CYBERSECURITY LAW & STRATEGY

AUGUST 2018

General Data Protection Regulation: Defense or Offense?

By Nina Cunningham

IT professionals everywhere now know that new data protection rules — the General Data Protection Regulation (GDPR) — went into effect on May 25th across Europe, changing how organizations treat personal data. This was the first overhaul since the EU's Data Protection Directive in 1995, shortly after the EU was established. Ostensibly, GDPR's mission is to strengthen and unify the EU's protection of online privacy rights and promote data protection for citizens of the 28 countries currently in the EU. In the global economy, however, GDPR serves as an alarm to all countries with business flowing across Europe and well beyond. Where business flows, data follow.

While GDPR is not currently in political debate, we should watch for this debate to bubble up. Staving off expanded EU policy from Britain survives as a BREXIT issue, and GDPR may urge other sovereign nations to question this expansion as well. It is a reminder that the EU is the policy-making umbrella for its member states. Initially, GDPR was welcomed by organizations having experienced data breaches and even more by affected individuals. A deeper concern is how the regulation will be imposed beyond the EU and how businesses and individuals will be affected as the umbrella opens to include other countries in the global economy.

Wired UK offers much commentary on GDPR, pointing to the confusion that remains largely because there is policy without corresponding implementation plans. With BREXIT in mind, it seemed important for the UK to respond early and independently. But as Clare Hopping pointed out in UK's IT Pro's online report: "GDPR won't only apply to UK companies while Britain remains a part of the EU. That's because GDPR is not dependent on whether or not a company is based in a member state. When the legislation comes into effect it will apply to any organization processing or using EU residents' personal data." The UK Data Privacy Act received Royal Assent and became law on May 23rd, immediately ahead of GDPR.

Compliance Challenges

While everyone seems to understand the goals as privacy, protection, and data-owner control, not the least of the difficulties has been prescribing the technical requirements to reach the desired outcomes. Organizations have been left largely to their own devices to invent, copy, or purchase programs that would complement their own current infrastructures and meet regulations they know to be imposed on all organizations trading in the global market.

It is still a challenge to understand precisely what is required of organizations, and a greater challenge to find specific avenues for compliance. The UK law represents a middle ground between the EU imposition on member states and countries who comply out of business necessity. Many of the requirements are loosely construed and IT departments are likely to struggle for solutions that demonstrate strong governance and meet regulatory requirements. They must follow GDPR principles of privacy but also interpret those principles with technical applications that allow their firms to monitor and control the use and flow of personal data. Nuts and bolts must complement existing systems and applications while carefully including legacy programs.

Another Point of View

In April, Luke Irwin reviewed this topic at IT Governance UK Blog. Irwin points to GDPR Article 32 as mandating that organizations implement "appropriate technical and organizational measures" to manage risks. The blog advocates vulnerability scans and penetration testing and offer a free webinar on penetration testing as a compliance solution. Nothing more technical is prescribed.

A plethora of recommendations are available from IT professionals on how to comply with the new regulation. Organizations look for technical advice within certification standards, such as the ISO 27001 standards on information security. In May, the IT Governance UK Blog introduced ISO 27001 distance learning. The UK's independent public interest authority, the Information Commissioner's Office (ICO), issued a paper on the 12 steps of compliance, with a Self-Assessment Tool for organizations. The fulfillment techniques still ignore technical requirements.

The vagaries of GDPR will preoccupy the IT industry for some time as it works out the fine points of interpreting and implementing required practices. Largely, they need to adapt to the on-going risk of liability and the accompanying dangers of abuse. Failures in compliance will be felt immediately by multinational data-centric organizations in the form of heavy financial penalties, and organizations everywhere with customers and data traveling the globe will want to avoid liability.

A Stamp of Approval?

At some point it will be useful for organizations to assert themselves as *GDPR Compliant* with a formal stamp of approval. Many recommendations have been laid out and claims made as to what compliance entails, but to date there is no board that certifies an organization as *EU GDPR Compliant.* The lack of technical requirements precludes it. Nonetheless, new companies and old offer opportunities to become EU GDPR Compliant. Some, such as UK's Trust-Hub, offer a suite of products to fulfill the requirements, so compliance may be achievable.

A blog at Trust-Hub describes their platform offering to fully protect and store data within the meaning of GDPR (and all it hopes to achieve), and points to the heavy financial penalties for non-compliance. There is no risk management through insurance, as insurance companies are unlikely to insure what they cannot predict from past experience or actuarial measure. Because data breaches must be disclosed as a matter of law, an organization's brand may be affected for the long-term. Liability notwithstanding, cyber-threats are real and in an uncertain world the threat of a breach remains.

Examples of reputational harm and huge costs from liability are the data breaches at Experian and Equifax, two high-profile credit rating bureaus. They show how vulnerable companies can be when uninsurable. While it is not certain that the U.S. will follow suit with the severe penalties imposed by GDPR, companies will need to be aware of the costs if they intend to do business worldwide. Yet the nature of the liability and what entities are liable are far from clear.

The wider the community of attack and deeper the databases, the more difficult it is to assign liability when these breaches take place. Vast amounts of money are deflected from the bottom line of corporations and government agencies, and individuals are rendered helpless when merely carrying on the business of the day. In GDPR there are only two responsible entities, the *data processor* and the *data controller*. With enormous data breaches at credit rating agencies and unlimited liability for risks imposed by GDPR, firms could find it tough to accept credit cards or permit new customers to apply for credit. Credit cards are used globally, so it is difficult to imagine the workings of the worldwide economy with unlimited data at risk and unlimited liability for the consequences. Does GDPR help or further hinder the world marketplace?

Phil Lee of Fieldfisher addressed the issue of uncertainty attached to unlimited liability for creating business agreements in the age of GDPR. Even a year ago, he pointed out in a post that GDPR is *eerily quiet* on the issue of what entity is liable for a breach and is assessed the fine. With only processors and controllers, each will have to blame the other and fight it out.

There is earnest effort to offer a positive spin on this body of regulation. After all, it seems to give power to the people, including the so-called *right to be forgotten*. It offers transparency in the form of a 72-hour breach reporting, stronger consumer consent, and high fines by authorities for putting customer data at risk. At the same time, it puts the burden entirely on the global marketplace, where the deep pockets of industry are held capable of absorbing the costs. Little seen are the certainty of gridlock and the chilling effect on contracts, agreements.

Trust-Hub is opportunistic regarding compliance with GDPR, a great starting point for staying ahead of competition and building trust with consumers. Under global privacy regulations, consumers are mere *data subjects*, the favored term in the protection industry for individual persons. Despite this appellation, Trust-Hub sees consent of the consumer to be only a *formidable* but not insurmountable challenge. The means of achieving trust are unclear.

Formidable is probably the operative word. In the full text of GDPR, there are 99 articles setting out the rights of *data subjects* and obligations placed on organizations covered by the regulation. Solution providers may sell a path out of uncertainty with consumers, but the *competition* is equally subject to GDPR. Many will end up in court to sort out liability between data processor and data controller. There is uncertainty as to where enforcement will come from, how consent will be gained, monitored and measured, and what happens when companies worldwide are hit by an attack that is not yet within the professional imagination to ward off or guard against. This creates a reasonable incentive for law firms to be as global as possible as complaints about breaches come up in the EU countries and others with complementary law.

In December 2017, *Forbes*' Tech Council reported on the territorial scope of GDPR, saying it would *not* apply when data is collected for EU citizens outside the EU. The U.S. may feel safe under GDPR, but most of the literature suggests liability begins *at the site of the data subject*. This makes precedent the author's earlier suggestion that "any U.S. company that has a Web presence (and who doesn't) and markets their products over the Web will have some homework to do."

Solutions

Whether negative or positive, wrought with terror or offering a panacea, a multitude of firms offer solutions for compliance with GDPR. But they do not resolve the uncertainties. With the threat of non-compliance so high, the cost of investing in a packaged solution seems small. Simply comparing the certifications each product has earned may be enough to mitigate the uncertainties of regulations and directives that present more questions than their imperatives might suggest. The Securities & Exchange Commission announced such a directive in February this year in Press Release 2018-22, and detailed it in their Interpretive Guidance on Public Company Cybersecurity Disclosures. Will interpretive guidance be provided industry by industry?

Packaged solutions look better all the time. No doubt companies offering comprehensive compliance solutions will over-promise; often it will be hard to tell. It is incumbent on IT professionals who purchase these products to ask the right questions about how those promises are backed up, what each certification means, how the software is updated as the threat environment evolves, and how weaknesses in the purchased services will be overcome. All this adds to the challenges of negotiating contracts and moving on with business.

Law firms need guidance as much as any entity in this abyss, but they also must be able to provide it. They need second opinions from consultants who say they can design a solution, from IBM to Clark Hill

Strasburger's new Cybersecurity Consulting team. It is very possible no two opinions will match. Nonetheless, actions taken may be noticed and monitored, so it is probably critical to act on behalf of a company, customer, and client with the same zealous effort expended on a client in any attorney-client relationship. Avoiding liability is a great incentive for treating data with care. As such, it seems much better to treat every customer as a client in a confidential relationship than as a mere *data subject* in an unknown transaction.

*****

Nina Cunningham, Ph.D., is an affiliate of Altman Weil, Inc., and president and CEO of Quidlibet Research Inc., a global strategic planning and cost management firm founded in 1983.