INTERNATIONAL BUSINESS SOLUTIONS CONSULTING
COOKIE POLICY

How Data Protection Laws such as the EU cookie law can affect your website's use of cookies

The first data protection law was enacted in Germany in 1970. Since then, the European Union has led the rest of the world in data protection and online privacy legislation. The first comprehensive data protection regulation for the European Union, the EU Directive on Data Protection, was enacted in 1995 and covered the collection, use, transfer, and security of personal information of residents of any European Union countries.

In 2018, the European Union's General Data Protection Regulation (GDPR) went into effect, establishing seven principles that should govern the collection of personal information. These principles are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Any company or individual that processes personal information of European Union citizens must comply with the GDPR, regardless of where data is stored or processed. The European Union is currently comprised of 28 countries with a combined population of over 500 million people, so the GDPR is likely to affect a significant portion of the customer base of any company that does business internationally. In addition, over 80 nations have enacted their own data protection laws that govern the collection and use of personal information.

Websites that are operated solely in the United States or other countries not covered by the GDPR may include a statement warning users that the site is intended only for residents of certain countries. Even if a company is willing to ignore 500 million potential customers however, there is no guarantee that such a warning would be sufficient to avoid possible penalties if the company knowingly collects information about users in EU countries.

Furthermore, while the United States does not currently have a federal GDPR equivalent, several states have enacted their own data protection laws, and new laws are on the horizon. The California Consumer Privacy Act of 2018 (CCPA) goes into effect on January 1, 2020, for many businesses and will require disclosure of any personal information being collected about a California resident. Data subjects residing in California must also be given the opportunity to refuse to allow such collection if the business is subject to the CCPA. Unless a business is willing to eliminate residents of California as well as residents of the EU from their customer base, website operators should be learning how to comply with both the GDPR, CCPA, and other similar legislation that may follow.

INTERNATIONAL BUSINESS SOLUTIONS CONSULTING
COOKIE POLICY

Personally Identifiable Information & Cookies

Personal information is generally defined as any information that can be used to identify an individual, such as a user's name, address, phone number, geographical location, and biometric information. The GDPR also includes a user's IP address under the definition of "personal information." The CCPA will go even further by expanding the definition of "personal information" to include browsing and search histories, online purchase histories, and consumer profile information. Disclosures about when and how personal information is collected, and the rights of data subjects to control the collection and use of their personal information, are usually contained in a privacy policy. Often, though, privacy policies do not address the kind of data that is collected by cookies.

Cookies often collect aggregate information about their users that is not specifically identified with one individual, but if that information, combined with other data, such as a user's IP address or device information, can be used to identify an individual, it becomes "personal information" for the purposes of the GDPR and must be treated as such. Although cookies are not mentioned specifically in the Data Protection Directive and only once in the GDPR, both regulations protect all information gathered about EU residents, including information gathered automatically using cookies or other technologies.

In 2012, the U.K. Information Commissioner's Office published a set of guidelines on the use of cookies under the Data Protection Directive. The I.C.O. is an independent body established by the government of the United Kingdom for the purpose of upholding information rights and governing compliance with data protection and information freedom laws. These guidelines are still applicable under the GDPR and can provide some guidance on how companies' cookie policies can be structured to comply with data protection laws. In particular, the guidelines discuss the importance of providing users with the required notice before information is collected by cookies, and the opportunity to consent to such collection.

INTERNATIONAL BUSINESS SOLUTIONS CONSULTING
COOKIE POLICY

Using Cookies

If a user navigates to any link on a company's home page, even to open the privacy policy, cookies may have already been placed and information collected. Those cookies may collect personal information or may collect data that, combined with other data, could be used to identify an individual. If so, the placement of cookies would violate the GDPR's requirement that users be given an opportunity to consent to the collection of such data.

The clearest and most effective way to notify a user in advance of the collection of information using cookies is to provide a web banner or "pop-up" cookie notice that appears automatically when the home page is accessed for the first time. According to the I.C.O. guidelines, a cookie notice that requires some affirmative action, such as closing a web banner or clicking a consent button, will provide the required notice and ability to consent. An implied consent notification may also be sufficient if the user is notified of his implied consent before any cookies are placed on his device.

Consequences of Not Complying With Data Protection & Cookie Laws

The GDPR authorizes supervisory authorities to impose various penalties, including:

- Issuing a warning
- Ordering a temporary or permanent ban on data processing of EU residents
- Ordering the processor to erase data processed in violation of the law
- Banning the transfer of data to certain countries
- Imposing significant fines

How To Comply With Data Protection & Cookie Laws

Crafting a cookie notice that complies with not only the GDPR, but also with the data protection laws of individual EU and non-EU countries is a nearly impossible task. Fortunately, ready-made cookie disclosures are available. The free and open source Osano Cookie Consent, for example, is designed to comply with the GDPR, current U.S. state data protection laws, including the upcoming CCPA.

With the free Cookie Consent tool, website operators can choose from several cookie notification options, including an "opt-in" disclosure, in which the user must specifically agree to the use of cookies, an "opt-out" disclosure, in which the user is given the option of blocking some or all cookies, and an "implied consent" disclosure, in which the user is informed that his continued use of the website implies consent to the use of cookies.