PART2MELT

COOKIE POLICY

2020

COOKIE POLICY

We use technologies on the site **https://www.part2melt.com**

(the Site) to gather information that helps us develop our online experience. In this Cookie Policy, we mention to these technologies, which include cookies, web beacons and gifs, collectively as cookies.

This policy describes the different types of cookies used on the Site and how you can control them. We may change this Cookie Policy at any time. Please have a look at the last effective date at the top of this page to see when this Cookie Policy was last revised. Any changes in this Cookie Policy will become impressive when we make the revised **Cookie Policy** available on or through the Site.

Any personal information that we gather through the use of cookies is got through transparent realize to you and through your consent. Where applicable, we provide you with the opportunity to opt out.

We hope that this Cookie Policy helps you understand, and feel more confident about, our use of cookies. Please also look our Privacy Policy to understand the other aspects in which we apply information we gather about you. If you have any further queries, please contact us **https://www.part2melt.com**

Types of Cookies

In general, there are three different ways to classify cookies: what aim they serve, how long they undergo.

Duration

Session cookies – These cookies are temporary and dissepear once you close your browser.

Persistent cookies — This category encloses all cookies that remain on your hard drive until you delete them or your browser does, depending on the cookie's expiration date. All persistent cookies have an expiration date written into their code, but their duration is able to change. According to the ePrivacy Directive, they should not last longer than 12 months, but in practice, they could remain on your device much longer if you do not take action.

Provenance

First-party cookies — As the name implies, first-party cookies are put on your device directly by the website you are visiting.

Third-party cookies — These are the cookies that are placed on your device, not by the website you are visiting, but by a third party like an advertiser or an analytic system.

Purpose

Strictly necessary cookies — These cookies are essential for you to browse the website and use its features, such as accessing secure areas of the site. Cookies that allow web shops to hold your items in your cart while you are shopping online are an example of strictly necessary cookies. These cookies will generally be first-party session cookies. While it is not required to obtain consent for these cookies, what they do and why they are necessary should be explained to the user.

Preferences cookies — Also known as "functionality cookies," these cookies allow a website to remember selections you have made in the past, like what language you choose, what part you would like what your user name and password are so you are able to automatically log in.

Also known as "performance cookies," these cookies pick the informations about how you use a website, like which pages you visited and which links you clicked on. None of this information can be used to identify you. Their purpose is to develop website functions. This involves cookies from third-party analytics services as long as the cookies are for the exclusive use of the owner of the website visited.

Marketing cookies — These cookies track your online activity to provide advertisers deliver more relevant advertising or to limit how many times you see an ad. These cookies are able to

share that information with other organizations or advertisers. These are persistent cookies and almost always of third-party provenance.

These are the main ways of classifying cookies, although there are cookies that will not fit into these categories or may for multiple categories. When people complain about the privacy risks presented by cookies, they are generally talking about third-party, persistent, marketing cookies. These cookies are able to include important amounts of information about your online activity, preferences, and location. The chain of responsibility (who can access a cookies' data) for a third-party cookie can get complicated as well, only heightening their potential for abuse.

kies and the GDPR

The General Data Protection Regulation (GDPR) is the most comprehensive data protection legislation that has been passed by any governing body to this point.

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which in particular when combined with unique identifiers and other information received by the servers may be used to create profiles of the natural persons and identify them.

What these two lines are stating is that cookies, insofar as they are used to identify users, qualify as personal data and are therefore subject to the GDPR. Companies do have a right to process their users' data as long as they receive consent or if they have a legitimate interest.

Cookies and ePrivacy Directive

Passed in the 2002 and amended in 2009, the ePrivacy Directive (EPD) has become known as the "cookie law" since its most notable effect was the proliferation of cookie consent pop-ups after it was passed. It supplements (and in some cases, overrides) the GDPR, addressing crucial aspects about the confidentiality of electronic communications and the tracking of Internet users more broadly.

Cookie compliance

To comply with the regulations governing cookies under the GDPR and the ePrivacy Directive you must:

Receive users' consent before you use any cookies except strictly necessary cookies.

Provide accurate and specific information about the data each cookie tracks and its purpose in plain language before consent is received.

Document and store consent received from users.

Allow users to access your service even if they refuse to allow the use of certain cookies

Make it as easy for users to withdraw their consent as it was for them to give their consent in the first place.

ePrivacy Regulation

The EPD's eventual replacement, the ePrivacy Regulation (EPR) will build upon the EPD and expand its definitions. (In the EU a directive must be incorporated into national law by EU countries while a regulation becomes legally binding throughout the EU the date it comes into effect.)