not be obstructed by the consent banner. The consent dialog must not be displayed on these pages.

☐ **Enable granular choice:** users must be able to give consent separately and independently for each specific purpose. This can be achieved by providing a button such as "Customize Settings" on the first layer, which leads to a detailed preference overview.

☐ **Clear default settings (Opt-In):** checkboxes, toggles, or sliders must be disabled by default, requiring users to actively opt in to provide consent.

Storage and withdrawal of consent

☐ **Storage of the decision:** the user's choice (whether consent or refusal) must be stored so that the banner does not appear on every page visit. After a period of 6 to 24 months, or if the purposes or services change, consent must be requested again.

☐ **Easy withdrawal at any time:** users must be able to withdraw previously given consent just as easily as they provided it. For this purpose, a permanently accessible link or a static icon (e.g., in the bottom-left corner of the screen) must be available on all pages at all times.

JustRelate

Required information

Information on the first level:

It must be clearly recognizable that two separate consents are being requested: one for the use of cookies (§ 25(1) TDDDG) and one for data processing (Art. 6(1)(a) GDPR).

The following information is mandatory on the first level:11

☐
- Specific information on all individual purposes (no vague wording): clear and concrete details must be provided for each individual purpose of data processing.
- Notice of profiling: it must be indicated whether individual user profiles are created or whether data is enriched with information from other websites.
- Information on data processing outside the EEA: users must be informed if data is processed outside the European Economic Area.
- Number of recipients: the number of controllers or recipients to whom the data is disclosed must be specified.

Detailed-Level Information:

☐
- Users must know who accesses the end device, for what purpose, for how long, and whether third parties are granted access.
- A list of individual cookies is not required.
- For services and cookies that do not require consent, the supervisory authorities recommend, for the sake of transparency, that they be mentioned in the privacy policy. however, listing them in the consent dialog is not required.

Correct categorization

☐ Services and cookies must be grouped according to their specific and precise purposes. There must be no uncategorized cookies and no “other” category.

☐ **Google Analytics and Google Tag Manager** fall under consent-required services. The reason for this is, in particular, the secondary use of data and the possibility of re-identifying users despite IP anonymization. This also applies without restriction to Google Analytics 4 (GA4)’s so-called Advanced Consent Mode.

In “Advanced Consent Mode,” the Google Analytics (GA4) script is loaded immediately, even before the user has made a choice in the consent banner. If the user refuses cookies (or does not respond), GA4 does not set cookies in the browser, but still sends so-called “cookie-less pings” to Google’s servers.

☐ Cookies used for billing **affiliate activities** are not exempt from the requirement to obtain consent.

☐ Even supposedly privacy-friendly web analytics services such as **Matomo or Piwik PRO** cannot, by default, be used without consent, as they also actively read out, among other things, the user’s screen resolution.

JustRelate

Numerous technical pitfalls

- [ ] The use of separate solutions for consent management and tag management carries a very high risk of incorrect triggering without consent, as each new service must be configured in two different systems. In addition, this requires complex configurations of trigger groups (“trigger groups”) in the tag manager.

- [ ] The setup of a legally and technically correct configuration proves to be particularly challenging in the context of **hybrid tracking** (with and without cookies), the collection of **advanced conversions** (including Advanced Conversions) involving personal targeting data, or **dual conversion tracking** (both via pixel and server-side), which requires strict deduplication of conversion data. The pitfalls are extremely numerous and can lead both to legal violations and to costly configuration errors in the management of advertising bids (ads).

- [ ] Many website operators rely on automatic scanning and blocking functions as well as automated categorization provided by consent management solutions. Although these tools can support manual review processes, they are prone to errors—especially with rarely used services. Caution is also required, as scans are sometimes performed only on a weekly basis, which can temporarily result in a state of non-compliance. Integrated tag and consent management solutions make automatic scanning and blocking functions unnecessary.

- [ ] **Since Google Maps and YouTube** transmit IP addresses and other device data to Google when loading scripts and iframes, and also set cookies, they must not be loaded by default without consent.

  In this case, the use of so-called **content blocking** is recommended: this ensures that, without consent, only a notice about the hidden content is displayed, along with the option to explicitly unlock it through consent.