Legal Insights

Wolters Kluwer

December 2018

How Banks and Regulators Are Already Re-shaping GDPR Requirements – Seven Lessons for You

By David R. Owen, Cahill Gordon & Reindel LLP

Many in the business community seem to be suffering "GDPR fatigue," a syndrome marked by growing disinterest in the EU's General Data Protection Regulation – especially now that the implementation deadline has passed.

Be warned: that perspective carries increasing risk.

Both regulators and the global business community – including financial institutions – are focusing more closely on these new privacy and data protection rules. Their efforts have wide-ranging implications for every type of firm, no matter a company's geographic footprint or its distance from the information economy.

Just last month, the United Kingdom's Information Commissioner's Office (UK ICO) issued a wide-ranging report to Parliament on its investigation into the abuse of personal data.[1] The report includes details on the first publicly-known enforcement notice under GDPR and offers an in-depth look at how officials are interpreting this new regulation.

Meanwhile, financial institutions and the global business community are incorporating consumer and employee privacy standards, including GDPR, into their own due diligence and decision making, weighing these increasingly-complex risks among their lending and in their business partners.

As a provider of cyber and privacy due diligence advice to many of the world's largest banks, I have increasingly seen GDPR compliance utilized as a key assessment item, sometimes serving as a proxy for the broader privacy and security environment. Before underwriting new debt or equity, today's leading financial institutions want to know clients are meeting GDPR and other privacy standards.

And, no type of business has been spared. Banks are applying these standards not only to consumer-facing businesses and data-related firms, but to every company that takes advantage of the ever-increasing availability of digital information. As a result, GDPR and related privacy issues are likely to touch every modern organization.

---

1 https://ico.org.uk/media/action-weve-taken/reports/2260277/investigation-into-the-use-of-data-analytics-in-political-campaigns-20181107.pdf

Yet even as GDPR is incorporated into the fabric of major business decisions, an October survey by the International Association of Privacy Professionals confirmed my anecdotal evidence of GDPR fatigue. More than half of the survey's 550 respondents in the business community said they are "far from GDPR-compliant," while only three-quarters believed the regulation applied to their company.

Whether a laggard or a leader in GDPR implementation, every company must operate consistent with the expectations of financial institutions and the wider business community. Yet the expectations of this community are not static, and instead evolve with new regulatory activity. In that context then, the UK's ICO report offers seven critical lessons.

First, the UK ICO sent a clear jurisdictional message: regulators will not hesitate to target firms anywhere in the world if EU citizen data is involved. One the regulator's primary targets, a data analytics firm called AggregateIQ Data Services (AIQ), was headquartered in Canada. All businesses, no matter its location, must take heed.

Second, regulators will offer no amnesty to businesses that acquired personal data before GDPR's implementation deadline. The regulators consider personal data of E.U. citizens relevant if firms "continued retention and processing" of the data. Indeed, older pre-GDPR data is likely to be particularly suspect. Firms the world over need to assess the data they hold, no matter when they first obtained it.

This leads to the third recommendation: firms must conduct a comprehensive, enterprise-wide GDPR impact assessment, if they have not already. Given the current regulatory focus, big data companies should take particular care – as should any company that has obtained any user data from such businesses. The best impact assessments offer at least 60 questions designed by experts, to guide the process. Software tools and consultants can provide additional assistance. Only through such an assessment can firms determine their exposure to GDPR-related risks.

Fourth, firms must review how they collect and process data, including any personal data relating to employees, customers and business partners. While this will be part of any comprehensive assessment, the subject bears particular emphasis given the UK ICO report. Firms must know the terms of use under which any personal data was retrieved and the date the data was retrieved. Those records must also be available, in case of a regulatory or due diligence inquiry. Firms cannot use personal data in unexpected ways, or outside the terms of use. If any user data was bought from third parties or harvested from open sources, companies must cross reference the third parties' relevant disclosures at the time the data was collected, and compare those terms with their own practices.

Fifth, firms must consider whether re-consent of data-subjects is required. Where customer or personal data is used in marketing or other solicitations, re-consent is necessary if the data is utilized in ways not explicitly covered by prior consent. Remember also, re-consent is not required if the data was acquired by the firm "during the course of or during negotiation for sale" and the terms of consent match current practice. If current practice does not match the terms of consent, or consent records are missing, then a company holding or processing personal data of E.U. citizens must re-consent them.

Sixth, firms must act expeditiously. GDPR hold-outs face increasing dangers, of which future enforcement actions and costs are only one element. The new and expanding regulatory and enforcement apparatus also amplifies firms' reputational and headline risks. In addition, as privacy compliance becomes ingrained in underwriting, banks and others will treat ongoing compliance efforts and review as an indispensable element of their investment decisions. Also, corporate boards will be under increasing pressure to promote corporate responsibility on these issues as part of their fiduciary duty. They, and the executives they designate responsible (another requirement under GDPR that is too often ignored), must have an emergency response plan in place if data gets lost or stolen, or something else goes wrong.

Finally, firms must ensure they are staying abreast of the changing regulatory landscape – a challenge which will continue to shift as technology evolves. Written laws and regulations are static, but technology stands still for no one. As a result, expect GDPR regulators to consistently re-evaluate and reorient their priorities in an attempt to keep pace. And expect the requirements of banks and financial institutions to evolve with those regulatory activities.

Those who refuse to evolve with these changes could someday find their GDPR fatigue is, in fact, fatal to their business operations.

ABOUT THE AUTHOR

David R. Owen leads Cahill's privacy and cybersecurity practice, advising leading financial institutions and global corporations including boards of directors, audit committees and officers in connection with privacy and cybersecurity law. David is qualified as a Certified Information Privacy Professional (CIPP-US) by the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community. David also advises clients on significant litigation, investigation and regulatory matters covering a broad range of legal and factual contexts including federal and state securities laws, banking laws and regulations, as well as insurance and reinsurance litigation in state, federal, regulatory and arbitration jurisdictions throughout the country and internationally.