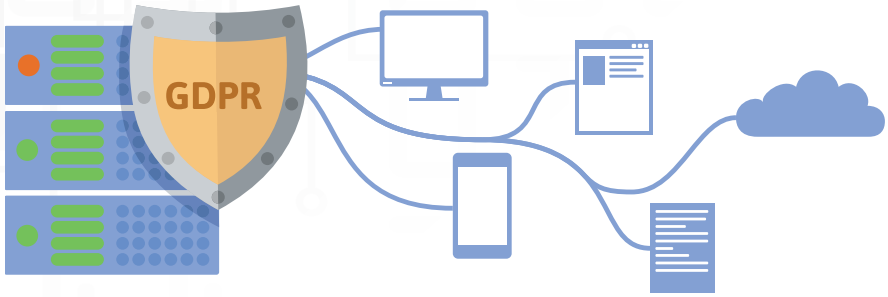
The European Union's New Data Privacy Law:

A Very Different Approach



There are, occasionally, changes in law or regulations that can accurately be characterized as shifts in "paradigm." The recent elimination of "net neutrality" may be one of these shifts. The trend away from federal government regulations, particularly those protecting consumers, might be another shift. In the world of cybersecurity and the legal standards of care currently in place in the US, the European Union (EU) has taken a new and sufficiently different approach to qualify as such a paradigm change.

By way of background, and as described in previous articles, cybersecurity protection under US federal and state laws has been a "patchwork." On the federal level, there are 16 separate statutory schemes imposing duties upon individual industries. For instance, financial institutions have the Graham Leach Biley Act (GLBA) while health care entities have the Health Care Insurance Portability and Accountability Act (HIPAA). Additionally, government contractors, especially Department of Defense contractors, have very high levels of required cybersecurity protection built into their respective Federal Acquisition Regulations. Federally supported education institutions, telecommunication companies, federally subsidized housing, and even federal retirement plans have targeted cybersecurity requirements.

Currently, 48 states have also enacted their own individual cybersecurity statutes.

A problem with the US patchwork approach, particularly for lawyers attempting to identify applicable standards for business clients, is that businesses may be subject to many of those statutes simultaneously. Worse, the statutes are not uniform and indeed are often conflicting. For example, these statutes use different definitions for protected data and "breach." The statutes impose different notification requirements and varying degrees of protection and penalties. Furthermore, some statutes allow for individual causes of action based on statutory violations, while other statutes require government enforcement.

The EU's GDPR

Effective in May of 2018, the EU's "General Data Protection Regulation" (GDPR) has taken a very different approach. Indeed, it's even different than what has been in place in Europe for many years.

Previously, EU countries have operated under a series of "Directives," which acted as guidelines for "best practices." These Directives were non-binding, and the individual countries took their own approach to enforcement. This system was similar to the US "patchwork," but it had the added complexity of separate and sovereign countries. For purposes of international trade and the need for common protocols in the use and storage of private data, this system was a problem. In fact, from the perspective of US businesses, the inconsistencies between EU member countries were severe enough that the US Department of Commerce negotiated a "Safe Harbor Framework."

That Framework allowed US companies and organizations to meet EU data protection requirements and permitted the legal transfer of personal data between the EU and the US. If a US company satisfied the Framework's cybersecurity requirements, the company was deemed compliant with the EU member countries' individualized cybersecurity laws and with the general EU Directives. Approximately 4,500 US companies signed up and complied with the Safe Harbor Framework and have been conducting data based business successfully across Europe for many years.

So What Has Changed?

Between 2012 and 2016, the EU went through a process of reviewing and rewriting their data privacy laws. It was a painstaking project and all EU members participated. By the end, there had been over 3,000 amendments and many striking differences between previous EU directives and the new GDPR.

A threshold change was that the new laws were no longer guidelines. They became "regulations," which means they are binding and now the equivalent of our US federal statutes. Although there remains some lack of clarity regarding whether enforcement will be centralized or left to the individual counties, the new GDPR regulations are binding and uniform for all EU members.

The most startling aspect of the GDPR is how profoundly different it is from our own cybersecurity laws. It did not pay homage to any existing models, but instead went back to original principles and built an entirely new structure. The foundation was to declare data privacy a "fundamental human

right". Under US law, that would be the rough equivalent to amending our Constitution to add data privacy to the Bill of Rights. From that new fundamental human right, a variety of comprehensive and controversial requirements have been created.

The GDPR's definition of private data is very different than the approach taken by US law or earlier EU directives. Previously, the quantum of data declared private typically involved some type of personal identification information or especially sensitive data, such as health related material. But under the GDPR, private data would include any digital data that "could lead to identifying an individual."

Another key change requires that computer software and hardware incorporate "Privacy by Design." That appears to mean that an individual's right to data privacy be safeguarded in the creation of software and hardware, from beginning to end. An individual's data privacy is no longer an afterthought to be fixed merely by patches and updates. It must be an integral component from the beginning. Another feature of the GDPR requires that individual owners of data be fully informed and give clear consent to how and where their information will be used and who will have access, and further that explanations and disclosure be highly "user friendly." This appears to be an "opt in" system. Small print legalese contained in banners would be anathema to this new standard. The warnings on cigarette packages may be a closer example of adequate disclosure.

Perhaps most importantly, an individual's data must be both "portable," meaning he/she can take it away in some machine-readable format, and it also must be "erasable." Stated differently, a component of this new right of data privacy includes the obligation that an entity holding such data must erase it if directed by the owner. From the perspective of software and hardware engineers, these changes may be viewed as profound and, according to some, extremely difficult to achieve. Nevertheless, that's what the GDPR says and what it expects.

Finally, in enacting the GDPR the EU put a strong exclamation point after it in the form of penalties. They are extreme. Violators can be subject to penalties of 4% of global gross income or 20 million euros, whichever is higher.

Why Do We Care?

In creating the GDPR, the EU also redefined its jurisdiction, making it extraterritorial. It applies to any entity offering goods or services to individuals or businesses located in the EU. It also applies to all entities involved in monitoring the activity of any individual located in the EU. It further applies to any "controller" of data located in the EU, meaning a company that uses private data and to any "processor," which appears to include data storage facilities in the EU.

An increasing number of US companies do business in EU countries. The GDPR has created a fundamentally different set of rules with which they will need to comply. Commentators and the current literature indicate that the previous Safe Harbor Framework will no longer apply. The EU has chosen to be the leader in this brave new world of cybersecurity.

What Should We Do?

The remedy, as discussed in previous articles, is for any business subject to statutory cybersecurity requirements to begin the process of adopting an internal plan consistent with the National Institute of Standards and Technology (NIST) protocols. The new EU GDPR imposes international laws that could be relevant to some businesses and thus need to be included in that NIST plan. Such plans are not "one size fits all" and allow for a spectrum of business sizes and budgets. Importantly, a NIST plan documents and demonstrates a company's efforts at compliance which could become important in the event of breach and subsequent legal proceedings.

Kurt Hermanns is 'of counsel' at Gordon Thomas Honeywell, after a lengthy career with the United States Attorney's Office. He specializes primarily in federal criminal related risk management issues for South Sound businesses.

Kristina Southwell is a litigation associate at Gordon Thomas Honeywell. She has been following developments in privacy law and cyber security for several years. Kristina is a graduate of Indiana University Maurer School of Law and former clerk for the Washington State Court of Appeals.

Christal Harrison is a graduate from the University of Washington School of Law. She recently clerked at the Washington State Court of Appeals and is an associate at Gordon Thomas Honeywell, where she focuses on business transactions.