SATORI CONSULTING

GDPR: A GUIDE TO READINESS

The European Union (EU) is implementing the General Data Protection Regulation (GDPR) that takes effect May of 2018. Any businesses offering goods or services to and/or monitoring the behavior of EU residents must be prepared to meet the requirements of the regulation.

This white paper summarizes the main GDPR requirements and provides practical insight into readiness preparation. It is designed to highlight the key requirements and provide insight into the development of a thoughtful plan to comply.

January 2018

New York, 212.918.4560

Satori CONSULTING

gdpr@satoriconsulting.com

Contents

INTRODUCTION

The European Union's (EU) General Data Protection Regulation (GDPR) takes effect May 25 of 2018, and businesses must be prepared to meet the requirements of the regulation. This can be a tall challenge given the various privacy and security requirements included in the regulation. The level of preparation will vary from business to business based on the organization's level of privacy and security maturity, and level of compliance with the EU Directive. GDPR replaces the EU Directive 95/46/EC introduced in 1995.

This white paper summarizes the main GDPR requirements and provides practical insight into readiness preparation. This document is not intended to serve as a comprehensive guide to all GDPR requirements. The intended audience is business and technical leaders responsible for managing risk, maintaining compliance, or implementing information security within the organization.

GDPR TERMS AND DEFINITIONS

There are several GDPR terms used throughout this document that require clarification. These terms are defined below.

GDPR Terms

- *Data Protection Authority (DPA)* – A DPA is an authority that is responsible for enforcing data protection regulations within a EU member state. DPAs also investigate potential GDPR violations and determine fines for confirmed offences.
- *Supervisory Authority* – The supervisory authority is an entity that acts as a DPA.
- *Controller* – A controller is an entity that collects or processes personal data from data subjects.
- *Processor* – A processor processes data on the behalf of a controller. Examples of processors include AWS (e.g., EC2, S3 services), Google (e.g., GCP service), Scale, and Twilio. Processors are legally liable if they are responsible for a breach.
- *Data Subjects* – These are natural individuals whose data is processed by a controller or processor. Data subjects are EU citizens or residents.
- *Personal Data* – Information that identifies a data subject is considered personal data. Example identifiers include name, phone number, email address, physical address, and location data. This applies to data regarding customers, employees, and third parties.
- *Data Protection Officer (DPO)* – The DPO is a data privacy expert that works with organizations (controllers and processors) to achieve and maintain compliance with GDPR requirements. This role may or not be an employee of the organization.

WHAT IS GDPR?

GDPR is a regulation that enhances the rights of data subjects to govern the privacy of their personal information and ensure that controllers take the right steps to protect it. At its core, GDPR brings transparency to the collection, use, and retention of data subjects' personal information. This places new responsibilities on the organization to provide transparency in the lifecycle management of personal data.

The regulation applies to organizations operating outside of the EU that:

1. Offer goods and services to EU residents
2. Monitor the behavior of EU residents

The expectation is that businesses comply with the requirements as described in the regulation. Organizations are not required to produce a certificate or other official document (there is no GDPR certification at this time).

The penalty for GDPR non-compliance can vary. At this time, the maximum penalty is the greater of €20 mil (~$24 mil) or 4% of the previous fiscal year worldwide revenue. The supervisory authority determines the actual penalty based on the circumstances of the incident. Consideration is given to criteria such as the type of data exposed, number of data subjects affected, level of harm to data subjects, and mitigating controls implemented by the controller/processor. In theory, if the organization lawfully processed the personal data and exercised due care in protecting it, the penalty should be lower than the maximum described above.

KEY GDPR REQUIREMENTS

This section provides a summary of the most notable GDPR requirements. Addressing all of the requirements is not practical as the regulation includes 99 articles. The notable requirements can be summarized as principles, privacy, and protection (see Figure1, Key GDPR Requirements Summary). Organizations must understand these requirements and potential implications to their business.

Figure 1. Key GDPR Requirements Summary

Principles
▪ Data processed lawfully, fairly, and transparently ▪ Collect data for legitimate purposes ▪ Only collect personal data needed ▪ Personal data must be accurate and kept up-to-date ▪ Personal data is kept in a form which permits identification of data subjects for no longer than is necessary ▪ Personal data must be processed in a manner that ensures appropriate security

Privacy (Rights of Data Subjects)	Protection (Controllers and Processors)
▪ Transparent information, communication and modalities for the exercise of the rights of the data subject ▪ Information to be provided where personal data are collected from the data subject ▪ Information to be provided where personal data has not been collected from the data subject ▪ Right of access by the data subject ▪ Right to rectification ▪ Right to erasure ('right to be forgotten') ▪ Right to restriction of processing ▪ Right to data portability ▪ Right to object	▪ Data Protection Officer ▪ Data protection by design ▪ Data protection impact assessment ▪ Records of processing activities ▪ Security of processing ▪ Notification of a personal data breach to the supervisory authority ▪ Communication of a personal data breach to the data subject

Principles

Principles provide guidance for adhering to privacy and protection requirements. They underpin GDPR compliance. The GDPR principles described below are practical and should be applied to the collection and processing of any personal data.

- *Data processed lawfully, fairly, and transparently* – Lawful processing requires consent (or valid business purpose for processing) and processing consistent with stated purpose. Additionally, organizations must clearly and plainly communicate what data is collected and how it will be used. Consent is a key concept and is discussed in more detailed in this section.

- *Collect personal data for legitimate purposes* – Processing of data must not extend to purposes it was not originally collected for.
- *Only collect personal data needed* – Limit data collection to what's needed for the stated business purpose. Collecting additional personal data will unnecessarily increase risk for the organization and data subjects.
- *Personal data must be accurate and kept up-to-date* – Take measures to maintain the correctness of data and respond to rectification requests in a reasonable timeframe.
- *Personal data is kept in a form which permits identification of data subjects for no longer than is necessary* – Data retention of personal data must be defined, and data may be anonymized if required for an extended period of time. Personal data may be retained longer if needed for reasons such as public interest or scientific research as long as the appropriate controls are in place.
- *Personal data must be processed in a manner that ensures appropriate security* – Appropriate security controls must be in place to maintain the confidentiality, integrity, and availability of personal data.

These principles must be communicated throughout the organization using existing security training and awareness programs. Considering principles during design and planning (build security in) will reduce the need to re-factor products later in the process, saving the organization time and money.

Consent

Understanding consent is important because it plays a key role in establishing the ability to lawfully process personal data. Consent is the act of a data subject freely agreeing to the processing of personal data and affirming their agreement by taking action (e.g., selecting a check box on a form). This consent is based upon clear language explaining what personal data is collected and how it will be used. Guidelines for obtaining consent are described below.

Guidelines for obtaining consent

- Simple and plain language must be used to communicate privacy terms
- Consent must be voluntary (opt-in)
- The data subject must take action to give consent
- Consent must be easily withdrawn

There is a parental component to consent when services apply to children under the age of sixteen (age may vary by member state). Where parental consent is required, organizations must make a reasonable attempt to verify guardianship.

It's important to note that consent is not always required to lawfully process personal data. Consent is not required where there is a contractual obligation with the data subject, public interest, or vital interest of the data subject.

Privacy

Protecting the rights of the individual is a key objective of GDPR. This is commonly referred to as Rights of the Data Subject. GDPR empowers EU citizens and residents with more control over what data they will freely share, how that data is used, and how it's managed. Below is a summary of the rights of the data subject provisions in the regulation.

Rights of the Data Subject

- *Transparent information, communication and modalities for the exercise of the rights of the data subject* – Response to data subject requests must be clear and in plain language. The responses must be made in a timely manner, but where requests are unfounded or excessive, organizations may either not satisfy the request or charge a fair fee to process it.
- *Information to be provided where personal data are collected from the data subject* – Organizations must provide data subjects certain information when data is collected. This information ranges from contact information of the controller and Data Protection Officer (DPO) to a description of the data collected to how long the data will be stored. The intent is to educate the data subject enabling them to make informed decisions.
- *Information to be provided where personal data has not been collected from the data subject* – This provision applies when personal data is collected from sources other than the data subject. The controller is obligated to inform the data subject when data is collected. This excludes when the data subject already has the information or when providing the information is impossible or involves a disproportionate effort.
- *Right of access by the data subject* – The ability to inquire whether the organization has personal data relating to the data subject, and, if so, what data is processed and for what purpose.
- *Right to rectification* – Organizations must correct inaccurate information identified by the data subject.
- *Right to erasure ('right to be forgotten')* – Data subjects may request organizations to erase their personal data. Erasure of data can be triggered by a data subjects' withdrawal of consent, unlawful processing of data, or the stated purpose for processing the data is no longer valid. There are scenarios where full compliance with the request is not mandatory.
- *Right to restriction of processing* – The processing of personal data may be halted when its accuracy is being contested or processing is unlawful and data subjects oppose erasure.
- *Right to data portability* – Data subjects have the right to receive information they have provided to an organization in a standard electronic format.
- *Right to object* – Data subjects have the right to object to the use of their personal data especially in the case of direct marketing purposes. This right to object also applies to automated decision-making and profiling where it can significantly harm the data subject.

GDPR attempts to balance protection of rights of the data subject with the ability to conduct business. For example, the right to be forgotten provision requires organizations to erase personal data, but data needed for valid business processing can be retained.

Compliance with the rights of data subject will require implementation of processes to support request handling. Automating processes and providing self-service will reduce the load on internal teams responsible for responding to these requests.

Protection

This section addresses the key requirements controllers and processors must fulfill to protect personal data. GDPR controller and processor protection requirements reflect industry standard practices. Compliance with existing standards such as ISO 27001 will greatly simplify GDPR compliance. The GDPR protection requirements include:

GDPR Controller and Processor Key Requirements

- *Data protection by design and default* – Principles must be applied, and protective controls must be designed during the development of solutions that process personal data. The intent is to build security in rather than retrofit controls. The intended outcome is more effective security.
- *Data protection impact assessment* – Prior to introducing new technologies, an assessment must be performed to determine the impact on personal data to ensure proper protection is maintained. The DPO must be consulted to determine the risk and obtain agreement on the security controls needed to reduce it to an acceptable level.
- *Records of processing activities* – An inventory of personal data processing must be maintained. The inventory must include information such as the purpose of processing, personal data description, data subject description, data retention, and protective controls.
- *Security of processing* – It's important to note that GDPR does not require specific technical controls to be implemented; however, Security of Processing does require a level of security appropriate to the risk. The organization must assess risk and ensure reasonable controls are in place to maintain the confidentiality, integrity, and availability of personal data. This ranges from authentication to pseudonymization to encryption.
- *Notification of a personal data breach to the supervisory authority* – Organizations must contact their supervisory authority within 72 hours in the event of a data breach.
- *Communication of a personal data breach to data subjects* – Breach communication is required when personal data is exposed and may cause harm to data subjects. Communication may not be required if the data is encrypted. Organizations must consult with their supervisory authority to determine if communication with data subjects is needed.

The protection requirements apply to all entities responsible for storing, transmitting or processing personal data. This includes Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) cloud services providers as well as other partners responsible for processing data in the technology supply chain (e.g., monitoring services). GDPR requires all of these providers to maintain GDPR compliance if they have a role in processing personal data.

APPROACH TO GDPR READINESS

Achieving GDPR readiness requires a dedicated effort to assess the situation and implement the right remedies to achieve compliance. The amount and type of personal data collected along with customer use cases contribute to the compliance effort. Other factors that contribute to the effort needed to achieve compliance include:

GDPR Compliance Effort Contributing Factors

- Maturity of privacy management practices
- Knowledge of EU personal data within the environment – where it's stored and how it's used
- Understanding of the technology environment associated with the storing, transmitting, and processing of personal data (includes third party services)
- Maturity of security within the environment

Organizations that possess reasonable maturity in these areas will extend less effort to achieve GDPR readiness. On the other hand, organizations ramping up capability must be prepared to dedicate the necessary resources.

Figure 2. Approach to GDPR Readiness

Figure 2, Approach to GDPR Readiness, describes the steps needed to prepare for GDPR and ultimately operationalize the processes needed to maintain compliance over time. Execution of these steps will satisfy the key GDPR requirements described earlier in this document.

Preparation

Organizations must take the necessary steps to prepare for GDPR compliance. This includes establishing ownership of data privacy to ensure accountability and obtaining a strong understanding of the regulation.

Assign GDPR Ownership

The organization must assign accountability for data privacy to ensure there is a proper understanding of GDPR requirements and how to comply with them. The DPO takes on this role. This role is critical to ensuring the organization can collect and process personal data needed to continue business operations while satisfying GDPR requirements.

All organizations are not required to hire a DPO. Organizations with less than 250 employees or perform minimal processing of personal data are exempt from the DPO requirement. Organizations should consult their supervisory authority to obtain guidance regarding the DPO requirement.

Understand the Regulation

A strong command of the regulation must be obtained prior to performing the assessment and pursuing implementation. The DPO must lead the effort to educate key stakeholders within the organization. This document provides basic insights, but it's strongly recommended to reference official GDPR documentation. There is an abundance of GDPR information. Below is a summary of the most helpful:

GDPR Reference Information

- General Data Protection Regulation full text [1]
- General Data Protection Regulation condensed text [2]
- Web-based reference of the General Data Protection Regulation [3]
- Handbook on the General Data Protection Regulation [4]

Assessment

After obtaining an understanding of the regulation and what's required, the organization must assess the risk associated with their activities as well as their ability to comply with GDPR requirements. The DPO must lead the assessment and ensure the right focus.

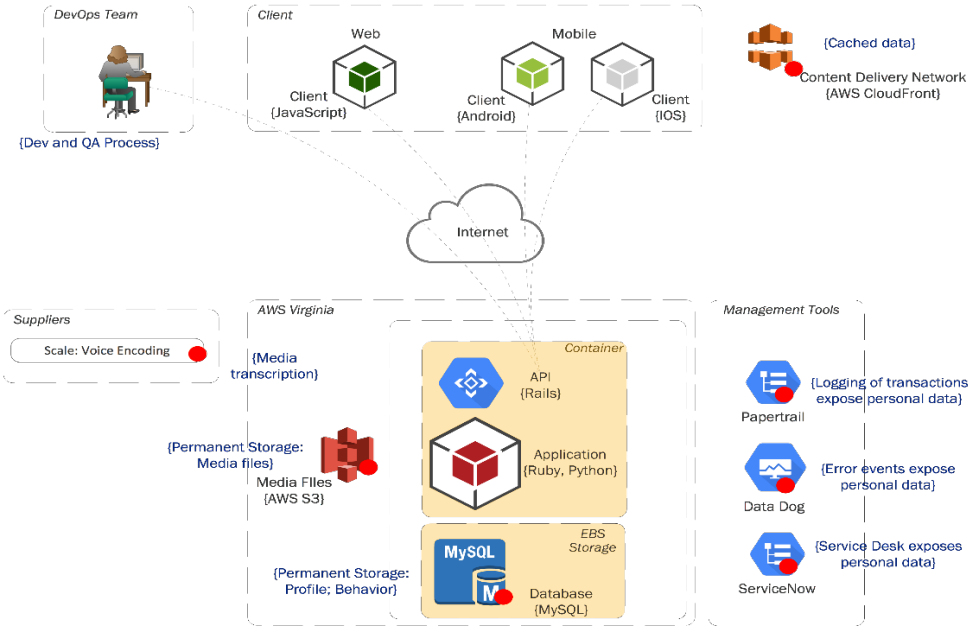
Understand the Risk of Activities

The first step in the assessment process is to understand the risk of current processing activities. Developing an inventory of services that collect or process personal data is mandatory. Organizations must address the following questions for each service to gain clarity.

- What categories of personal data are processed?
- What purpose is the data collected and processed?
- Where is the personal data processed and stored?
- Who is responsible for processing the data (e.g., internal department or third party)?
- What is the volume of personal data collected?

The inventory of services must be combined with a flow mapping the storage, processing, and transmission of personal data. Third party processors responsible for processing personal data must be identified. The objective is to follow up with an assessment of these third-party processors to ensure they are GDPR compliant.

Figure 3. Example Personal Data High-Level Technology Mapping



The comprehensive inventory and data flow view can now be used to assess the risk of activities. Table 1, Activities Risk Summary, provides an example risk rating. This helps to determine the risk to data subjects, level of focus needed for compliance, and potential impact of penalties. Organizations should focus on the high-risk activities and develop methods to reduce it. Options for reducing risk range from anonymizing data to encryption to eliminating the collection of data. A plan must be developed for each high and medium-high risk activity.

Table 1. Activities Risk Summary [5]

Activities likely to be high-risk	Activities likely to be medium-high risk	Activities likely to be low risk
▪ Large-scale processing of Sensitive Personal Data ▪ Automated profiling ▪ Systematic monitoring ▪ New data processing technologies ▪ CCTV monitoring of public spaces	▪ Processing Sensitive Personal Data ▪ Processing the personal data of vulnerable individuals ▪ Large-scale processing of personal data	▪ Anonymized data ▪ Pseudonymized data ▪ Secure small-scale processing of personal data

Perform the Readiness Assessment

A readiness assessment is needed to identify GDPR gaps. This readiness assessment focuses more broadly on the organization's ability to adhere to principles, comply with rights of the individual, and meet protection requirements. A survey should be used to guide the assessment and ensure the right points are addressed. The questions below are representative of the points that should be included in the assessment.

Example Assessment Questions

- Is there a lawful basis for collecting and processing personal data?
- Is consent properly obtained and tracked, where applicable?
- Are there processes in place to maintain rights of the individual?
- Are there processes in place to maintain the protection of personal data?
- Are processors, where applicable, compliant with GDPR?
- Are there processes in place to effectively manage the lifecycle of data?
- Are processes in place to support breach notification?
- Are processes in place to perform DPIA where applicable?

The organization should categorize the gaps identified according to risk and effort, and layout a plan to address them. The gaps plan must be combined with the activities plan to develop a comprehensive approach to reducing risk and complying with GDPR requirements. The DPO must lead the charge to execute the comprehensive plan.

Implementation

Implementation addresses the items needed to establish a foundation for GDPR compliance. This section provides insight into the implementation steps needed to inform the organization, address consent, and establish privacy and security controls.

Inform the Organization

Communication is key to effective achievement and maintenance of GDPR compliance. This starts with informing the organization to ensure personnel understand what GDPR means to the organization and what's needed from them. Additionally, GDPR must be included in security training and awareness to keep the organization informed over time.

A summary of the steps needed to inform the organization is described below. The key stakeholders include business and technical leadership, product managers, project managers, architects, customer care, and security personnel. These roles are critical to evangelizing effective practices throughout the organization to achieve and maintain GDPR compliance.

Steps to Inform the Organization

1. Educate business and technical leadership on the implementation plan and obtain buy-in and commitment of resources
2. Communicate GDPR principles to product managers, project managers and architects and help them understand how to apply them when designing products and solutions
3. Educate developers and operations personnel to apply principles and build in security when developing code and executing operational processes
4. Train customer care how to response to data subject requests and handle personal data
5. Communicate processor contractual language to procurement personnel – hold processors accountable for GDPR compliance
6. Update security and awareness program and educate the employee community on key GDPR concepts – personal data definition, personal data handling and incident reporting process

Address Consent

The DPO must work with the right personnel within the organization to identify where consent applies and how to obtain it. Legal personnel should be involved, as consent will most likely impact privacy terms. Keep in mind that opt-out is no longer an option. A summary of consent implementation considerations is described below.

Consent Implementation Considerations

- Inventory were personal data is collected from the user/customer
- For each instance of personal data, determine if consent is required
- If consent is required, update language to provide clear and concise information. Also, ensure the key points are addressed (e.g., data collected, how it will be used, how long it will be retained).
- Provide a means to affirm consent (check box). This includes implementation of the capability to track and report consent from data subjects.

Address Rights of the Individual

The DPO must provide input to determine how rights of the individual apply to the organization. This information is needed to guide development of processes to enable handling of data subject requests. Organizations serving many data subjects and collecting a significant amount of personal data should be prepared to handle a high number of requests. Automation is key for these organizations.

A summary of rights of the individual implementation considerations is described below. The considerations are few, but implementation can be time consuming. Keep in mind the considerations apply to all rights (see Figure 1, Key GDPR Requirements Summary).

Rights of the Individual Implementation Considerations

- Develop a process to authenticate data subjects submitting requests. It's important to ensure the individual making the request has the authority to do so.
- Establish a channel to enable data subjects to submit requests. The channel can be email, a web form, or some other medium. Consider the volume of requests and information that must be captured when selecting the channel.
- Implement internal processes needed to respond to the request. The response to some of these requests is nuanced and may require manual review.
- Develop a process to track requests and ensure proper notification is provided. Thirty day response is required, but the period can be extended for complex requests or excessive number of requests. The data subject must be notified within thirty days if additional time is needed.
- Train customer care personnel to handle requests
- Maintain a record of data subject requests and their outcome

The DPO must manage these processes to ensure the organization is handling requests in accordance with GDPR requirements. A lack of responsiveness can lead to data subjects initiating complaints with the supervisory authority.

Protect Personal Data

The GDPR protection requirements promote leading security practices to ensure the confidentiality, integrity, and availability of personal data. Organizations with mature security practices will require less effort to manage personal data risk. This section describes how to address the GDPR protection requirements referenced in the Keys to GDPR Requirements.

- *Data protection by design and default* – Educating product managers and architects as described in the Inform the Organization section of this document will ensure security is considered early in the design process. This will promote consideration of GDPR principles and guide the design and architecture of solutions along with software development activities. The organization should combine these principles with additional security principles to enable holistic risk management. Example security principles include:
  - Simplicity – Remove unneeded technologies, features, etc. to limit the attack surface
  - Least privilege – Limit interactive and programmatic access to sensitive data
  - Limited trust – Services accessing data must be authenticated, authorization must be limited, and transactions logged
  - Plan for failure – Assume technology/services will fail and account for protection of data when it occurs
  - Traceability – Ensure all transactions are logged and can be attributed to a user or program

- *Data protection impact assessment (DPIA)* – The DPIA is similar to risk assessments currently performed in many organizations. A DPIA should be performed when changes such as introduction of new technology or implementation of new software features impact access, processing, storage, or transmission of personal data. The organization must perform the impact assessment early in the design process. Below is a summary of considerations for DPIA implementation.

  DPIA Implementation Considerations

  - Define and document the criteria that triggers a DPIA

- Create a DPIA template document to ensure the right issues are addressed. For example, ensure the type of personal data is identified and who requires access to it. Additionally, identify any processors that will handle personal data and the exposure that may result.
- Personnel must assess the need (use criteria described above) for DPIA evaluation during solution or feature design
- Perform the DPIA
- Identify and prioritize risk
- Establish a plan to reduce risk to an acceptable level. This may include de-identification of data, minimizing data collected, or increased logging and auditing.
- Review the plan with the DPO and obtain approval. The DPO should communicate with supervisory authority if any ambiguity arises.

- *Records of processing activities* – The organization must establish and maintain an inventory (e.g., spreadsheet, database) of the processing activities associated with personal data. At a minimum, the activities assessed during the DPIA must be included in the inventory. Maintenance of the inventory is critical. There are three avenues to ensure this occurs: DPIA, change management integration, and governance review. Execution of DPIA must trigger an update to the processing inventory to capture new processing activities.

- *Security of Processing* - Each organization must ensure the right security controls are in place to effectively manage threats to personal data. Table 2, Security Controls Considerations, highlights the controls organizations should consider implementing to maintain the confidentiality, integrity, and availability of personal data. These controls are not referenced in the GDPR regulation but they are needed to manage risk. A reference to ISO 27002 artifacts is included in the table to demonstrate the readiness of organizations complying with or aligned to the ISO 27001 standard.

Table 2. Security Controls Considerations

GDPR Considerations	ISO 27002 Artifacts
IT Security Policy	Security Policy
Security Processes and Procedures	Security Operations Runbook
Information Classification	Asset Management Policy
Access Control	Access Control Policy
Data Protection (anonymization, pseudonymization, or encryption)	Cryptography Policy
Malware Protection	Operations Security Policy
Network Security	Communications Security Policy
Secure Software Development	Systems Acquisition, Development, and Maintenance Policy
Security in Systems Lifecycle Management	Systems Acquisition, Development, and Maintenance Policy
Security Monitoring	Operations Security Policy
Vulnerability Management	Operations Security Policy
Change Management	Operations Security Policy
Breach Notification and Communication	Security Incident Management
Disaster Recovery	Business Continuity Management
Processor Management	Supplier Relationships

Anonymization and pseudonymization of data is a key consideration when protecting data. Anonymization permanently eliminates the ability to personally identify an individual using the data (remove name, identification number, email address or other personal identifiers). Pseudonymization replaces personal data with other identifiers and stores the mapping in a separate file. Either of these approaches can be used or the organization can encrypt the personal data. The approach taken should be adequate to manage the risk.

- *Notification and Communication of Personal Data Breach* – The security incident management process must be updated to enable an effective response to personal data breaches. The first step after confirming a breach has occurred and validating the impact is notifying the supervisory authority. At a minimum, the following information should be made available to the supervisory authority.

  Supervisory Authority Notification Information
  - Description of the breached data source
  - Description of information included in the breach (data categories, data fields, number of records exposed)
  - Number of data subjects impacted by the breach
  - State of the personal data included in the breach (clear text/raw format, pseudonymized, anonymized, or encrypted)
  - Date breach occurred

  Based on the nature of the breach, a communication must be provided to data subjects impacted by the incident. The supervisory authority will advise on the need to contact data subjects. Business leadership, legal, and corporate communications personnel must clarify the process for customer (data subject) communication. Work out this process in advance. Attempting to develop this on the fly during an incident can be very painful and inflict harm to the business. Organizations should address the following points when communicating with data subjects.

  Data Subject Communication Points
  - What happened?
  - What data was exposed?
  - When was the data exposed?
  - What is the organization doing about the breach?
  - What actions can the data subject take to manage the potential impact?
  - What are the sources of additional information?

Maintenance

Maintaining GDPR compliance (or any compliance) can be a challenge. The key to success is integrating compliance into existing processes to ensure the right focus is maintained. This also leads to improved efficiencies. Upon completion of implementation, the following items should be addressed.

- Principles must be ingrained into the organization to promote the right culture. Continual training and consideration of principles during design, development, and change management is essential.
- Documentation of processing activities must be maintained
- Product development/service planning should consider personal data privacy and protection – lawful processing, cross-border considerations, and data minimization
- Planning and/or threat modelling process must incorporate DPIA.
- Incident response process must include supervisory authority communication and customer notification requirements when incidents include personal data of data subjects
- Update standard contract terms to address data protection clauses
- Third party risk management process must consider processor compliance
- Periodic review of request handling must be included in the governance process

SUMMARY

GDPR can be a complex to navigate. The primary intent of the regulation is to provide data subjects more insight into and control of their personal data. The key to successful compliance begins with establishing the DPO role (internal or external) and educating the organization.

Compliance isn't a one-time activity. Each organization must first recognize its obligation and then think more deeply about responsible collection and protection of personal data and approach the subject more strategically. The benefits of doing this not only apply to compliance, but also lead to increased customer willingness to adopt the organizations' products and/or services. Over time, consumers will understand and appreciate the value of data, and patronize businesses that handle their data responsibly.

Achieve and maintain effective privacy and security practices not because of the regulatory obligation; establish a culture that values data and treats it with the care it deserves.

REFERENCES

[1] General Data Protection Regulation, full text
http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

[2] General Data Protection Regulation, condensed text http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[3] Web-based reference of the General Data Protection Regulation http://gdpr-info.eu/

[4] Handbook on the General Data Protection Regulation
https://www.whitecase.com/publications/article/chapter-1-introduction-unlocking-eu-general-data-protection-regulation

[5] White & Case Guidance on Risk Analysis
https://www.whitecase.com/publications/article/chapter-2-preparing-gdpr-unlocking-eu-general-data-protection-regulation

48 Wall Street
Suite 1100
New York, NY 10005
Phone 212.918.4560

info@satoriconsulting.com