Global Feature

CHANGE ON THE HORIZON

General Data Protection Regulation: Are You Prepared?

Last year the EU approved its General Data Protection Regulation, or GDPR, the latest regulation designed to protect citizens' privacy amidst a seemingly endless flood of data breaches worldwide. This new regulation reinforces Europe's reputation as today's toughest watchdog on privacy and creates new risks (and potential penalties) for companies operating across the globe. The following pages shed some light on the scope of the GDPR and help outline what businesses can do to ensure they're prepared.

Let's step back in time. In 1995, the Data Protection Directive (DPD) was passed to protect the processing of personal data and its associated transferal within the countries that comprise the European Union (EU). In summary, the DPD was designed to accomplish two goals; to protect the privacy of individuals while allowing personal data to be shared within the EU. In order to achieve these goals, the DPD established criteria for the collection of personal data while affording rights to data subjects.

While the DPD was helpful, it was far from perfect, and technological changes soon outpaced the regulations. One of the largest flaws of the DPD was the inconsistency that resulted as each member state had its own set of rules. Compliance with numerous and varying regulations proved challenging, protection and enforcement were inconsistent and it was costly to manage. While it offered a good foundation, laws from 20 years ago weren't created with the rise of social networking sites, cloud computing, and smart cards in mind.

It became increasingly evident that a new framework for data protection in the EU was needed, and quickly at that. In 2012, the European Commission proposed a new regulation called the General Data Protection Regulation (GDPR) in order to provide better controls in an era that required it. Its primary intent was to provide stronger and more consistent data protection for EU citizens while also protecting personal data housed within the continent by global companies.

After years of negotiation on the scope of the GDPR, new regulations were agreed upon in December of last year. With the GDPR implementation date approaching and an abundance of new requirements coming with it, here is what companies will need to do in order to ensure their data protection programs are ready.

Applicability

The GDPR is expected to go into effect by the summer of 2018 and shall apply to all 28 member states of the EU. Having said that, its impact will be far greater than just European businesses, and will apply to all companies that use or house personal data for Europeans. The data itself does not need to be housed in Europe.

As a result, all companies with operations in the EU in addition to those based outside of the EU that process the personal data of EU residents will need to carefully evaluate the GDPR's requirements. Such organizations should determine how information security and data protection programs will need to be updated in an effort to prepare for the new rules. It cannot be stressed enough that the reach of the GDPR extends far beyond the boundaries of the EU.

Key Changes

Some of the key changes of the GDPR as compared to the DPD are as follows:

1. Response to Data Breaches

Over the next two years, organizations will need to develop a system to:

a) Create a data breach response plan to evaluate the risk of harm to consumers;

b) Build into that plan provisions to notify the Supervisory Authority within 72 hours of discovering a breach (if the event is deemed to be high risk); and

c) Be prepared to notify data subjects without delay (unless security measures in place shall prevent an event from being high risk)

Under the GDPR, personal data includes any information relating to an identified person (data subject). In addition to public authorities, organizations that handle sensitive data like health information, require the personal information of customers as a central aspect of the business, or those which process large amounts of personal data, are at considerable risk and will require a Data Protection Officer (DPO).

Simply put, DPOs are privacy experts, and because of the GDPR they will soon be in demand across the globe. These experts are primarily tasked with protecting privacy and handling personal data; it's all about protecting the people. Finding one may prove to be a challenge as there is not an abundance of DPOs. For this reason, organizations may look to train existing employees as an alternate option. DPOs will monitor compliance, train internal staff, and conduct internal audits. They will also respond to inquiries submitted by data subjects, handle matters of consent, and process requests to be forgotten, among other responsibilities.

The ramifications of the GDPR are quite impactful. If any party has access to organizational data, they can contribute to a breach. Organizations will need to ensure the protection of such data, and this extends to third parties such as cloud providers as well as to business partners that might have access to company systems. Consequently, robust due diligence measures will need to be implemented prior to entering into a business relationship with third parties and as part of the ongoing monitoring and auditing process once a relationship has been established.

2. A Right to Be Forgotten

Europeans will have the right to request information be erased if:

a) The data is no longer necessary for the reason it was initially collected;

b) Data subjects wish to remove their consent;

c) Data subjects object to the processing of their personal data;

d) Data was illegally processed;

e) A law requires data controllers (organizations that own the data) to erase the data; or

f) The data was collected as part of an offering to children

Under the right to be forgotten, EU residents may also choose to have their information removed from a search engine if the information is incomplete or irrelevant. As a result, businesses

Facts & Figures

890,000,000

*There have been nearly **890 million** records breached and over 4,800 data breaches made public since 2005.*

***Source**: Privacy Rights Clearinghouse.*

will need to be sensitive to the rights of the data subject, and be prepared with a process to fulfill requests to be forgotten.

3. Clear and Detailed Privacy Policies

Organizations must offer individuals information regarding the use of their personal data in a clear and explicit manner. Moreover, data controllers need to provide a reason for the data collection. Thanks to the GDPR, standardized icons will help create more transparency by serving as a highly visible and easily interpreted means of informing individuals.

4. Consent

If companies wish to process special personal data, consent to process data must be freely given and explicit. Such consent must come in the form of a signed statement as opposed to a pre-clicked box. As a result, the data subject will have the opportunity to decline and refuse to proceed.

Children are also protected under the law. When services are offered to children under the age of sixteen, a parent will be required to provide consent. There is one exception as member states have the option of lowering the age limit to as young as thirteen years of age.

Examples of special personal data, for which a consent is required, include the following categories:

- Associations;
- Biometric/genetic information;
- Clothing;
- Criminal convictions;
- Foundations/trade-union memberships;
- Health/sex life;
- Personal security measures;
- Philosophical/religious beliefs;
- Political opinions; and
- Racial/ethnic origin

Did You Know?

With far more aggressive penalties, the GDPR will have the potential to achieve more effective enforcement than the current DPD. The current fines are too weak to impact organizations with large amounts of revenue. For instance, in December of 2013 and January of 2014, Google was charged with data protection violations that took place in Spain and France respectively. Google faced fines totaling a mere $1.1 million, a fraction of the $2.3 billion fine the company could have been forced to pay if the GDPR was in effect at the time.

> A good starting point is to audit existing data and gain answers to vital questions. What is the data used for? Where is it stored – and on how many systems? Who has access? Are all of those individuals company employees, or do you have third parties with access to some or all of your system?

5. Right to Transfer Data to Another Service Provider

Companies may not transfer data to countries outside the EU that do not provide a strong enough level of protection, even within the same enterprise. One interesting aspect of transfers is the regulations provide individuals with the opportunity to transfer data between services. For instance, users could choose to move emails from one provider to another. This particular change is quite astounding in its potential applicability and will undoubtedly need to become clearer as time unfolds.

6. Penalties

Sizable fines of up to four percent of organizations' total annual revenue or more than $22.6 million, whichever is greater, can be imposed for breaking the rules. This figure is a dramatic increase, as the approaching penalty is 40 times the current maximum penalty. With this in mind, data controllers may seek to accommodate requests to remove information, simply to avoid the potentially severe consequences of failing to comply.

When we look at other pieces of legislation such as the UK Anti-Bribery Act for instance, there was tremendous hype that accompanied its enactment. Yet in the years to follow, there were no corporate prosecutions. One could infer that awareness was raised and subsequent program improvements led to the reduced likelihood that violations would occur. Or, since we are seeing prosecutions now, such as the Sweet Group PLC, sentenced in February of 2016, it's quite possible that the development of cases took time.

In the case of the GDPR, the substantial increase in requirements, combined with the fact that individuals take their personal data quite seriously, certainly leads to the significant possibility of elevated levels of enforcement in the foreseeable future. Do not become complacent if, like other regulations, it takes some time to see the first GDPR violation case. After all, nothing is more painful than being turned into a global example of failure.

Lastly, the GDPR opens the door for data subjects to take a right of action and potentially seek compensation. Companies should keep an eye on this as the regulation evolves.

> It cannot be stressed enough that the reach of the GDPR extends far beyond the boundaries of the EU.

Recommendations for Organizations

Since the GDPR will not come into play until 2018, now is the time to prepare. A good starting point is to audit existing data and gain answers to vital questions. What is the data used for? Where is it stored – and on how many systems? Who has access? Are all of those individuals company employees, or do you have third parties with access to some or all of your system? Data map now, and if nothing else, you may be able to get rid of data you don't need to store or clear up systems you no longer require.

IT can host meetings to determine how long data should be retained, remove duplicate data, ensure data is complete, review permissions and classify data accordingly. Chief information officers and chief ethics and compliance officers (CECOs) can work together to oversee this process.

In accordance with the new regulation, CEOs will need to make the GDPR part of the long term strategy for the organization, and work with board directors to make it part of their agendas and a component of short and long term plans. Key aspects such as staffing, budget, internal controls, resources, and risk management will need to be considered. There are also implications for stakeholders; companies will have to disclose operational costs associated with GDPR compliance to investors.

Key functions including IT and HR will need to partner with compliance to develop strategies to acquire a data protection officer (DPO) or train existing staff.

Organizations should focus their efforts on written standards by developing a clear and comprehensive GDPR policy and related resources, and updated privacy policies that are easily understood by their target customer base. Focus on your consents, including those for children under the age of sixteen. Training programs will also be needed to educate employees about their new obligations. Moreover, CECOs should provide assurance that the proper systems are in place to maintain compliance, and ensure employees are following the newly adopted policies and procedures. CECOs will need to collaborate with the internal audit, risk, HR, procurement, and legal functions in particular.

As expected, new breach detection and response systems will need to be implemented and tested well in advance of the GDPR going into effect. If a breach should occur, having a solid foundation in place will help mitigate the consequences when questioned by regulators.

Due to the high prevalence of data breaches, organizations should also look to protect themselves by obtaining insurance coverage and inserting language regarding ownership of responsibility into the contracts of data processors (i.e. cloud providers).

Lastly, updates concerning internal controls over information security and ERM results may be shared with the audit committee of the board. Observations and key findings should be included.

Closing Thoughts

In the modern era, the question is "when" and not "if" the next data breach will occur. The GDPR was long overdue and is certainly a step in the right direction. It will be imperative for organizations to become familiar with the new requirements and begin to develop successful strategies to ensure compliance is met.

Looking ahead, more information will become available. Organizations would be served well to learn as much as possible by following the guidance that European regulators will continue to share on the new regulation.

On a similar note, updates are expected in the near future regarding the EU-US Privacy Shield (EU-US PS), the proposed replacement for the invalidated Safe Harbor agreement. The EU-US PS, allowing data to be transferred between the EU and the US, has received quite a large amount of criticism. With the GDPR set to arrive in 2018, even if an approved version of the EU-US PS is passed in 2016, it will more than likely undergo future revisions in order to comply with GDPR requirements.

As we can see, a lot of changes in the world of data protection are on the horizon. While laws change each and every day, the GDPR in particular carries with it a whole series of new demands. Perhaps the most important question is, "How ready are you?"

Did You Know?

*According to a report by the International Association of Privacy Professionals (IAPP), companies in Europe alone will need to appoint over **28,000** DPOs before the GDPR goes into effect in 2018. These DPOs will need to possess "expert knowledge of data protection law and practices."*

Author Biography

***Les Prendergast** is VP and Managing Editor at The Ethisphere Institute with more than eight years of experience in the ethics and compliance field. He's dedicated to using Ethisphere Magazine as a platform to help organizations strengthen their ethics and culture, including enhancing their governance and compliance practices, and to share best practices among corporate leaders.*

*His primary areas of expertise include overall compliance program assessment, culture and knowledge assessment, risk assessment, training and communication planning, and benchmarking. See his full bio in the leadership section at **www.ethisphere.com**.*