WHITE PAPER

Three Pillars for Successfully Addressing GDPR

Trustwave®

Overview

The General Data Protection Regulation (GDPR) defines how personal data should be collected, processed and stored. The key goals of the GDPR, which goes in to full effect on May 25, 2018 are:

- Give European Union citizens and residents greater control over their personal data
- Unify data protection laws in all European countries, which also simplifies the regulatory environment for international business
- Update data protection laws to incorporate Internet, mobile, social media and other current and emerging technologies

GDPR is a comprehensive data protection law for Europe as well as any organizations doing business in Europe. The regulation in its entirety is 88 pages long and includes 99 articles supported by 173 recitals. As you move your organization toward achieving and maintaining compliance with this far-reaching and complex regulation, we recommend that you structure your efforts around three key pillars for successfully addressing GDPR:

1. Understand your Processes
2. Manage Your Data
3. Develop an Ongoing Data Privacy and Security Lifecycle

Each of these pillars with recommended best practices is detailed below.

Pillar 1: Understand your Processes

A key first step to addressing GDPR is to understand fully how GDPR applies to your organization and to your data. But because GDPR is broad in scope and impacts all processes related to personal data, this understanding must go well beyond what is typical for most regulatory compliance. It can't be achieved by a siloed effort with a focus on IT practices. Typically, the affected data is not isolated into a specific network environment as it is with other data types or compliance mandates.

You must:

- Understand the GDPR both broadly and specifically with a view toward which of the 99 articles apply to your organization.
- Understand the regulated data your organization stores, processes or controls.
- Understand fully how data flows within your organization and the different collection and storage mechanisms for structured and unstructured data.
- Understand when your organization is a data processor and when it is a data controller. Many organizations play both roles and the requirements are different.
- Educate your organization to help refocus its mindset about personal data to meet the requirements of GDPR.

When evaluating the scope of GDPR, most people quickly understand that it will apply to personal data related to email communications with context that may identify individuals. The reach of GDPR goes far beyond normal marketing interactions, however.

For example, the Human Resources (HR) team, which manages employee personal data, has a key role in identifying where personal data exists and how it is maintained and stored. In addition to documenting the processes for the organization's staff, HR should identify the processes for retaining information from prospective employees. Was consent obtained from the applicant to retain the data; how was that consent captured? What is the retention policy? Could an applicant easily recover that data should they need to?

Application developers also need to be aware of the information they are collecting and evaluate the data and processes relative to the GDPR. Review of the data collected by the application offers an opportunity for data minimization and a determination of whether the data meets the security principles in the regulation.

The user activity data should not be repurposed for business intelligence without specific permission from the user. There must be processes in place to adhere to the "right to be forgotten." When a user cancels a service or deletes an account, your organization should respect the right of the user to delete all their account information and related data and make that process visible. Deleted accounts that are stored as "inactive" with associated personal data may result in GDPR penalties.

If data leaves the European Union, you will need to ensure the country where the data is received has either an adequate transfer mechanism or appropriate safeguards defined. For data that remains in the EU, this does not apply. Organizations must check that adequacy decisions are current; this can be verified with the European Commission.

When creating a detailed map of how personal data flows through your organization, include the types of data extraction and reporting that your organization performs. Even mature organizations often do not have a full view of the types of information that are being shared with groups such as the sales team, the marketing department, the Board of Directors or business partners.

Process review must include personal data in all its forms and for its entire lifecycle: electronic, paper, stored on media. Further, your organization must understand when you are the processor and when you are the controller for each process and data set. GDPR applies differently to each role. Most organizations will be both controller and processor depending upon the process:

- In the controller role, gathering the data, you must have appropriate reasons for obtaining the data and only use that data for the purpose that was intended.
- In the processor role, processing the data on behalf of the controller, there is a different set of responsibilities that must be met.

To successfully comply with GDPR, your entire organization may need to shift its perspective about personal data and who owns it. Your organization is the custodian, not the owner of the data, which belongs to the data subject. Think of data as DNA in document form – the ownership is clearly with the data subject.

Pillar 2: Manage Your Data

Good data management goes far beyond securing data; it involves maintaining data integrity and the full lifecycle of data management. One of the biggest challenges of the GDPR is meeting the rights of data subjects regarding their personal data. These rights include appropriate and timely access to their personal data, granting and removing permissions, changing data, and stopping a process that includes
their personal data.

Another consideration is that many organizations do not understand the content of their data and how to value it appropriately when assessing the risks to the data during its lifecycle, including handling and transmission. The first line of defense for good data management is employee training, followed by technology implemented by IT. To move forward with a full appreciation of the value of your data and the systems and processes managing the data, your organization needs to consider:

- Where is my data?
- Is my solution or processing appropriate to my customer needs?
- How is consent obtained and documented?
- What is the retention policy?
- How do we ensure effective and efficient response to a request for information from a data subject?
- Do we have processes for appropriate and timely communication when there has been a data breach?
- Have we established policies and procedures related to the above?
- What is the cost per data element if it is lost?
- What volume of data do you keep or control?

Your organization should ensure your solutions are fit for their purpose and that you can identify or act on any data subject request. Recognize that customer information may be in emails and may be very difficult to remove or manage.

After a thorough data management review, most organizations will find that some important data is left in unexpected pockets and unprotected. Identifying these areas of exposure allows your organization to remediate the issues and move toward better data management.

Pillar 3: Develop an Ongoing Data Privacy and Security Lifecycle

To successfully address GDPR, your organization should adopt a practice of continuous process improvement for the ongoing data privacy and security lifecycle. Testing and remediation should be practiced for current processes, while significant updates to systems and technologies create the appropriate inflection points for instituting "privacy by design and default" as required by GDPR. Privacy by design is an approach to systems engineering which takes privacy into account throughout the whole engineering process.

The data privacy and security lifecycle must be considered beyond digital data. As noted, GDPR applies to personal data in all its forms, including paper-based and data stored on media. Understanding where the data lives, what the processes are, and all the organizational members who touch it, is a key part of bolstering the data privacy and security lifecycle. Security awareness training for the organization will help address some of the requirements.

For current processes with privacy data, organizations should have an ongoing program that:

- Evaluates controls
- Establishes a GDPR baseline (security maturity and risk assessments are critical for baseline analysis)
- Remediates any gaps found
- Tests and further remediates any non-conformities

Note that the testing of security controls should be done with a real-world simulation. Unlike testing required by some other compliance and data security standards, where an effective test need only determine whether you are able to break in to a specific data environment, good GDPR testing will include the complete process. GDPR testing should incorporate how data is handled, secured, destroyed, and which people have access to the data and processes to test the complete lifecycle. This type of extensive testing is often referred to as purple teaming, with the red team simulating the attack and the blue team instituting counter measures. This fuller picture of the exposed data and appropriate defenses provides the knowledge needed for adequate remediation.

It is critical to consider GDPR when introducing new solutions and project management. The adoption of new solutions, new deployments and indeed any change in technologies or processes, is an opportunity to integrate privacy by design. Don't let old technology and old ways
of operating dilute your efforts to improve your data privacy and security lifecycle.

Getting Started

Ensure that your GDPR effort is understood to be an organization-wide initiative and that it can't be siloed to a single department such as IT.

The fastest path to compliance will be to engage a knowledgeable expert to help you. Your expert can help you facilitate the critical first step of broadly identifying your data and processes throughout your organization. From there, your expert can help you with your risk and/or security maturity assessment and development of an ongoing data privacy and security program.

How Trustwave Can Help

Trustwave delivers key GDPR services based on its deep understanding of compliance requirements and security expertise. Trustwave can help you assess how well you are meeting GDPR requirements and help you create a strategic plan for improving your organization's compliance. GDPR services include:

GDPR Workshop

- Helps you understand the scope of the regulation and the requirements
- Helps you understand the extent to which your entire organization must engage in addressing the GDPR

GDPR Privacy and Information Security Risk Assessment

- Helps you holistically and strategically assess how well your organization is addressing the GDPR
- Helps you develop a strategic plan for remediating gaps

Data Privacy Impact Assessment

- Helps you evaluate ongoing compliance with your high-risk processes as required by the GDPR
- Additional services to support your organization's GDPR compliance:

Security Maturity Assessment

- Helps you understand the levels of controls you have in place within your organization and helps you identify any that need to be adjusted to meet the GDPR requirements

SpiderLabs® Purple Teaming Service

- Simulates threats to your organization based on real-world intelligence to train your team in both the defensive and offensive arts. Dedicated researchers, red teamers and blue teamers create tactics, techniques and procedures that closely replicate real-world threat actors to help your organization resist, detect, respond and recover. During this engagement, we actively coach your blue team to detect and respond with our Trustwave SpiderLabs experts in your own environment.

Data Security and Monitoring

- Helps secure, protect and monitor your data at rest for compliance with GDPR

Trustwave also offers a broad security portfolio and industry-leading managed security services to help you incorporate the up-to-date solutions required to adhere to the GDPR.

For more information,
visit **General Data Protection Regulation Compliance**.

Trustwave®

TRUSTWAVE.COM