
# Cookie Compliance

Checklist provided by Fort Privacy

June 2020

# Website Cookie Checklist Provided by Fort Privacy

| | |
|---|---|
| **Completed by:** | **Insert Name / team** |
| **Date of completion** | **[TBC]** |
| **Website** | **[TBC]** |
| **Website contact details** | **[TBC]** |
| **Conclusion** | **[TBC]** |

| STEP 1: Cookie Information examined | | |
|---|---|---|
| **Document** | **Yes/No** | **Link / Location** |
| Cookie Banner | | |
| Cookie Notice/statement | | |
| Data Protection statement | | |
| Cookie management tool | | |

| Cookies Checklist | |
|---|---|
| **i. Lawful Basis Consent/Further Processing** | |
| **Establish GDPR Compliant Consent for Cookies**<br>• Ensure there are no pre-checked boxes related to the setting of cookies.<br>• Ensure that the default settings for all non-necessary cookies is set to "off" or "reject".<br>• Ensure that consent is obtained for each purpose for which cookies are set.<br>• Ensure consent is not bundled, i.e. an "all or nothing" approach to accepting or rejecting cookies. Users must be able to reject non-necessary cookies.<br>• Ensure users are able to vary their consent easily at all time via the website.<br>• Ensure that the cookie banners is designed in such a way that they do not 'nudge' users into accepting cookies.<br>• An option to reject must have equal prominence in any banner or user interface.<br>• Ensure there are no accessibility issues with the consent mechanism.<br>• Ensure users are always able to withdraw consent or change permissions for cookies or other tracking devices. | |
| **Using a Consent Management Platform**<br>Ensure when using a consent management platform, that it works in the manner intended.<br>This means that the tools and buttons on the user interface do what they purport to do. If a user checks or unchecks preferences, these preferences must be respected and recorded, as appropriate. | |

| | |
|---|---|
| **Meeting ePrivacy Requirements**<br><br>Ensure all cookies categorised as 'necessary' or 'strictly necessary' meet the strict conditions for either of the two exemptions set out in Regulation 5(5)*<br><br>Ensure that consent is required for all non-necessary cookies including where no personal information is processed.<br><br>* Regulation 5(5): Paragraph (3) does not prevent any technical storage of, or access to, information **for the sole purpose of carrying out the transmission of a communication over an electronic communications network <u>or</u>** which is strictly necessary **in order to provide an information society service explicitly requested** by the subscriber or user. | |
| **Further Processing Cookie data**<br><br>Ensure that the processing of data which occurs subsequent to the setting of cookies is compliant with the provisions of the GDPR, including the provisions relating to data subject rights.<br><br>This is particularly important where subsequent processing involves appending or matching any other data to an explicit profile or an identifier that involves the processing of personal data. | |
| ii. **Retention** | |
| Ensure the lifespan of 'strictly necessary' cookies is proportionate relation to the purpose it is used for and they set to expire once it is not needed.<br><br>"This suggests that cookies that match the [consent exemption criteria] will likely be cookies that are set to expire when the browser session ends or even earlier. | |
| **iii. Transparency** | |
| Ensure data protection and cookie statements are always prominently displayed and easily accessible to the user. | |
| Ensure the cookie information is accessible without the user having to consent to cookies or dismiss a cookie banner. | |
| Ensure the cookie statement includes clear and comprehensive information that includes the purposes of the processing of the information for all cookies that are used. | |
| Ensure the cookie statement is presented to the user with layered information about the technologies in use. | |
| Ensure the cookie statement includes information about how to reject the cookies. | |
| Ensure non- necessary cookies are not set prior to the user clicking on the cookie information | |

| | |
|---|---|
| Where a link to a cookie statement is presented in a pop-up or cookie banner, ensure that the banner does not obscure the text of that policy. | |
| Ensure cookie statements are kept-up to date with accurate information about what cookies are used by the website.<br><br>Ensure associated data protection statements are similarly accurate. | |
| Where the controller has multiple websites ensure that each of them has their own data protection and cookie statements which reflect the underlying reality of the processing. | |
| iv. **3rd Party Cookies** | |
| Examine the possible joint controller issues arising from the use of third-party assets and plugins.<br><br>Ensure that controller-processor contracts, which reflect the actual facts of the processing are in place where required. | |
| Examine the use of other technologies such as web beacons (pixels) and fingerprinting technologies.<br><br>To the extent that any controller uses such technologies, they should be aware that Article 5(3) of the ePrivacy Directive (and by extension Regulation 5(3) of the ePrivacy Regulations 2011) is applicable. Opinion 9/2014 of the Article 29 Data Protection Working Party on the application of Directive 2002/58/EC to device fingerprinting should be studied in that regard.<br><br>Note: these might require a DPIA to be carried out. At the very minimum an LIA will be required. | |