The GDPR and US Small and Medium-sized Companies: Simple Tools to Begin the Compliance Process

Jeffrey Hall

Executive Summary

The European Union's (EU) General Data Protection Regulation (GDPR) becomes fully enforceable on May 25, 2018. Many small and medium-sized enterprises (SMEs) in the United States are not aware they will be affected. They do not realize that the deadline is looming. Some have never heard of the GDPR.

The GDPR expands the scope of the European Directive that it replaces and introduces new requirements, and financial and operational penalties for non-compliance. SMEs that must comply with the GDPR will benefit from guidance and simple tools, which are free or inexpensive:

1. To conduct an initial GDPR readiness assessment
2. To execute a data mapping exercise
3. To ensure that website cookie and tracking technologies meet the GDPR's consent and notification guidelines
4. To enable individuals' access to their data and the processing status and purpose, as well as the ability to "be forgotten", by having their personal data removed

Acknowledgement

I would first like to thank my Critical Challenge Project advisor, Professor Deborah Hurley of the School of Professional Studies at Brown University. From the time I first approached her to advise my project to the submission of the completed paper, Professor Hurley provided me consistent, firm, and compassionate guidance. Drawing on her extensive experience within the privacy and data protection field, she kept me moving in the right direction, while also ensuring that my work remained my own. I am truly honored to have met and worked with a professional of her caliber.

I would also like to thank Bruce Cowper, who is the Senior Trusted Cloud Advisor, National Cloud Programs for Microsoft and is their subject matter expert for achieving GDPR compliance. Bruce helped me refine my topic scope during my initial research and made sure I understood the implications of my assertions. His no-nonsense industry perspective was extremely valuable and refreshing.

Finally, I would not have been able to complete this project without the unfailing support of my wife, Tammy. During our 20 years of marriage, she has supported me during the best and worst of times and remained a steadfast example of love, strength, and the indomitable human spirit. From the bottom of my heart, thank you and I love you very much.

Introduction

In 2016, the European Union (EU) adopted the General Data Protection Regulation (GDPR), which will become fully enforceable on May 25, 2018. Compared with prior regional and national laws within the European Union, the GDPR has increased range of applicability. It applies not only to organizations established in the EU that process personal data of EU residents, but also to organizations, even if not established in the EU, that offer goods or services to EU residents or monitor their behavior.

Many organizations in the United States are still unaware that the GDPR may apply to them. Other US organizations are seeking to understand and comply with the GDPR, but questions abound as the May 2018 deadline looms. In order for US SMEs to begin the process of meeting the GDPR requirements, they must first learn about the regulation, including, importantly, whether they fall within its scope and the penalties for non-compliance.

US SMEs will need both an in-depth understanding of the GDPR's technical requirements and an awareness of the free or inexpensive resources that currently exist to help them fully meet these compliance steps:

1. Conduct an initial GDPR readiness assessment.
2. Create a data mapping inventory of their organizational data flows

3. Ensure website cookie and tracking technologies meet the GDPR consent and notification requirements
4. Verify that technical capabilities exist to allow users easy access to their personal data

The General Data Protection Regulation

The GDPR is the EU's privacy and data protection regulation, which will replace the Data Protection Directive (DPD) 95/46/EC. The GDPR was adopted to address certain aspects of the DPD, such as with regard to subsequent technological advances, and to harmonize further the data protection laws across Europe.[1]

For example, since the GDPR's predecessor was a directive and not a regulation, each EU member state had to adopt individual laws, in order to implement the DPD. This resulted in variations in treatment of personal data among the EU member states. The GDPR will have direct effect, without requiring the additional step of national legislation. Moreover, with the advent of cloud computing and ever larger data traffic across national borders, the GDPR will further facilitate the free flow of personal data across the EU.[2]

[1] "Home Page of EU GDPR." EU GDPR Portal. Accessed March 29, 2018. http://www.eugdpr.org/.
[2] Corrales, Marcelo, Mark Fenwick, and Forgó Nikolaus., *New Technology, Big Data and the Law* (Singapore: Springer Singapore, 2017), 33.

The GDPR includes 99 articles and 173 recitations[3], which are organized into chapters covering specific themes.

Substantial Penalties for Violations of the GDPR

Among the new features of the GDPR are the liabilities for non-compliance, by which violations can incur penalties as high as four percent of the organization's annual global turnover or 20 million Euros, whichever is larger.[4] Such a penalty could drive a SME out of business. In addition to these fines, there are other severe penalties, such as the loss of the right to conduct business in the EU.[5]

Technical Requirements

Organizations operate as controllers or processors or both, with regard to personal data that they hold. Article 4 of the GDPR defines a data controller[6] as a legal entity that determines the purposes and means of the processing of personal data. Article 4 defines a processor[7] as a legal entity that processes personal data on behalf of the controller. It is possible and often the case that the controller also processes the data, functioning as both controller and processor.

---

[3] "General Data Protection Regulation." 2016/679 Regulation (EU). *Official Journal of the European Union* (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1.
[4] "Frequently Asked Questions about the GDPR." EU GDPR Portal. Accessed March 29, 2018. http://www.eugdpr.org/gdpr-faqs.html.
[5] General Data Protection Regulation, Article 58(2f).
[6] General Data Protection Regulation, Article 4(7).
[7] General Data Protection Regulation, Article 4(8).

Pursuant to Article 32, controllers and processors must implement appropriate technical and organizational measures, in order to ensure that any personal data of an individual residing in the EU, which is processed by that organization, are sufficiently protected.[8]

In addition to the language of Article 32, the words "technical and [security] organizational measures" appear ten more times in the text of the GDPR.[9] The pervasive references underscore their importance.

Although technical measures are a critical component of the GDPR, the specifications for how organizations must implement the required technical measures are noticeably absent from the regulation. According to GDPR Recital 15, the protection of natural persons should be technologically neutral, in order to prevent creating a serious risk of circumvention.[10]

Nonetheless, this general language has created much consternation among organizations, which fear that they will not be compliant by the May 25, 2018, deadline and may, therefore, incur severe penalties.[11] In order for US SMEs to meet the GDPR's requirements, they will need clear and efficient guidance on the steps that they will need to

[8] General Data Protection Regulation, Article 32.
[9] General Data Protection Regulation, Articles 4, 5, 24, 25, 28, 30, 32, 34, 83, 89.
[10] General Data Protection Regulation, Recital 15.

[11] "News Release." 2018. *Veritas Study: Organizations Worldwide Fear Non-Compliance with New European Union Data Regulation Could Put Them Out of Business*. Accessed March 29. https://www.veritas.com/news-releases/2017-04-25-veritas-study-organizations-worldwide-fear-non-compliance-with-new-european-union-data-regulation-could-put-them-out-of-business/.

take.

Meeting the GDPR Requirements

Organizations seeking to meet the requirements of the GDPR will need to complete these critical tasks:

- Identify gaps in existing technology capabilities to support privacy and personal data protection
- Create a data mapping inventory of their organizational data flows
- Ensure website cookie and tracking technologies meet the GDPR consent and notification requirements
- Verify that technical capabilities exist to allow users easy access to their personal data

Identify gaps in existing technology capabilities to support privacy and personal data protection

In order for a SME to meet the requirements of the GDPR, it must first undertake a thorough, rigorous review of its current technological capacity to protect the privacy and personal data of its employees and customers. As data can exist within many corporate systems in both structured and unstructured formats, it is important to identify not only all systems containing the data, but also the interfaces employees use

to access them and any shortcomings in the hardware and software components of each system.[12]

US SMEs should consider the following list of questions as a basis for understanding their ability to properly secure the data they hold. These questions will naturally lead to further questions and allow the organization to create a complete picture of their existing readiness state.

Technical Security Measures

- Has the organization deployed one or more firewalls at the edge of the corporate network? Have these firewall appliances been configured with a robust set of traffic forwarding rules that is based on a recent analysis of the types of data flowing in and out of the network?
- Has the organization deployed one or more Intrusion Prevention Systems (IPS) and/or Intrusion Detection Systems (IDS) at the edge of the corporate network? Are these appliances configured to use the latest signatures? What process is in place to ensure they always contain the most current signatures?

[12] "GDPR Services." 2018. *24 Solutions*. Accessed March 29. https://www.24solutions.com/en/compliance/comply-with-the-requirements-of-the-new-data-protection-act/gdpr-services/.

- Does the organization use a Security Information and Event Monitoring (SIEM) system? Is this SIEM fully configured with a complete inventory of corporate assets? Have all monitoring agents been installed on all endpoints intended to be monitored? Are the appropriate alerts configured?

Disaster Recovery and Business Continuity

- Has the organization deployed backup and recovery software capable of capturing full, incremental, and differential file backups? Where is this data stored? How many backups are maintained? Is there a documented restore test process in place? How often does the organization test the restoration of backup files?

Data Protection

- Does the organization use encryption, such as Transport Layer Security (TLS), Datagram TLS (DTLS), or other encryption and hashing technologies within the enterprise network? Are virtual private network (VPN) technologies, such as IPsec, used for all remote access connections?
- Are all storage appliance hard disks encrypted? Are all desktop, laptop, and mobile device hard disks encrypted?

User Administration

- Does the organization centrally administrator all user authorization and authorization via methods such as LDAP, RADIUS, TACACS, etc.?
- Has Role-Based Access Control (RBAC) been implemented to provide segregation of duties and least-privilege access?

Recommendations for SMEs to identify their current GDPR readiness state

Given the close proximity of the May 25, 2018 compliance deadline, it is critical that SMEs use existing resources to gauge their GDPR readiness. Fortunately, a number of free and inexpensive resources exist. Any resources used will need to be tweaked, however, to reflect the organization's unique hardware and software resources, as well as overall networking and computing architecture.

The following five free or inexpensive resources, from providers with years of experience and solid reputations, may be helpful:

1. Nymity (https://www.nymity.com/gdpr-toolkit.aspx)

   The Nymity GDPR Compliance Toolkit is available, free of charge, and includes not only detailed documentation for understanding their toolkit and the relevant GDPR articles, it also includes a spreadsheet with "two sets of questions to ensure demonstrable compliance is embedded

throughout [the] organisation; one for the privacy office and one for the operational and business units."

2. IAPP and TrustArc Partnership (https://iapp.org/resources/article/gdpr-readiness-tool/)

   The International Association of Privacy Professionals (IAPP) and TrustArc have partnered together to provide a single-user license of the TrustArc Assessment Manager, which is provided free for IAPP members. This assessment includes more than 60 questions that are mapped to specific GDPR requirements.

3. Microsoft (https://www.gdprbenchmark.com/)

   Microsoft offers both a basic and detailed version of their GDPR readiness assessment. The basic version is a quick online self-evaluation tool, while the detailed version is available for download by Microsoft's partners at http://aka.ms/gdprdetailedassessment.

4. Varonis (https://info.varonis.com/gdpr-risk-assessment)

   Varonis's free GDPR readiness assessment will be conducted by a dedicated engineer and address these tasks:

   - Identify in-scope GDPR data
   - Find and revoke excessive access to personal information
   - Audit user activity and detect risky behavior / ransomware

- Identify and prioritize gaps in GDPR compliance

5. OneTrust (https://onetrust.com/pricing/#assessment-automation)

   OneTrust offers both a free GDPR assessment for IAPP members and also a free trial that helps organizations understand their existing readiness gaps via free templates, a self-service portal, and detailed executive reports.

Create a data mapping inventory of their organizational data flows

An organization will only be able to protect fully the personal data that it stores and processes, if it knows where the data are and how they are being used. In compliance with GDPR Article 30, organizations must fully understand how data flows through their environment, as a prerequisite to securing it sufficiently and analyzing it for risks. Maintaining a data mapping inventory also enables the organization to respond better to individuals requiring that their personal data be corrected, accessed, or deleted.[13]

According to IT Governance, a UK-based consulting firm focused on IT governance, risk management, and compliance solutions, data mapping has the following three key elements:[14]

[13] "Data Mapping Automation." n.d. OneTrust. https://onetrust.com/products/data-mapping/.
[14] "Data Flow Mapping under the EU GDPR." 2018. *IT Governance*. Accessed March 29. https://www.itgovernance.co.uk/gdpr-data-mapping/.

1. Understanding the information flow – The transfer of information from one location to another, such as between entities within the EU, between an external entity and an entity within the EU, etc.
2. Describe the information flow – Will there be unforeseen or unintended uses of the data during the full lifespan of the data's processing and transmission? Is too much data being collected? Are all parties to the data transfer fully aware of the implications of their actions during the data transfer? What will the potential future use of the data be?
3. Identify its key elements – What kind of data is being collected, stored, and processed? How is this data categorized? In what format is the data stored (i.e. hardcopy, digital, etc.)? How has the data been transferred and shared internally and externally to the processor's environment? Through which locations has the data passed?

GDPR Article 30(1) states the minimum required data that must be identified and mapped:[15]

- Organization's name and details
- Purpose for processing data
- Description of the categories of individuals and personal data

[15] General Data Protection Regulation, Article 30.

- Categories of recipients of personal data
- Details of transfers to third countries
- Retention schedules
- Description of technical and organizational security measures

Recommendations for SMEs to map their organizational data flows

Following the initial readiness assessment, the organization's next task will be to conduct a data mapping exercise using this procedure:

1. Hold one or more meetings among the company leadership and senior IT personnel to identify the types of data being collected, stored, and processed.
2. Identify the computer systems and storage appliances where the data is being processed and stored. Is data being processed and stored in multiple physical locations? If so, all locations and systems will need to be identified.
3. Identify all applications being used to process personal data.
4. Record and track this information using simple tools, such as spreadsheet applications and diagramming tools, like Microsoft Visio.

During this process, an organization can utilize existing free or inexpensive data mapping services, such as the following:

1. IAPP and OneTrust partnership (https://iapp.org/resources/article/data-mapping-automation-tool/)

   Through a partnership with IAPP, OneTrust offers a free license to IAPP members for its Data Mapping Automation Tool. This tool provides pre-built templates to the user, which are designed to greatly simply the data mapping process. This tool not only creates a data flow inventory via various input methods like questionnaires, scanning, workshops, and bulk import, but it also creates visual data maps that are automatically created, based on the input data.

2. Vigilant Software (https://www.vigilantsoftware.co.uk/topic/data-flow-mapping-tool)

   Vigilant Software's Data Flow Mapping Tool is available for less than $1,500.00 and provides an easily-repeatable solution that logs personal data items involved in the processing. Additionally, it generates data flow reports, embeds data protection by design, and gives optional access to security controls.

Ensure website cookie and tracking technologies meet the GDPR consent and notification requirements

One of the primary and often first interactions that individuals have with an organization is via its webpages. In many webpages, personal data are requested and stored, in order to provide the appropriate viewing or browsing experience. The GDPR includes requirements for how organizations must implement the technical abilities to notify individuals of any consent obligations. Additionally, the organization must allow the individual to opt out of any data collection requirements that the user finds undesirable. The technical ability to query the user for this input, store the selections, and enforce the user's wishes are critical steps in meeting the GDPR's technical requirements.

Given user expectations of powerful, interactive, dynamic, and content-rich webpages, organizations spend significant time and budget incorporating a wide range of sophisticated technologies in their websites. Organizations are estimated to outsource as much as 80 percent of their website functionality to third-party vendors, which specialize in such services as data management, multimedia hosting, marketing analytics, content delivery, customer identification, and payment processing. As a result, organizations may typically control less than 25 percent of the code running in their

websites.[16] Further, it is common for websites to have dozens of third-party cookies, which are often unauthorized and persistent. To make matters worse, the third-party vendors providing services and storing cookies in an organization's websites change continuously, which makes forcing them to adhere to a standard of compliance very difficult.

On the positive side, the GDPR provides a consistent definition and application of website compliance requirements across all EU member states. To date, organizations have had to follow a number of different compliance frameworks promulgated by the individual EU member states.[17]

Recommendations to assist SMEs in ensuring their website and tracking technology meets the GDPR consent and notification requirements

Given the complexity of understanding which third-party vendors are implementing their code and cookies within a given website, it is important that organizations utilize the existing free and inexpensive solutions already available on the market. In this section, three solutions are presented:

1. IAPP and OneTrust partnership (https://onetrust.com/iapp-eprivacy/)

[16] "What the EU's General Data Protection Regulation Means for Website Compliance." 2017. *Digital Content Next*. June 28. https://digitalcontentnext.org/blog/2017/06/23/eus-general-data-protection-regulation-means-website-compliance/.
[17] "Cookie Consent & Website Scanning." n.d OneTrust, https://onetrust.com/products/cookies/.

OneTrust offers a free license to IAPP members for their Website Scanning & Cookie Compliance tool, which scans a single website against a database of 5.5 million known cookies. The user is able to monitor their website scanning within a centralized dashboard. Additionally, the tool automatically updates the organization's cookie policies, based on the website scans.

2. TrustArc (https://www.trustarc.com/products/consent-manager/)

   The TrustArc Cookie Consent Manager provides an easy means of managing user consent, whether it is implied consent, expressed consent, or a hybrid mix of the two. Via this tool, the organization's administrators are given a range of important functionalities, such as privacy compliance scanning, reverse IP address lookups, privacy compliance reports, visual customization and branding, browser language settings detection, and consent application programming interfaces (API) to allow integration into existing tools and applications.

3. Cookiebot (https://www.cookiebot.com/en/)

   Cookiebot is a simple tool that is currently used on over 9,000 websites, manages over 100,000,000 monthly user consents, and supports over 40 languages. This tool helps administrators achieve three

critical compliance tasks: Cookie consent, cookie monitoring, and cookie control.

Ensure technical capabilities exist to allow users easy access to their personal data

Among the most discussed requirements of the GDPR are the rights of users to request their personal data, as well as the deletion of that data. These rights granted to the user ("data subject") appear in the following three GDPR articles:

1. Article 15: Right of access by the data subject[18]
2. Article 17: Right to erasure ("right to be forgotten")[19]
3. Article 20: Right to data portability[20]

In order to meet the GDPR's requirements for ensuring user access to personal data, as well as ensuring the right to have them removed from the controller's and/or processor's systems, the organization must ensure the appropriate software and operational processes are in place.

For example, the organization must be able to provide a copy of all personal data, at no cost, in an electronic format that is both machine-readable and transmitted easily. The organization must also be able to provide a status to the user of his or her personal data, as well as the purpose for which the data are being processed. If the user

[18] General Data Protection Regulation, Article 15.
[19] General Data Protection Regulation, Article 17.
[20] General Data Protection Regulation, Article 20.

desires that his or her data be deleted, the organization must have the software automation and/or processes in place to satisfy this requirement, unless there is legitimate justification for retaining it.[21]

Recommendations for SMEs to ensure they have the technical means to provide users with access to their personal data

To support the requirements of GDPR articles 15, 17, and 20, an organization should do the following:

- Complete a data mapping exercise to know where all data are, whether they are sensitive or not, and the purposes for which they are being processed.
- Ensure software applications or automation processes are in place to search quickly and easily for a specific user's data. The data must be able to be easily exported into a machine-readable digital copy (for example, a .csv or .xml file).
- All interactions with the personal data should be logged into a centralized monitoring system that is sufficiently redundant to maintain high availability. This monitoring system should also be able to detect and alert appropriate

[21] Blažek, Maja. 2018. "SharePoint and GDPR Compliance - Classify, Prepare and Protect." *SysKit Blog*. Accessed March 29. https://blog.syskit.com/sharepoint-and-gdpr-compliance-classify-prepare-and-protect.

personnel, in the event that interactions with the personal data fall outside established “acceptable use” boundaries.

- A web portal should be created to provide the user with easy access and insight into his or her data, as well as how the data are being processed and their current status.

It is possible for SMEs to implement many of these measures manually. There are also commercial solutions. For example, OneTrust provides a solution for building a data subject rights request web portal.[22]

Via its solution, OneTrust assists the organization in tailoring a branded web form and linking the form to the organization’s privacy policy webpage. When individuals submit data access requests, the organization is notified. The web portal will also automatically request an extension, if a deadline approaches. When the user request is fulfilled, the collected personal data is transmitted securely to the individual and the transaction is logged. Finally, all required audit documentation is created.

Conclusion

[22] “GDPR Compliance.” n.d OneTrust, https://onetrust.com/products/gdpr-compliance/.

The stakes have never been higher for US SMEs that engage in activities falling within the scope of the GDPR. For those organizations that have not met the GDPR requirements or do not yet realize that they will even be affected, the GDPR's May 25, 2018 deadline is rapidly approaching.

To meet the GDPR's technical requirements, SMEs must take quick action using free or inexpensive resources currently available. The first step for organizations is to become aware of and more familiar with the GDPR.[23] There are a number of overview guides.[24] [25] Of particular importance for US SMEs will be to determine if they fall within its scope. Also, a good understanding of the financial and operational penalties for non-compliance will highlight the urgency for compliance and consequences for failing to do so.

SMEs beginning the process of complying with the GDPR's technical requirements will first need to conduct a readiness assessment of their ability to protect the personal data they hold. During this phase, the organization will inspect every hardware and software component of their computing, storage, and networking infrastructure and explore their ability to secure personal data at rest and in transit. As questions are answered, additional questions for deeper

[23] "Summary of Articles Contained in the GDPR." EU GDPR Portal. Accessed April 5, 2018. https://www.eugdpr.org/article-summaries.html.
[24] Calder, Alan, ed. *EU GDPR: A Pocket Guide*. Ely, Cambridgeshire, UK: IT GOVERNANCE Publishing, 2016.

[25] Calder, Alan, Richard Campo, and Adrian Ross. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. Ely, Cambridgeshire, UK: IT Governance Pub, 2016.

validation will naturally arise. To guide them through this process, various toolkits, readiness assessment packages, and benchmarking tools are available.

After identifying the technological gaps for securing personal data, SMEs will need to create a data inventory of where their personal data is located, including on which computer systems, storage appliances, and networks. In order to fully protect the personal data an organization holds, as well as to provide additional services mandated by the GDPR, their location must first be known and documented. Along with involving organizational stakeholders in identifying where the data physically resides, SMEs should also use existing free and inexpensive tools to complete this vital step in meeting the GDPR's technical requirements.

In today's globally-connected world, a user's first experience with an organization is most often its corporate website and other online resources. For this reason, SMEs must be mindful to ensure that their website cookie and other tracking mechanisms comply with the GDPR's technical requirements for appropriate consent and user notification. Existing free or inexpensive resources exist to enable SMEs to navigate this complex set of mandates.

One of the biggest technical changes introduced by the GDPR is the expanded focus on ensuring users not only have access to the processing status of their personal data, but to the data itself and their right to obtain a copy of that data and if desired, have it removed from the organization's systems. SMEs will need to ensure they use currently-available resources to allow users to easily contact them with any such requests, as well providing the feedback or personal data in an easily-read format within a reasonable timeframe.

While the GDPR includes requirements for other areas, including operational and personnel aspects of protecting personal data, using the free and inexpensive resources currently available on the market to meet its strict technical requirements is a very effective place for US SMEs to begin their journey to compliance.