MDO | PARTNERS
LAW | COMPLIANCE | ETHICS

Insights

TOP 10 GDPR COMPLIANCE TIPS

With the European Union (EU) General Data Protection Regulation (GDPR) effective as of May 25, 2018, companies all over the world are updating their privacy policies and taking other measures to ensure they comply with this important new law. Even if your operations are not in the EU, your company may be subject to GDPR if you collect, store and/or transfer personal data of individuals in the EU. Failure to comply with GDPR may subject your company to fines equal to 4% of global revenue. Below are ten helpful GDPR compliance tips that companies should adopt to help comply with GDPR and minimize risk, fines and penalties.

1) Document the "Personal Data" You Collect

Under the GDPR, "personal data" means "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier" (e.g. date of birth, email, home address, identification numbers, etc.). Companies should document what type of personal data they collect, where it originated and who they share it with.

2) Identify the Purpose of your Data Collection

The GDPR requires companies to have a lawful and specific purpose for collecting personal data. Moreover, they must provide information about why they collect the personal data of individuals. As such, companies must have detailed explanations about why such personal data is being collected and be prepared to disclose it in their privacy policy or upon request.

3) Determine and Disclose How Data is Stored

All companies subject to the GDPR are required to disclose to individuals how they store the personal data collected. For that reason, and for cybersecurity reasons, it is advisable that every company select the most appropriate data storage option for their business, whether on a company's server or with a third-party data storage provider. The key is to disclose it and explain how this decision was made.

4) Issue a Clear and Concise Privacy Notice

Companies need to explain how they are complying with the GDPR. The best way to communicate such compliance is by issuing a clear and concise Privacy Notice to the individuals whose personal data it collects. The Privacy Notice should address:

- What is the GDPR;
- Why it applies to your company;

- What measures your company is taking to comply; and
- How can the individual contact you with questions.

5) Update your Privacy Policy

The privacy policy is the cornerstone of a company's privacy compliance program. Companies should update their privacy policy to ensure it satisfies the key elements of the GDPR. Specifically, the policy should indicate the specific purpose for which personal data is collected, as well as how such data is stored and used. Companies must ensure that individuals accept the terms of the privacy policy.

6) Obtain Consents and Permit Withdraw

The GDPR requires companies to secure specific consent from individuals regarding the collection, use and transfer of their personal data. It also provides them with an explicit right to withdraw such consent. Accordingly, companies must provide the mechanism for obtaining and documenting such consents. Further, you need to ensure individuals are provided with an opportunity to withdraw his/her consent for the company at any time they collect personal data.

7) Deliver GDPR Training

Training is a critical component to any effective compliance program. With the changes to the privacy policies and procedures under the GDPR, it is important for companies to train their key personnel to ensure they will abide with the new protocols designed to comply with GDPR. Companies should invest the time and resources to prepare and deliver thorough training on key privacy policies and procedures to employees.

8) Prepare to Honor Privacy Rights

Under the GDPR, individuals have broader rights over their personal data stored by a company. As such, companies should be prepared to respond to individuals who exercise such rights, including the right to have their personal data deleted, corrected, and transferred, and the right to object to profiling regarding. If applicable, companies may need binding corporate rules for organizations to lawfully transfer personal data outside of the EU. In addition, companies must provide the contact information for the person responsible for data collection and storage in the company.

9) Maintain Records of Compliance Efforts

The GDPR imposes serious fines on companies that fail to comply the law's requirements. For that reason, companies should maintain adequate records of their compliance efforts, including any updates to policies and procedures, logs of trainings delivered, investigations and reporting of data breaches. Doing so, will strengthen a company's defense in the event an individual or government agency challenges your compliance with the GDPR or the adequacy of your privacy compliance program.

10) Establish Data Breach Response Procedures

The GDPR requires companies to report certain data breaches to the Information Commissioner's Office (ICO) after becoming aware of a breach, and in some cases may be required to notify individuals. To address these requirements, companies should establish data breach response procedures to help detect, report and investigate data breaches. Failure to report such breaches can result in fines, penalties and other liability.

In light of the enforcement of GDPR, it has become critical for companies to enhance their Privacy and Data Protection Compliance Programs. Companies should be updating their policies and procedures to protect sensitive information and personal data. MDO Partners encourages companies to adopt the tips outlined in this article and assess what other privacy measures may be required to comply with GDPR and other applicable privacy laws. Our attorneys and advisors have experience advising clients on privacy as well as cybersecurity matters. We can assist companies in establishing effective privacy compliance programs.