Strategic Perspectives

Wolters Kluwer

January 24, 2018

Part Two: Practical Ways to Comply with GDPR in Time for May 2018 Implementation

By Cynthia J. Cole and Neil Coulson, Baker Botts LLP*

This is the second of the two-part series of articles looking at the impact of Europe's new General Data Protection Regulation on U.S. companies. In this article, Cynthia Cole and Neil Coulson examine practical compliance steps that U.S. companies can take to ensure that they are ready.

Once a company has determined that Europe's General Data Protection Regulation (GDPR) applies to its data protection and storage practices, it must quickly implement appropriate measures in order to become compliant before the Regulation take effect on 25 May 2018.

Where previously companies may have assumed the risk of data breaches as part of the overall cost of doing business, now the penalties are so steep that noncompliance may endanger the company's ability to remain in business as a practical matter. There are practical steps a company can take now to minimize its risk.

Step 1 - Internal Audit: Does GDPR Apply?

As explained in Part I, first a company must assess whether GDPR applies. GDPR extends beyond the borders of the European Union to any companies which touch the personal data of people living in Europe, no matter where those companies are incorporated or located.

Any company which collects information through which its customers or potential customers in the EU can be identified (for example by data entry onto a website) needs to conduct a thorough internal audit. If a company offers customers residing in Europe any goods or services for sale online, they too should perform an audit to see which of their practices may need updating before 25 May 2018. As we explained in Part I, what constitutes personal data is widely defined. IP addresses are within that definition, so if a company captures the IP addresses of its website users it needs to be careful.

Step 2 - Top Down Company-Wide Cultural Shift

Under GDPR, if a consumer's data is held and used by the company, it must be done with the express informed consent of the customer that extends to all uses of that data by the company.

---

* Baker Botts partner Neil Coulson is the Department Chair - Intellectual Property in London and Moscow. Cynthia J. Cole is Special Counsel in Palo Alto in Baker Botts corporate, technology and privacy and data security practice groups.

This presents a drastic shift in how companies, especially American ones, have traditionally viewed data. Going forward, US companies must ultimately consider data and data protection through a wider, more global lens that encompasses GDPR's basic tenets regarding personal privacy. As an anecdotal example, companies are now looking at implementing GDPR compliance as a global standard for their operations.

In order to accomplish this shift, it is likely that basic procedural changes will need to be built into the company's online and data storage practices. However, these changes are more than logistics: they must arise from a cultural change in how ownership of personal information is perceived.

New concepts of personal privacy will need to be integrated into the everyday business practices of the organization, across all departments handling personal data. It's not just an issue for legal. It cuts across all a company's business units. Final responsibility for these changes must come from the Board of Directors and flow down throughout the organization.

Increased Board Oversight and Responsibility

Compliance should be viewed as a company-wide issue. An effective evaluation will consider all possible customer touchpoints within an organization, including not only the customer base but also the supplier base and all geographic locations.

After 25 May 2018, board members will no longer be able to deflect responsibility for GDPR compliance to an organization's IT group, legal department or information officers. Data use and storage and, more dramatically, data and cybersecurity hacks impact multiple aspects of the company's business, including operations, business relationships, compliance/disclosure obligations and costs.

What should a board do? While each company operates under its own set of circumstances, every board should consider and implement prudent business practices which acknowledge that the company has increased obligations to a data subject, and that a data subject has increased rights in relation to his/her personal data.

Logistical Modifications and Contract Review

Some logistical changes that companies have implemented include transferring data services to a cloud service provider or a third-party hosting service. Sometimes these services may also be transferred to a different branch of the organization.

Whether these responsibilities are transferred internally or eternally, it is still highly likely that the organization will be dealing with EU residents' personal data. Therefore companies must be extremely careful about what obligations are being assumed (if the personal data is received from a third party) or imposed (if the personal data is provided to a third party) and address these obligations and any possible breaches in contractual language.

An important segment of the internal audit should cover review of all contracts pertaining to data collection and storage, and clarification of respective responsibilities. For example, companies should look at the assignment of liability to, or receipt of an indemnity from, a third party service provider for any breach.

Step 3 - What Data Protocols Do We Have?

Remarkably, many companies do not even know the full extent of the data they have collected, or the reach of their data protocols across departments and subsidiaries. Oftentimes, management may have found it too cumbersome or expensive to determine, consolidate or make consistent the various ways of handling data across the company.

Management needs to have internal discussions representing a wide range of the company's job functions regarding the data collection and data use that the company is making. This discussion should include:

- What disclosures and liabilities is the organization is taking on?
- What is the department and organization's comfort level with these new responsibilities?
- Do we understand and agree with the representations made in our contracts going forward, including issues of liability?
- What can our organization do now and what we can do going forward in terms of data collection?

This kind of self-analysis can be quite difficult for many companies to conduct effectively. However, this scrutiny must be applied vigorously on a company-wide level in order to be prepared for GDPR.

Don't Forget to Review Future Capabilities

For companies in the technology and emerging markets, the audit should asses not only what the technology used by a company currently accomplishes, but also its possible future capabilities for the collection and storage of personal information.

For example, a company should examine its approach to local storage, both when it is providing its customer support service and remote access to that support. The analysis here is also two-fold: first, what can a company allowably do with a consumer's personal information? And next: what future data access protocols are in place and what will their capacities be? A company's self-audit examination does not end with what technologies an organization is able to access today but must look ahead to what technologies it may be able to access in the future.

For international companies, this may require a shift in policy that effects all customers, not just those residing in the European Union. The complications inherent in erecting a two-tiered system, with different data requirements for EU and non-EU residents, are too cumbersome and costly to be worthwhile, plus might pose an unreasonable risk of treating protected data incorrectly.

Can an Organization Rely on Disclosures?

Once it is determined that the company must comply with GDPR, it must create protocols by which customers who choose to opt out may easily and quickly do so, and it must be able to provide proof that the customers' wishes have been followed.

GDPR emphasizes the need for transparency and fairness. A company must explain clearly what it intends to do with the information it asks for and how long it will hold it.

A company's disclosure language should be clear and accurate, and its online placement should be easy to find (not hidden in small print in footnotes for example). With clear and prominent text laying out the terms, a consumer can then click "I Agree" as an affirmative indication of consent. This kind of protocol is likely to be sufficient under the new regulations.

Companies should work with both their legal and communications departments in addition to their web and graphics consultants to ensure that the disclosure content and process is easy to understand, straightforward and non-ambiguous.

The best disclosures utilize easy-to-follow steps where the subject can reasonably understand what they are being asked, and can unequivocally accept.

Conclusion

Companies can limit their risk of non-compliance by taking the broad approach in their data usage disclosure; this strategy creates a proactive defense in the case of a challenge. Without a wide-ranging approach to all aspects of data use and collection, the company's risk of liability increases considerably.

In the worst-case scenario where an organization is investigated for breach of GDRP, the company may mount a viable defense if it has put in place reasonable procedures. A strong paper trail showing an in-depth audit, new hires specialized in data protection and new internal procedures (with board-level oversight) will demonstrate a good faith attempt to mitigate risk and may well help defend against the onerous penalties of failing to conform with GDPR.