Cybersecurity & Data Privacy

STRATEGIC THINKING AND PRACTICAL LEGAL ADVICE

5 Considerations for General Counsel Regarding the EU General Data Protection Regulation

The European General Data Protection Regulation ("GDPR") entered in force on May 25, 2018 ("GDPR Day"). The GDPR sets forth a new regime for the protection of personal data in the European Union ("EU"). We briefly discuss below five things that general counsel should know about the GDPR, including lessons learned since GDPR Day.

Choose and Document Your Choice of a Lead Supervisory Authority

Cross-border processing is processing that is conducted by an EU-based organization whose activities occur in more than one EU member state or that "substantially affects" or is "likely to substantially affect" data subjects in more than one EU member state. In such instances, the supervisory authority of the "main establishment" or of the "single establishment" will act as the lead supervisory authority ("LSA"). Put simply, a company's LSA is the authority with the primary responsibility for dealing with the company's cross-border data processing activities. (Non-EU based entities do not benefit from such "one-stop-shop" mechanism.)

The determination of the LSA is not always easy. When you have identified your LSA, documenting your choice is important since the determination may be challenged by the supervisory authorities.

Review Your Data Processing Agreements

The GDPR requires data controllers to use a certain level of care in selecting data processors. For example, controllers should appoint processors that provide appropriate technical and organizational measures to comply with the GDPR. The GDPR also requires certain obligations to be included in the controller's data processing agreement ("DPA") with a processor, so setting clear obligations for a processor facilitates compliance with the GDPR.

When dealing with a data breach, for example, controllers have to rely on the actual provisions of a DPA that describe the steps that the processor should take to assist the controller and the level of information regarding the breach that the processor needs to provide to the controller. Avoiding vague clauses in this regard and having in place detailed provisions will allow a controller to more efficiently handle a data breach. The same is true when having to respond to data subjects' requests.

Manage Data Breaches Properly

In anticipation of GDPR Day, organizations developed breach procedures and response plans to notify authorities of data breaches. It is important to have procedures not only to detect, respond and manage a breach but also to assess the risks that the breach creates. This is because

organizations are required to communicate a breach to the affected individuals if the breach is likely to lead to a "high risk to the rights and freedoms of individuals."

Controllers' engagement with supervisory authorities is important—and challenging. Keep in mind that there are no truly "off the record" conversations with supervisory authorities about data breaches. However, there are instances where conversations with supervisory authorities are helpful, for example, when dealing with a notification that has to occur in phases.

Ultimately, organisations will be assessed on how they are managing breaches.

Handle Subject Access Requests Carefully

Among other rights, individuals have the right to request access to and obtain a copy of their personal data (referred to as "subject access requests" or "SARs"). Such rights can be exercised through a verbal or a written request, and organizations must respond, in principle, within one month.

Responding to these requests creates administrative work—and risk. For example, responding to a request may lead to data mishandling (e.g., a controller handing over personal data to an unauthorized recipient). Hence, developing processes to identify the necessary level of information that must be presented in order to verify an individual's identity before fulfilling the SAR will mitigate such risk. Further mitigations measures include conducting staff training, centralizing the tasks of responding to SARs and developing template letters to respond to SARs consistently across an organization.

Be Aware of New GDPR-Like Laws

The GDPR has inspired a number of similar laws in other countries, including Brazil, the United States (in the state of California) and India (whose law is still in draft form). While these laws have similarities to the GDPR, they also have substantive differences, including different requirements, from the GDPR. Therefore, compliance with the GDPR will not necessarily ensure compliance with these GDPR-inspired laws. Similarly, compliance with these other laws will not ensure compliance with the GDPR. However, companies can leverage any work done to comply with the GDPR to reach compliance with these other laws.

For more information about these topics, please contact any of the following lawyers.

Diletta De Cicco
+32 2 551 5945
ddecicco@mayerbrown.com

Charles-Albert Helleputte
+32 2 551 5982
chelleputte@mayerbrown.com

Lei Shen
+1 312 701 8852
lshen@mayerbrown.com