Are Your Website and Privacy Policy GDPR Compliant?

The European Union's General Data Protection Regulation (the "GDPR") became effective on May 25, 2018. Even if your business is located outside the EU, if it involves the receipt and storage of any personal data, you need to consider the GDPR's applicability. If the GDPR is potentially applicable, you may need to make some changes to your website and the privacy policy posted on it to be sure you are in compliance with the GDPR. In addition, if you rely on consent from individuals in the EU as the lawful basis to receive, store or otherwise process their personal data,[1] you should make sure that the consents you obtain are valid under the GDPR's strict requirements.

Does the GDPR Potentially Apply to Your Business?

The GDPR applies not only to businesses situated in an EU member state. It also applies to businesses and other organizations outside the EU, including in the United States, that receive and retain personal data of persons in the EU to offer them goods or services, whether they pay for them or not, or to monitor their behavior within the EU in some way. The mere accessibility of an ecommerce website to visitors in the EU is not, standing alone, sufficient to subject the website's operator to GDPR jurisdiction. However, if the site contemplates offering goods or services to individual customers in the EU, then it is most likely subject to the GDPR. Factors considered indicative of offering goods and services to EU customers include referring to customers or users in the EU on the website or other promotional materials, enabling payment in one or more EU member state currencies or offering a version of the website in a language spoken in an EU country (but not in the organization's home country, *i.e.,* English for US businesses.) If your business may satisfy the above criteria, then you need to consider the rest of this article.

What Changes May Need to be Made to Your Privacy Policy to make it GDPR Compliant?

The GDPR has introduced some new rights for individuals in the EU whose personal data is stored (called "Data Subjects") and some of the rights that had existed under the now-repealed EU Data Protection Directive have been expanded. The privacy policy your organization posts on its website – and which it must follow – now needs to refer to these rights and inform individuals in the EU of your policies concerning them. Typically, this requires adding a new section to your privacy policy called "Rights of Individuals in the European Union" or something similar.

Rights to which a GDPR compliant privacy policy should refer include:

a. The right to access the personal data the organization is processing, as well as to receive information about the particulars of the processing activities;

b. The right of an individual in the EU to have the personal data concerning him or her be corrected or updated;

[1] Consent is not the only available basis upon which an organization may lawfully process personal data. Other potentially available bases include (a) the processing is necessary to perform under a contract with the EU individual in question, and (b) processing is necessary for the legitimate interests pursued by the organization or by a third party.

c. The "Right to Erasure," sometimes called the "Right to be Forgotten," which enables individuals in the EU to require the deletion of their personal data under certain circumstances "without undue delay." Circumstances that may trigger this right include the data's retention becoming no longer necessary for the purposes for which the data was collected;

d. The right to withdraw a previously given consent to the use of personal data;

e. The "Right to Object" to use of an individual's personal data for some types of "profiling" or automated decision making. This includes the right to be informed if the data subject's information will be used for automated decision making or profiling;

f. The "Right to Portability" in certain circumstances, which includes the right to get a copy of stored personal data an individual has provided and to transfer the data, unimpeded, to another organization;

g. The right to complain to a local data protection authority in the EU if a data subject believes that his or her data is being unlawfully processed.

A GDPR-compliant privacy policy also should advise individuals of the reasons for processing their personal data – typically, to fulfill contracts resulting from orders the data subject has placed – and let the data subject know the procedure for exercising any of the enumerated rights the GDPR provides.

How Must "Consent" to the Use and Retention of Personal Data be Obtained from EU Data Subjects?

The GDPR provides that to be valid, consent must be a "freely given, specific, informed and unambiguous indication of the [individual's] wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Accordingly, the types of passive consent schemes typically used on US websites and in US privacy policies—most often a statement to the effect that use of the website constitutes consent—will not comply with the GDPR. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. There is, however, still considerable uncertainty over exactly what is necessary to obtain GDPR-compliant consent.

Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them." In addition, individuals in the EU have the right to withdraw their consent at any time, and organizations must make it as easy to withdraw consent as it is to give consent.

There is no "one size fits all" solution to how GDPR compliant consent ought to be obtained in the context of an ecommerce site and its privacy policy. Imposing consent requirements that consumers find onerous can interfere with the effective presentation of the branding message and even drive consumers off the site. Accordingly, a happy medium must be reached. A number of different solutions have appeared on websites since the May 25, 2018 effective date of the GDPR. Most involve an initial window presented to the website visitor that either displays the privacy policy or a link to it, encourages the visitor to read the policy and presents a box to check to indicate consent to use of personal data in accordance with the policy. It is very important that the box not be pre-checked. The visitor must check it to indicate affirmative consent.

Cookies present a special case, and are regulated under a different legal regime in the EU – the ePrivacy Directive. Many sites are using a separate window to advise that cookies will be used and to ask for consent by checking a box.

It is also technologically possible to have the website present the GDPR-compliant consent

measures only to visitors from IP addresses within the EU. However, the cost and burden of this may make presentation to all visitors the better solution. In addition, a number of states (notably California) are beginning to pass new, enhanced data privacy statutes that introduce measures similar to some or all of those in the GDPR. Accordingly, it may make sense to begin obtaining GDPR-compliant consent from all visitors.

Your attorney should advise you on the optimal way to approach GDPR consent requirements for your website, so that GDPR-compliant consent is recorded without undue interference with your branding and commercial goals.

What are the Risks of Non-Compliance with the GDPR?

Why should a US-based business worry about compliance with the GDPR? The answer is that it can affect the organization's ability to do business in EU countries. As explained above, businesses based outside the EU may nevertheless be subject to the jurisdiction of EU privacy regulators, if they seek to do business with individuals within the EU. Non-compliance with the GDPR's requirements can potentially involve heavy fines. Fines can be imposed at three different levels. The highest level of fine is the greater of €20 million or 4% of the global annual turnover (i.e., revenue) of a business. However, a variety of aggravating and mitigating factors will be considered. Thus, although fines that onerous may be unlikely for all but the largest and most recalcitrant businesses, the potential for significant fines and interference with the ability to do business in the EU make it worthwhile to make the necessary investment in legal advice to make your website, privacy policy, and privacy protection practices GDPR-compliant.

For more information on the topic discussed, contact Donald Prutzman at prutzman@thsh.com, Michael Riela at riela@thsh.com, any other member of the Firm's Cybersecurity and Data Privacy practice, or the Tannenbaum Helpern attorney with whom you usually deal.

L. Donald Prutzman
212-508-6739
prutzman@thsh.com

Michael Riela
212-508-6773
riela@thsh.com

Drew Jaglom
212-508-6740
jaglom@thsh.com

David R. Lallouz
212-702-3142
lallouz@thsh.com

Beth Smigel
212-702-3176
smigel@thsh.com

Maryann C. Stallone
212-508-6741
stallone@thsh.com

Vincent J. Syracuse
212-508-6722
syracuse@thsh.com

Tannenbaum Helpern's Cybersecurity and Data Privacy practice is knowledgeable concerning compliance with the GDPR and available to assist your business in becoming and remaining GDPR compliant. In particular, we can review your privacy policy and help you institute the method of obtaining GDPR-compliant consent that best suits the needs of your business. We can also assist with other aspects of privacy and cybersecurity regulation.