

# 7 Best Practices for a compliant CMP

According to the GDPR, consent must be freely given, specific, informed, unambiguous and as easy to withdraw as to give. A tool like our CMP can help you to obtain such consent, but there are few things to consider. All in all, it is a website's decision on how to implement a CMP. Faktor has set up a few best practices that helps ensuring compliance.

## 1. Limit your partners

Review all parties that are on your site and check if all of them are adding value to what you are trying to achieve.

## 2. Explain in a simple way why you need your visitors consent

Visitors can be annoyed by having to define their settings on sites. Explain your data processing in a simple, informative and creative way : it will be appreciated and help you to establish trust.

## 3. Ask for consent on vendor and purpose level

Consent needs to be specific so ensure your visitors are able to specifically enable or disable purposes and vendors.

## 4. Include a Reject All button

There are different versions of CMP's. To ensure that it is as easy to reject as to accept cookies you need to include a reject all button.

## 5. Ensure cookies are not dropped by default

Consent needs to be explicit, which means consent buttons can not be on active by default and cookies can only be dropped after visitors have given consent.

## 6. Apply conditional firing

For parties that do not comply with IAB's TCF, you should apply conditional firing to ensure no cookies are dropped before the visitor has made their choice. This can be done through Faktor's Tag Manager and we can support you setting this up.

## 7. Keep your CMP up to date

Run periodic checks to ensure that no third party resources are being loaded without user's consent.

*A CMP can be a massive help to ensure compliance for your site, but be aware that compliance is not a click of a button activity and it is an ongoing process.*