UNDERSTANDING AND DEMONSTRATING ALIGNMENT WITH THE GDPR

Technological advancement, and the massive, global exchange of personal data borne of it, must have its counterbalances. The General Data Protection Regulation (GDPR) is the manifestation of this notion. Its provisions will significantly shift the international privacy landscape and force a far-reaching consideration of those rights the European Union believes are inherent and fundamental.

schellman

Quality, above all.

A BRIEF HISTORY

The GDPR's predecessor, the European Data Protection Directive ("the Directive"), was introduced in 1995 to harmonize the data privacy and protection standards of the European Member States. In concept, unifying each country's laws would endorse the free cross-border flows of personal data, ultimately spurring commerce and the general cohesion of the European nations. This was novel. Moreover, the breadth of the Directive outlining the rights of its residents was beyond any other privacy model seen before. However, over time it was revealed that the Directive allowed for considerable divergences in interpretation and implementation among the Member States and ultimately obsolesced in the wake of the globalization and evolution of technology.

In the late 2000s, centering on these observations, the European Commission held a series of conferences and talks to discuss reforming the Directive to maintain and strengthen its principles and to better address emerging challenges to privacy. These efforts ultimately lead to the lobbying of the GDPR to reface the Directive. From 2013 to 2016, through negotiations between the European Parliament, Council and Commission and the votes of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), the GDPR was officially adopted. It is effective on May 25, 2018.

APPLICABILITY

Many companies exploring this new privacy doctrine, in the Unites States and elsewhere, are asking "does the GDPR even apply to me?" and "how can the GDPR have province over our business if we're not even located in the European Union?" The GDPR applies to any organization that is offering goods or services (irrespective of payment) to residents of the European Union or who is monitoring residents of the European Union. Monitoring in the GDPR framework is referred to as "profiling" and is defined as the automated analysis or predicting of behavior, location, movements, reliability, interests, personal preferences, health, economic situation, performance, etc. It does not matter whether an organization operates physically within Europe (a concept referred to as "extraterritoriality"). This pertains to both data controllers and processors to the extent that processors (and relevant sub-processors i.e. subservice organizations) are obligated to accommodate controllers in carrying out their security and privacy obligations when procedural or technical barriers necessitate it. This means that a processor must assist a data subject in facilitating certain activities that uphold the rights of the data subject (like the right to access and rectify data or the right to erasure) if that processor solely manages any personal data or system layer germane to the controller's overall operation or IT production environment.

The "what" that is covered in this applicability equation is the processing of personal data belonging to residents of the European Union. This entails your common types of personal data (i.e. name, address, etc.) and now also includes categories of online data like static and dynamic IP addresses, cookie IDs, etc. Special categories of personal data, that historically has covered information like religious affiliation, political affiliation, sexual orientation, now encapsulates genetic information and biometric data as well and must only be processed for certain purposes explicitly stated in the framework. There are also specific handling requirements for personal data belonging to children. Children under the age of 13 can never give consent to the processing of their personal data as it pertains to online services. Consent for the processing of personal data belonging to children between the ages of 13 and 15 must be obtained from a data subject's parent (Individual Members States will define the age window).

KEY GDPR PROVISIONS

General Accountability

Accountability is one of the centerpiece concepts found in the new framework. For tone setting, it will be expected of both data controllers and processors to draft formal policies to document an organization's data privacy and protection posture and how it addresses the precepts of the GDPR. Policies should be tailored based on the nature, scope, context, and purposes of processing personal data as well as outline foreseeable risks to the rights of data subjects (describing technical and organizational controls in place to demonstrate compliance), involve training, and detail codes of conduct.

There are also explicit record keeping requirements that mandate both controllers and processors formally document particular aspects of their personal data processing practices. For controllers, details must be kept of

1. The name and contact information of the controller and Data Protection Officer
2. Purposes of processing personal data
3. Categories of data subjects, data, and recipients
4. International data transfers and related safeguards for those transfers
5. Data retention periods, and
6. Data security measures employed.

Processors have to formally keep similar materials that outline

1. The name and contact details of the processor and all engaged controllers
2. Categories of processing for each controller
3. International data transfers and related safeguards for those transfers, and
4. Data security measures employed.

It is stressed throughout the doctrine's text that necessary safeguards should be communicated, endorsed, and validated through the implementation of regimented GDPR training for staff and the undertaking of audits as an assurance measure.

KEY GDPR PROVISIONS

Data Protection Impact Assessments

In considering an organization's unique product or service and how different categories of personal data are collected, processed, and transferred as part of its core processing activities, a data protection impact assessment (DPIA) is an exercise to assess envisaged data processing activities with its associated risks and consequences to data privacy. The DPIA should be thorough enough to identify and plan for risk mitigation prior to carrying out processing to ensure protection of the rights and freedoms of affected data subjects. Processors are encouraged and controllers are required to perform DPIAs when processing will likely be considered "high risk" or for specific cases where there is a systematic/extensive evaluation of personal data, a large-scale processing of sensitive/criminal personal data, etc. DPIAs should include a description of processing and purposes, an assessment of data necessity and proportionality (which ties into minimization), an assessment of risks for data subjects, measures to address risks, and how to demonstrate compliance. When appropriate, DPIAs should also consider the data subject's and supervisory authorities perspective prior to processing; in particular, where personal data processing would result in a high risk to a data subject. This is quite a crucial activity for an organization and should include a cross-section of an organization's leadership and operations teams as it should serve to blue print the adequacy and currentness of existing data privacy and protection program.

KEY GDPR PROVISIONS

Data Privacy and Protection by Design and By Default

Data protection and privacy by design and by default is not a new concept, however, it appears as though the European Data Protection Board is going to bear down on this requirement starting in 2018, which demands that processes and systems are designed for handling personal data with privacy, data minimization, and security top-of-mind. Furthermore, the obligations of an organization will now include plan for privacy, data minimization and security by default when developing, designing, selecting and using applications, services or products that process of personal data. Equally as important, businesses must review their current access management program to evaluate its ability to safeguard personal data and to limit accessibility based on a 'need-to-know' basis.

Beyond introducing the necessary organizational and technical measures to satisfy this provision, the GDPR recommends utilizing technical controls, such as pseudonymization; where data is masked so that it cannot be attributed to a specific data subject without the use of additional information (data is kept separately to avoid the "mosaic effect" where data can be triangulated and made identifiable). Pseudonymization is different than anonymization; where data is made totally unreadable. Organizations technical control mechanisms, including encryption or pseudonymization, may vary based on the types of data processed and the nature and extent of processing activities.

KEY GDPR PROVISIONS

Data Protection Officers

Under the new GDPR framework, both controllers and processors are required to appoint Data Protection Officers (DPOs) when they are involved in the regular and systematic monitoring of data subjects or processing sensitive/criminal personal data on a large scale. DPOs must have an expert knowledge of data protection laws and the ability to support and advise the organization on all things related to personal data privacy. This role may need to be situated in Europe (based on the requirement of "DPO accessibility") and must be independent of conflicts business influences or interests and report to the highest management level. Where an organization lacks the means or capabilities to support an in-house DPO, outsourcing is permitted based on the guidance that's been released by the Commission. The DPO will serve as point of contact for all GDPR issues, be responsible for leading policy development and training, and will manage all necessary auditing and documentation obligations.

KEY GDPR PROVISIONS

Processor Governance

Article 28 of Chapter 4 in the GDPR (arguably one of the most important provisions) is the section that outlines the responsibilities of controllers when engaging processors. Part 1 of the article requires of controllers who are interested in delegating personal data processing activities to service providers to engage vendors only where they are willing and able to uphold the inherited obligations of the GDPR, and as outlined in a contractual agreement between the Controller and Processor. This part in itself is not actionable, but rather, sets the theme for the remainder of this article.

Part 2 of the article is certainly more prescriptive; stating that controllers must formally authorize the current and future use of an engaged processor's subservice organizations; in other words, controllers must approve processors engaging sub processors. Although the regulation lacks clarity on the criteria for a controller to authorize or reject an engaged processor's use of a subservice organization, processors should be prepared to have a means for confirming the privacy and security adequacy of a subservice organization they'd like to leverage.

Part 3 of Article 28 defines what must be stipulated in processor contracts, including

- The nature of the relationship with the processor (what the processor's service or product is)
- The length of the contract
- What the processor will actually be doing (as in what is the functional interaction between the controller and processor) as part of their service or product
- The types of personal data that'll be handled by the processor, and
- What general or specific GDPR requirements will be inherited by the processor

KEY GDPR PROVISIONS

Processor Governance (cont.)

Part 3 continues on in subpart A to stipulate the familiar requirements about processors only processing personal data as directed by the controller. This is basically the controller's way of saying "do as your told and nothing else". This specification ensures that the handling and use of personal data remains aligned with what data subjects have consented to. Subpart B drives the confidentiality requirements between the controller and processor, which were also part of the original Directive. Subpart C underlines the requirement that third party processors of the Controllers personal data must employ relevant controls associated with the requirements of Article 32, the Security of processing, that include, but are not limited to, the following:

- A controls framework must be implemented that was designed using a risk-based philosophy as it relates to personal data
- Processing systems and services have to sustain the tenets of confidentiality, integrity, availability and resilience
- Personal data should be restorable and accessible in a timely manner in the event of a physical or technical incident or disaster
- The pseudonymization, masking, encryption, etc. of data should be endorsed whenever possible
- The controls framework should be regularly tested and assessed for effectiveness
- A code of conduct should be in place to guide personnel in the performance of the activities necessary to uphold its obligations to the GDPR

Lastly, processors must be able to demonstrate they are upholding their obligations to the GDPR and also realize they are responsible for violations that arise in the use of subservice organizations.

KEY GDPR PROVISIONS

Notice

Notices are the primary way of communicating and establishing the GDPR's principles of fairness, transparency and purpose limitation. Notices should be presented at the point of collection and detail the following for data subjects:

- The contact details of your Data Protection Officer;
- The legal basis for collecting and processing personal data;
- Any legitimate interests relied upon;
- Retention standards and disposal procedures;
- The rights of data subjects; and
- Sources of data (if personal data was obtained anywhere indirectly)

Lawfulness (Legal Basis)

As detailed above, the legal basis for collecting and processing personal data should be contained in the notice. The GDPR has deemed processing to be lawful as long as it is limited to one of the following scenarios:

- Consent from the data subject has been obtained
- For the performance of a contract (directly related to the data subject)
- Compliance with legal obligations
- To protect the vital interests of the data subject or other natural persons
- For the performance of a task carried out in the public interest or when exercising official authority vested in the controller
- For the purposes of the legitimate interests pursued by the controller or by a third party

KEY GDPR PROVISIONS

Lawfulness (Legal Basis)

> It is important to note that consent has new requirements under the GDPR. Consent mechanisms should be clearly distinguishable from other matters, intelligible, easily accessible and in clear and plain language.

Consent must also be freely given and not a condition of the service being offered, which will hinder consent being used as the legal basis for processing in the scope of employment. Consent should be presented for each purpose in which personal data is being collected and should be a clear affirmative action which can be written, electronically submitted, or orally given (i.e. ticking a box on a website or selecting technical settings). Silence, pre-ticked boxes, and moving forward with processing due to inactivity are not means for consent. Lastly, data subjects should be given the right to withdraw consent (as easily as it was given).

KEY GDPR PROVISIONS

Rights of the Data Subject

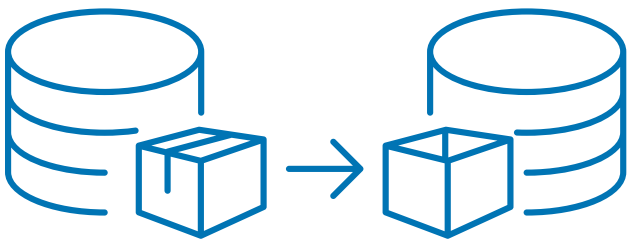
The spirit of the GDPR is to grant European residents rights over their personal data, and those rights by and large are distinctly presented in the legal text as follows:

Right of Access and Rectification

The offering of access to and the rectification of personal data will generally be trifurcated. Commonly, the first of its three stages involves a data subject exercising the ability to request and confirm if his/her personal data is being processed, what the present purposes of processing are, what the categories and sources of data are, who the recipients of that data are, and if any auto-decisioning practices are administered in the use of that personal data. Once confirmed, a data subject must be allowed a copy of that personal data free of charge. Lastly, data subjects must be permitted to update inaccurate personal data and request a supplementary statement of information if the data was initially incomplete. Please bear in mind that for the right of access and rectification, or any right detailed in the GDPR, it is the controller's responsibility to first verify the identity of the requester before carrying out the data subject's wishes.

Right to Portability

In the event a data subject wants to use the services of another controller, the legacy controller must be able to transfer that data subject's personal data in a commonly structured form that's machine readable directly to the new controller. This is an interesting stipulation as the controllers exchanging the personal data will likely be competitors.



KEY GDPR PROVISIONS

Rights of Individuals

Right to Erasure

This newly imbedded concept, commonly referred to as the "right to be forgotten", is arguably the most talked about provision of the GDPR. The right to erasure is the right of data subject to request a complete disposal of his/her personal data when certain conditions apply, like when consent is withdrawn, personal data is no longer needed for the purposes in which it was originally collected, or personal data was unlawfully collected.

As mentioned earlier, controller accommodation requirements have finally been baked into this new privacy doctrine and it certainly relates to the right to be forgotten. When procedural and systematic limitations are in place and a controller cannot fully purge or anonymize personal data when requested by the data subject, processors must accept their portion of the burden and facilitate requests to completion. The reality of a shared requirement like this is that many service organizations may have to undergo sometimes massive technology and infrastructure adaptations to accommodate. Some of the prevalent challenges seen thus far are as follows:

- When cloud service providers offer distributed storage as a service, incredible diligence is required when data that needs to be deleted is stored on more than one node in a replicated fashion

- When organizations have personal data on shared backup media; which could involve identifying the necessary backup image or images that contain the target file or files, finding the media with the related backup images, then duplicating all other backup images on the media and then cleansing that media. And if the backup image of interest also contains other files that must be kept, as is typically the case, then it would be necessary to restore that backup image, delete the file, and then backup the rest again.

KEY GDPR PROVISIONS

Rights of Individuals

Right to Restriction

The right to restriction will typically be initiated when a dispute over personal data (i.e. challenges of information accuracy, etc.) is underway, where data subjects have the right to request the stoppage of their personal data being processed until resolution. This should put data in limbo and requires the appropriate procedural and technical alterations to do so. Commonly this will be invoked when consent measures are contested, when legal claims dictate it, when data subject rights may be violated, etc. Albeit this chiefly falls on the shoulders of the controller, if a processor is used, they may be required to help with the processing ban. When a restriction is allowed to be lifted, it is the obligation of the controller to notify the data subject in advance.

Right to Object

Another nuance of the GDPR is the right of data subjects to object to specific types of processing as it relates to their personal information. Data subjects are now able to challenge a controller when they plan on using their personal data for 1) direct marketing, 2) research or statistical purposes, or 3) public interests or the exercising of public authorities. Only the right to object to direct marketing is absolute; meaning there is no need to demonstrate grounds for objecting. For the other two means of processing, it is the onus of the controller to justify the means of processing. Controllers are obligated to present these rights to data subjects at an early stage of the controller/data subject relationship.

BREACH HANDLING AND NOTIFICATIONS

Among some of these compliance bellyaches we've discussed, the GDPR's new breach notification requirements also seem to be a point of angst for many organizations. In the event of a breach involving European personal information (a breach being defined as the accidental or unlawful destruction of, loss of, alteration of, unauthorized disclosure or access to personal data), the controller needs to account for sub-processor to processor relationships, processor to controller communications, notifications to supervisory authorities and communications to impacted data subjects. Articles 33 and 34 of the GDPR outline breach escalation expectations.

> Sub-processors must notify processors immediately upon detecting a breach and processors must too notify controllers.

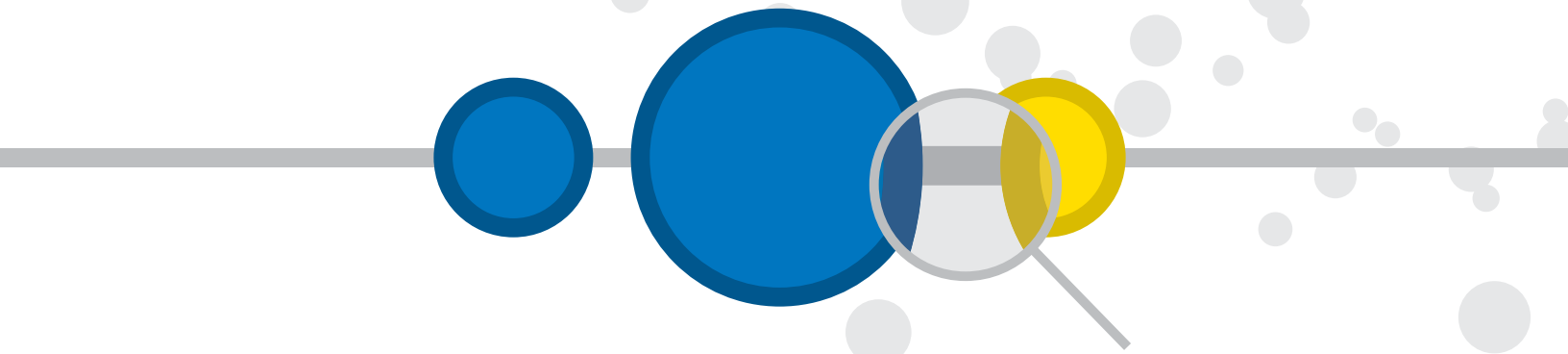
Controllers are required to notify supervisory authorities within 72 hours of having become aware of the breach. Notifications should include 1) the nature of the breach, including the categories and approximate number of data subjects and personal data records concerned, 2) the name and contact information of the organization's DPO, 3) the expected consequences of the breach, and 4) the mitigating activities carried out or in process to stopgap the breach. It is important to note that the controller must notify the lead supervisory authority within 72 hours, regardless of whether or not they have yet to collect all the related information. Article 33(4) allows for the information to be provided in phases to accommodate the investigative process.

BREACH HANDLING AND NOTIFICATIONS

Lastly, controllers must notify data subjects of personal data breaches without undue delay when a breach is determined to be high risk to the rights and freedoms of natural persons. The recently proposed guidelines issued by the Article 29 Working Party entitled Guidelines on Personal data breach notification under Regulation 2016/679 shed some light on the factors an organization should consider when determining whether or not the breach resulted in high risk to the rights and freedoms of natural persons. According to the opinion on breach disclosure, organizations should consider 1) the type of breach, 2) the nature, sensitivity and volume of personal data, 3) ease of identification of individuals, 4) severity of consequences for individuals, 5) special characteristics of the individual, 6) the number of affected individuals, and 7) special characteristics of the data controller. The notification to the data subjects of personal data breaches should contain the same information detailed above, in accordance with Article 34(2). It is important to note that notification to data subjects may not be required if one of the conditions outlined in Article 34(3) are met, but also that the supervisory authority has the final say-so per Article 34(4).

DEMONSTRATING ALIGNMENT WITH THE GDPR

Several times over, the GDPR calls out the imperatives of both data controllers and processors going through audits to assess and demonstrate their alignment with its provisions. Schellman & Company has a dedicated practice that offers readiness and attestation services to assist organizations in this effort. In engaging Schellman for readiness work, a business will have a validated description of the processes and systems that handle personal data, can verify the applicability of the many GDPR articles, can determine which applicable requirements are already satisfied by current policies and controls in place, and lastly be advised of all identified compliance shortcomings through a gap analysis.



The gap analysis will expound on associated risks and serve as a roadmap for necessary remediation. In undergoing an actual audit, the organization will be issued an attestation report that can be shared with customers and business partners alike to outline the determined applicability of the GDPR and what controls are employed to uphold the business' certain obligations. A report like this holds weight, as it is founded on the opinion of Schellman & Company, a CPA firm, and is delivered by data privacy and protection experts. It allows an organization to delineate itself as a committed subject of the GDPR by having a discernable summary of how it has addressed each individual article; shifting GDPR conversations from the vague and the confident and precise.

GETTING STARTED

- Familiarize yourself with the chapters and articles in the GDPR program. Schellman has additional content beyond this white paper shared through blogs and recorded webinars.
- Understand how and where your organization ingests, stores, and transfers European personal data.
- Assess how privacy mature (or immature) your enterprise is.

CONTACT US TODAY

Schellman offers several competitive differentiators for organizaions looking to align themselves with the GDPR. We are the first CPA firm that is 100% independent with no consulting agenda. We also offer organizations the opportunity to consult with our distinguished subject matter experts:

Avani Desai
Executive Vice President
CISSP, CISA, CIPP, CCSK

For more information or to contact us about your GDPR initiatives, go to www.schellmanco.com/gdpr


schellman