Surviving the second wave of GDPR

The European Union's General Data Protection Rule (GDPR) went into force on May 25, 2018. It triggered the "night of a million cookie warnings" as companies tried to demonstrate at least minimal compliance. The unintended consequence was the "day of a billion reluctant clicks" by people who didn't read the warnings because they wanted to get to all their free stuff.

So, done deal. GDPR is now in the rearview mirror. If only that was true.

GDPR compliance is a process to be undertaken not a state to be achieved and it has only begun. A body of case law will be developed over the coming years based on lawsuits already filed and others yet to come. The regulations themselves will be clarified, updated, and possibly expanded. Regional variations will become evident as member nations interpret GDPR within the framework of their legal systems. And, GDPR will become a template for the implementation of new privacy regulations such as the California Consumer Privacy Act.

What is the best way to build your own GDPR program on these shifting sands?

Today, companies may find themselves in one of three general categories. First, those (primarily large) companies that expended significant resources to understand and comply with GDPR. Second, companies that made a partial but honest effort to comply. Finally, those that did little or nothing or believe they are not subject the regulations.

The key starting points for all these companies is continuous analysis and triage. Even the largest companies need to regularly analyze their policies in order to adapt to the changing landscape. Triage is important because many companies do not have the knowledge or resources to do everything right away. They need to understand where they are not in compliance, what they need to do to achieve it, and develop a roadmap to get them there. While legal analysis is an important part of the equation, risk management also involves a business judgement. Understanding the regulations and balancing costs and benefits are the keys to triage.

What does triage entail? The obvious starting point is all previously identified issues that have not been addressed. Some companies undertook a significant compliance effort managed by internal staff or an external consulting firm. The findings of these analyses often result in a gap analysis and implementation roadmap.

Unlike a traditional gap analysis, a triage assessment does not attempt to identify every area of non-compliance. An intrinsic assumption behind the GDPR is that companies should take a risk-weighted

approach to compliance. Accordingly, a company that can demonstrate that it is taking an intelligent approach to prioritizing its compliance might well avoid regulatory penalties, even if it is early in implementing that roadmap.

A triage effort includes steps like the following:

1. Identify the three to five most critical areas of non-compliance
2. From these critical issues, select the one to three that have the best cost/benefit ratio
3. Develop a roadmap for how to address each of these issues

Any triage effort should include a fresh look at any "legitimate Interest" claims made by the company. Under GDPR, when processing data companies may weigh their legitimate interests against the privacy interests of the data subject. GDPR makes clear that the controller has to jump through additional hoops if it wants to rely on legitimate interests as its lawful basis for processing. And several regulators have already issued guidance to the effect that a formal legitimate interest analysis is good proof that a controller actually jumped through those hoops.

Many companies in the US appear to be relying upon legitimate interest, at least for the time being. But few of them have any formal backup for this decision. Once a few companies are sanctioned for relying upon legitimate interest without the supporting backup, the area will become a frequent area of focus for regulators.

One final thing to consider in a triage effort are any new initiatives underway within the company. For these, it is important to consider GDPR from the start. A Privacy Impact Assessment analyzes the impacts of a new technology upon the privacy rights of the individuals who will be affected by that technology.

A PIA is required when a new technology might pose a "high risk" to privacy. While this sounds like a high bar, many companies perform PIA's as a preventative measure, so that they can demonstrate to regulators that they did their homework. PIAs are not limited to groundbreaking inventions; the same standards apply to incremental product features, if those new features substantially change the privacy exposure of customers (or of third parties).

GDPR compliance is a process not a destination. Determining what steps to take now require a combination of legal and technical insights governed by sound business judgement. Wherever you company finds itself today, it is important to move forward intelligently and document each step.

MARLBOROUGH STREET PARTNERS

Marlborough Street Ventures LLC
6 Stonybrook Road
Westport, CT 06880
W: www.marlboroughst.com
E: info@marlboroughst.com