GDPR
A New Data Protection Landscape

Insights into this transformative piece of privacy legislation
EXECUTIVE SUMMARY

The European Union’s General Data Protection Regulation (GDPR) promises to be a transformative piece of privacy legislation. Already, it has sent ripples through the international privacy community.

Notable both for the unprecedented fines it is bound to impose and the stringent consumer protections it enacts, GDPR is unlike any legislation before it. Its reach far exceeds that of earlier privacy legislation, affecting nearly every organization worldwide that processes data of EU citizens.

Focal Point has advised many of its clients on the best path to GDPR compliance. This paper is an extension of that guidance. In it, we outline the major changes between GDPR and its predecessor, the Data Protection Directive (Directive). We also take deep dives into some of the groundbreaking changes that GDPR will usher in to privacy offices worldwide.

This paper covers:

• The path from the Directive to GDPR
• The roles, responsibilities, and rights of the new Data Protection Officer
• New data security requirements, including mandatory security controls and breach notification procedures
• Heightened sanctions, including some up to 4% of global revenue
• New individual rights, including the right to erasure and the right to data portability

With the deadline to GDPR quickly approaching, organizations must act now to bring their processes in line with the new requirements. Understanding the implications of this new legislation is the first step in building a roadmap to GDPR compliance.
HOW WE GOT HERE

EU Data Protection Basics

The European Union (EU) and the United States have very different regimens for protecting personal information. The United States uses a patchwork of privacy laws including the Health Insurance Portability and Accountability Act (HIPAA) for protected health information, Financial Credit Reporting Act (FCRA) for credit reports, and many more. In contrast, the EU considers privacy a fundamental right and uses the Data Protection Directive (Directive) to regulate the processing of personal data across Europe. True to character, European regulators recently approved a comprehensive privacy regulation that will take effect in 2018. The regulation applies to all foreign companies processing EU personal data, so American and Canadian companies should make certain their compliance programs are EU relevant.

GDPR Replaces EU Directive

In the works since 2012, GDPR was adopted on April 14, 2016, and is scheduled to go into force on May 25, 2018. GDPR replaces and expands the Data Protection Directive by centralizing powers that were previously reserved to EU member states.¹ Under the Directive, EU member states were allowed to pass laws to supplement the Directive, resulting in many states having different personal data laws. GDPR aims to harmonize Europe’s privacy laws and also restricts the ability of member states to pass their own data protection laws in the future.

GDPR Applies to Many American and Canadian Companies

Within the EU, businesses that collect individuals’ personal data are called “data controllers” and any use of personal data is called “processing.” Data controllers may use “data processors,” such as cloud service providers or billing companies to handle personal data. The individuals about whom data is collected are called “data subjects.” Historically, the Directive only applied to controllers of personal data. However, GDPR’s expanded jurisdiction applies to the processing of personal data of all EU residents, even if the controller or processor is located outside of the EU.² This means that American and Canadian companies that sell goods and services to EU residents will be subject to GDPR.
KEY TAKEAWAYS OF GDPR

Below are some key areas for organizations to consider when aligning their compliance environment to the GDPR requirements:

New Obligations in the Data Ecosystem

Companies will be required to obtain unambiguous consent when collecting EU personal data. For websites, this will require the checking of a box or other technical configurations to clearly indicate the data subject’s acceptance of the terms of processing. Companies must also build in new personal data protections in the form of identity-masking techniques such as “pseudonymization,” which makes individual identification more difficult. Employees should be trained in these practices, and companies must regularly audit the data they maintain and document the reasons for its collection. Additionally, all uses of high risk data will be subject to a privacy impact assessment to account for the risks of processing and to identify potential safeguards.

Requirements for a Data Protection Officer

Companies that currently monitor data subjects using targeted online advertisements or customer loyalty programs will be required to appoint a Data Protection Officer (DPO). One study suggests this new requirement will result in up to 28,000 new DPOs in Europe alone.3 American and Canadian businesses with no physical presence in the EU may also be required to appoint a DPO if they monitor personal data from EU employees or customers.

Increased Security Requirements

Data controllers and processors will have increased security responsibilities when storing or processing personal data. GDPR requires that both data controllers and data processors take security measures proportional to the risks of processing and the types of information involved. In the event of a data breach, companies will be required to inform privacy regulators within 72 hours upon discovery and notify data subjects “without undue delay.”

Possibility of Multi-Million-Euro Fines

Violators of EU data privacy law, including American and Canadian companies, will be subject to potential fines of up to 4% of annual revenues or € 20 million, whichever is higher. Because this scales

“Larger companies could face massive fines - potentially millions of Euros.”
with the size of a company, larger companies could face massive fines – potentially millions of Euros.

**Expanded Individual Rights**

Individuals also gain rights: the right to be forgotten and the right to data portability. The right to be forgotten allows an individual to request that a corporation delete that individual’s information once its retention can no longer be legally justified. Under the right to data portability, individuals may request a copy of all automated data which a company possesses about them. This data must also be delivered in an easily transferable format which could be an arduous and expensive task for some companies.

In the subsequent sections of this paper, we take a closer look at these key areas of GDPR, including the role of the DPO, increased security requirements and the repercussions of non-compliance, and changes and additions to individual rights.
Under the GDPR framework, any private sector organization that carries out “regular and systematic monitoring of data subjects” as part of its principal business activities will be required to employ a DPO by the May 25th, 2018 enforcement date. This includes American and Canadian companies that routinely process large-scale or sensitive EU data.

Which Companies Will Require a DPO?

If the monitoring or tracking of personal data is central to the business, a DPO will be required. The DPO mandate will apply to businesses ranging from startup healthcare apps to major financial institutions. Any private entity that processes special categories of data, including health, genetic, racial, religious, or biometric information of EU residents, will be obligated to employ a DPO. These categories cover an expanse of personal information, and companies that collect data ranging from simple food allergies to thumbprints will fall within the jurisdictional scope of GDPR.

Roles and Responsibilities

Article 39 of GDPR, “Tasks of the data protection officer,” outlines the overall roles and responsibilities of the DPO. It states that the primary function of the Data Protection Officer is to inform and advise the data controller on how to “monitor compliance” with GDPR. This includes conducting privacy awareness training, performing compliance audits, and, wherever appropriate, issuing privacy impact assessments. DPOs are also responsible for acting as the liaison between the company and a supervisory authority.

Qualifications

As a general practice, DPOs should be proficient in IT and data security processes and should also have a strong understanding of corporate risk that extends beyond basic legal compliance. A constructive DPO will apply a risk-based approach to data protection without being excessively obstructive in a company’s core processing operations. Businesses can scale existing infrastructure and leverage corporate compliance departments to allocate an available resource as a DPO. Alternatively, companies are also permitted to make use of third-party services to fill the DPO position.
It is important to note that DPOs are not the same as Chief Privacy Officers (CPO). While the duties of a CPO and DPO will likely overlap in the course of day-to-day operations, the key distinction is that a DPO is responsible for managing compliance as well as reporting instances of internal non-compliance to a supervisory authority.

**Immunity**

Under the new GDPR framework, DPOs are protected by law and cannot be dismissed for exercising the duties of their position. Because of this, some companies may choose to employ DPOs on a semi-annual contract and then opt to renew or replace the DPO if necessary.

**Takeaway**

For information-driven enterprises, data protection is an integral part of sustainable growth. Undoubtedly, in the wake of GDPR, the default reaction of most entities will be to reluctantly take on a DPO as a means of complying with an unavoidable regulatory obligation. However, for prudent businesses, a rare opportunity exists to preselect a highly knowledgeable and localized resource to safeguard valuable customer and employee data before GDPR formally takes effect in 2018.

---

**THE DPO AT A GLANCE**

**Who needs a DPO?**

Every organization that processes the data of EU citizens as part of its principal business activities.

**What does the DPO actually do?**

Manages and reports on GDPR compliance. Leads privacy awareness training, performs audits and privacy impact assessments.

**Who is qualified to be a DPO?**

Any IT or Data Security professional with a strong understanding of corporate risk.

**Can a third party serve as the DPO?**

Yes. Alternatively, you could assign DPO responsibilities to an existing resource.

**Isn’t the CPO already the DPO?**

No. Chief Privacy Officers and Data Protection Officers have separate functions and responsibilities.

**What rights does the DPO have?**

DPOs are granted a great deal of independence and have immunity from dismissal or penalty for performance of their job tasks.
DATA SECURITY UPDATES

GDPR has made several critical updates to data security requirements, which will provide greater protection for personal data and hold companies responsible for security failures. Now, data controllers and processors must implement new security measures and comply with uniform breach notification laws.

Security Controls

GDPR requires that “taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.”

Not only must data processors and controllers adopt proper security measures to ensure the confidentiality, integrity, and accountability of personal data, GDPR now explicitly mentions specific security controls that organizations must implement.

Companies wishing to comply with GDPR must implement the below measures:

Breach Notification Laws

Security is such a high priority within GDPR that EU regulators have included a detailed breach notification rule. The inclusion of a breach notification rule not only highlights the importance of data security, but also holds organizations accountable for their personal data security failures. Similar to the HIPAA Breach Notification Rule under the jurisdiction of the U.S. Department of Health and Human Services, which requires healthcare entities to report breaches of personal health information to regulatory authorities, GDPR has specific requirements for breach notifications.

The following notifications are required under the GDPR breach notification rule:

- Data controllers must report breaches of personal data to Supervisory Authorities (SAs) without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If the controller can demonstrate that the data incident is unlikely to result in a risk to the rights and freedoms of natural persons, there is no need to report the incident to SAs.

Security Measures

- The pseudonymization and encryption of personal data
- Steps to ensure the resilience of systems and services processing data
- Measures that allow organizations to restore the availability and access to personal data in the event of a breach
- Frequent tests, assessments, and evaluations of the effectiveness of the security measures

“...The inclusion of a breach notification rule not only highlights the importance of data security, but also holds organizations accountable...”
• If a data controller determines that a breach would result in a high privacy risk, then the data controller must also notify the affected individual(s) of the breach without undue delay.

• Data processors must notify data controllers of all breaches without undue delay, but processors have no other notification obligations under GDPR.

With its increased focus on data security, GDPR has laid out sanctions and hefty administrative fines that are much higher than those seen in the past. The previous Data Protection Directive merely stated that sanctions had to be defined by Member States; however, GDPR now gives organizations explicit guidance on exactly what type of sanctions may be rendered. SAs now have authority over both data processors and data controllers and are able to impose large penalties in addition to, or instead of, their corrective powers.

A few high-impact SA corrective powers include:

• The power to suspend data transfer to a recipient in another country;

• The power to order a data controller to communicate a personal data breach to the data subject; and

• The power to impose administrative fines.

Under GDPR, administrative fines vary by the severity of the violation, but can range from the greater of €10 million or 2% of total annual worldwide turnover to €20 million or 4% of total annual worldwide turnover. Larger fines will mostly likely be reserved for breaches that involve “special categories of personal data,” which include race or ethnic origin, political opinions, and religion or beliefs, among other things.

With data security now playing a larger role in data privacy oversight under GDPR, it is critical that companies subject to GDPR ensure that their security standards meet these stricter obligations.

GDPR has laid out sanctions and hefty administrative fines that are much higher than those seen in the past.
THE EXPANSION OF INDIVIDUAL RIGHTS

Under GDPR, European regulators have expanded individual rights to include four new rights. In addition, four rights from the Data Protection Directive have been carried over with some changes.

Directive’s Individual Rights Renewed

Right to Access
The right of access allows European data subjects to request an account of all his or her information held by a data controller. Under GDPR, a data controller must provide more information to a data subject than under the Directive, including the duration that the data will be stored and information on the other individual rights of data subjects. In addition, GDPR requires data controllers to create a standardized process to respond to access requests. This process could include setting up a single point of contact for requests and a procedure for DPOs to accept or reject requests and respond to them.

Under the Directive, a nominal fee was charged for access to information, but a data subject will now be able to access their data for free, unless the data controller can claim that the request is manifestly excessive.

Right to Object
The right to object allows European data subjects to stop a data controller from using or processing their information in certain situations. Under the Directive, the data subject could object on compelling legitimate grounds to the processing of their personal data related to their own personal circumstances. A justified objection would prevent the data controller from any further processing. The data subject is also able to object to any processing of personal data used for direct marketing purposes.

While continuing the Directive’s prohibition of objectionable data-processing activities, GDPR is also making data processing for scientific and historical research and statistics objectionable. The data controller must now prove a “compelling legitimate interest”
to continuing processing data when a data subject has objected. This is a serious shift away from the Directive, which made the data subject prove compelling legitimate grounds to object.

**Right to Rectify**

The right to rectification gives data subjects the ability to correct inaccurate or incomplete information held by a data controller. Under the Directive, a data subject only had the right to correct information when necessary to ensure the fair processing of that data. GDPR has now expanded the right to rectify data to all personal data about the data subject.

Additionally, GDPR requires a response to a data rectification request within one month, if there are no extenuating circumstances. Data controllers must now also share rectification requests with any third parties that have obtained the information from the controller prior to making the requested rectification.

**Right to Object to Automated Decision-Making and Profiling**

The right to prohibiting automated decision making was reflected in the original Directive in limited form. Under the Directive, a data subject had the right to not have legal or “significant” decisions made about him or her based solely upon automated processing of personal characteristics.

For reference, automated decision making is typically performed when an organization performs “profiling” activities, including the collection of data for evaluation, such as predictive or behavioral analytics, of a data subject to determine present or future preferences, behaviors, or attitudes. A common example of profiling and automated decision-making can be found in target marketing performed by organizations, in which the organization processes personal data, profiles the individual, and makes decisions concerning the individual or predicts the individual’s behaviors or actions. GDPR now lists several characteristics prohibited from automated decision-making, including race, national origin, religious/philosophical beliefs, sexual orientation, and genetic/biometric data.

Although GDPR grants individuals certain rights to restrict automated data processing, GDPR inherits the Directive’s exceptions that deny data subjects’ right to prohibition of automated decision making.
under certain cases. These are exceptions in cases of necessity under contract between the data controller and the data subject, and as authorized by law. Additionally, GDPR adds several more exceptions, including explicit consent, necessary to protect the data subject, "manifestly publicly available data made public by the data subject," legal necessity, and necessary for public or private health.

New Individual Rights under the GDPR

Right to be Informed

GDPR emphasizes transparency of the data controller’s information practices. The right to be informed obligates data controllers to provide “information necessary to ensure fair and transparent processing” to data subjects, typically through a privacy notice and when an access request is made. Limitations to the information must be provided when the personal information has been indirectly obtained (i.e., information created by a controller about the data subject) rather than information that is directly obtained. All the information that is provided to a data subject by the data controller must be concise, intelligible, easily accessible, written plainly, and free of charge.

Right to Erasure

The right to erasure, formally known as the right to be forgotten, is the right of data subjects to request that a data controller delete all their information that is being maintained about the data request. The request must be forwarded to any and all data controllers/processors that received the data subject’s information through that data controller. The right to erasure is applicable in the following situations:

1. The data is no longer needed for the original purpose;
2. The data subject has withdrawn his/her consent and there are no other grounds for processing;
3. The data subject has objected to the processing;
4. A legal obligation requires the erasure;
5. The processing is unlawful; and
6. The data was collected in relation to offering information society services to a child.
However, the right to erasure is not an absolute right. A company can object to the erasure of an individual’s data on the following grounds:

- Right of freedom of expression and information;
- Necessity of use for a legal obligation relating to a public interest task or official authority;
- Public health purposes;
- Archiving purposes in the public interest, research, or statistical purposes; and
- Necessity in legal claim or defense.

**Right to Restriction of Processing**

The right to restrict processing allows a data subject to prevent further use of his or her personal data, while allowing the data controller to continue storing the information. A data subject can successfully prevent a data controller from further processing their data in the following situations:

1. The subject has contested the accuracy of the personal information;
2. An objection to the processing has been made and the company is deciding if it has legitimate grounds for continued processing;
3. The processing is unlawful, but the data subject requests restriction rather than erasure; and
4. When the data subject seeks to prevent deletion by a data controller based on the information’s value in a legal claim or defense.

Similar to the right to erasure, any third party that received the information from a data controller in receipt of a valid request by a data subject must be informed by the controller. Additionally, a data subject must be informed if, and when, the restriction is lifted by the data controller.

**Right to Data Portability**

The right to data portability allows data subjects to obtain their personal information from a data controller and bring that information to another data controller of their choosing. The right to data portability applies when:

1. The personal information of the data subject has been supplied by the data subject;
2. The processing is based on the data subject’s consent or for the performance of a contract; and
3. When processing is carried out by automated means.

Data controllers must provide this information free of charge and in a structured, commonly used, machine-readable format. If the data subject requests that the information be transferred directly to another data controller, the information must be provided without undue delay. GDPR requires that a transfer of information must be provided within one month, unless the requests are complex or numerous. Two additional months can be added without being considered an undue delay in such situations.

In the case of an extension or a rejection of a request, the data controller must provide justification to the data subject within one month.

**Importance of Individual Rights**

The expanded individual rights of European data subjects in the new GDPR are indicative of the changes to the collection, transfer, and processing of data that has occurred since the Data Protection Directive was passed twenty years ago. The expansion of individual rights will require that companies subject to GDPR keep individuals in mind when using personal information in their current operations and in innovative new ways. GDPR also highlights the importance of an individual’s control over the data that companies collect and store about them. Companies will need to be prepared to comply with these new individual rights related requests by early 2018.

“GDPR highlights the importance of an individual’s control over the data that companies collect and store about them.”
NEXT STEPS

With GDPR approaching, companies in Europe and around the world will need to make a number of changes to their privacy programs, policies, and procedures in order to meet GDPR standards. While GDPR has streamlined privacy legislation in the EU, doing away with the various laws of EU member states and centralizing these powers into one regulation, there remain a number of daunting changes facing companies that process the data of EU citizens. With the penalties for non-compliance poised to set record levels, companies should move quickly to begin addressing these challenges.

Organizations should immediately begin assessing their current privacy and security programs against the GDPR requirements, allowing sufficient time to remediate any gaps. With expanded individual rights, greater data security requirements, and the addition of the DPO, most organizations are facing significant changes to their privacy and security programs. In order to comply with GDPR, companies must have absolute visibility into how personal data is used within their organization, from collection through to processing, transmission, and storage.

For many countries outside of the EU (such as those in the US and Canada), tackling international privacy regulations can be a seemingly impossible task, and understandably so - this is a realm of unfamiliar laws and regulations. Companies that are not well-versed in international privacy regulations or lack the resources to move their organizations into compliance should consider engaging a third party assess current operations and develop a clear, step-by-step remediation roadmap. A third-party assessor can also provide privacy and security experts to support remediation efforts to ensure you meet every requirement. Come May 2018, these companies should be able to continue EU business operations smoothly without fear of penalties.

GDPR is placing greater responsibility on the organizations that collect and process EU citizens’ data to do so in a way that protects the privacy rights of individuals. North American companies willing to take on this responsibility and work with EU personal data must make every effort to protect these customers and ensure their unique rights as EU citizens.

The full text of the GDPR (Regulation (EU) 2016/679) can be read at eur-lex.europa.eu.

THE AUTHORS

Focal Point’s "GDPR: A New Data Protection Landscape" whitepaper was written by:

Erica Walker, JD, CIPP/US ewalker@focal-point.com | Connect
Jay Wholley, JD, CIPP/US jwholley@focal-point.com | Connect
Melinda Tijerino, CIPP/US mtijerino@focal-point.com | Connect
PREPARING FOR GDPR

If you do not have an accurate and reliable inventory of your sensitive data, including how it is collected, stored, processed, transmitted, and accessed, it is critical to prioritize this effort to achieve and maintain long-term compliance with GDPR and other privacy regulations.

Focal Point has been assisting clients in this effort since GDPR was first announced. While our approach can vary by organization, our ultimate goal is to put you in control of your data, and gives you the tools to manage compliance as regulations evolve. Our offerings include:

**GDPR Readiness Assessment**
There are likely to be deltas between the way your business operates today and how it must operate under GDPR. A readiness assessment specifically targets these gaps, bringing your path to compliance into focus. Each readiness assessment results in a detailed roadmap that is specific to your environment, people, and situation. The roadmap sequences the technical and operational steps required to achieve compliance, and provides actionable recommendations on achieving these goals in your organization.

**Information Mapping**
Understanding how your company collects, processes, transmits and stores data – as well as how it’s used and who uses it – is the foundation of your data privacy program and the key to complying with regulations like GDPR. To map the flow of data through your organization, we go right to the source: your users. Using our proprietary survey tool, we collect usage patterns from your user base and deliver insight into the actual practices being used in the day-to-day creation and handling of sensitive data.

**Information Mapping Governance**
Focal Point offers a tech-enabled extension of the data mapping process, allowing you to maintain the accuracy and completeness of your data map over time. Our SaaS tool automates the survey distribution and collection process, periodically requesting updated surveys from your users. Ongoing maintenance of your data inventory prevents costly restarts and ensures continuous alignment between management’s understanding of data practices and the practical usage of data within the organization.

About Focal Point

Focal Point’s Data Privacy team has developed and implemented privacy programs for some of the nation’s largest and most complex organizations. Our privacy professionals have expertise in a number of privacy regulations and frameworks, including international privacy laws, U.S. state regulations, HIPAA, HITECH, GLBA, and NIST. Most of our privacy experts are Certified Information Privacy Professionals (CIPPs) and Certified Information Systems Auditors (CISAs), and a number of Focal Point’s experts are Juris Doctors with backgrounds in privacy law. Our privacy team is actively involved in the data privacy community, presenting on key privacy issues at leading security and privacy conferences and contributing to leading industry publications.

Contact us:
Eric Dieterich, Data Privacy Practice Leader
786.390.1490 | edieterich@focal-point.com | focal-point.com