WHITE PAPER

GDPR Compliance and Its Impact on Security and Data Protection Programs

An Osterman Research White Paper

Published January 2017

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

Protecting personal data has been an important issue in the European Union (EU) for more than 20 years, and the recently ratified General Data Protection Regulation (GDPR) takes data protection to an entirely new level. In addition to a new set of legal requirements that necessitate both organizational and technological responses, the GDPR is applicable to almost every organization around the world that collects or processes data on residents domiciled within the EU, including permanent residents, visitors and expatriates. Compliance is thus predicated on the geographical location of the individuals about whom an organization holds personal data, not the domicile of registration for the organization.

This represents a sea change in how organizations must protect the personal data of anyone in the EU, and it may have implications for how they protect the personal data of non-EU residents, as well. Hence, the "General" Data Protection Regulation could better be called the "Global" Data Protection Regulation, and in light of the financial penalties associated with non-compliance, requires serious attention and action from all organizations doing business across Europe (including the United Kingdom post-Brexit), both in the EU and in the European Economic Area (EEA).

KEY TAKEAWAYS

- The GDPR is the new data protection regulation from the EU, released in May 2016 with an implementation date of May 25, 2018. Organizations anywhere in the world that collect or process personal data on EU residents must comply with the new regulation, or they will face significant financial penalties and reputational damage.

- Complying with the GDPR requires both organizational and technological measures in response. Organizational measures include appointing a Data Protection Officer, policies and training on handling personal and sensitive personal data, and an approach for executing a Data Protection Impact Assessment (DPIA). Technological measures for protecting personal or sensitive personal data include data classification, data loss prevention, encryption, managing consent more explicitly, data transfer limitations, and technologies that enable data subjects to exercise their rights to access, rectify, and erase personal data held by data controllers (subject to certain conditions).

Complying with the GDPR requires both organizational and techno-logical measures in response.

- The GDPR is focused on the *protection* of personal data, not merely the *privacy* of personal data. Complying with the protection mandate requires a higher degree of proactive and far-reaching effort on the behalf of organizations that control or process personal data.

- The enforcement date of May 2018 is less than 18 months away, and all organizations affected by the GDPR, by virtue of controlling or processing personal data on or about EU residents, must take immediate action to develop a coordinated organizational and technological response to address the new requirements.

- Among the mid-sized and large organizations surveyed for this white paper, all of which will be subject to the GDPR, the majority (58 percent) are not sufficiently familiar with the wide scope of the regulation and the penalties it includes. Only 10 percent believe their organizations are "completely ready" to comply with the requirements of the GDPR.

ABOUT THIS WHITE PAPER

A survey was conducted for this white paper, some of the results from which are included herein. However, all of the results will be published in a separate survey report shortly after the publication of the paper.

This white paper and survey were sponsored by Actiance – information on the company is provided at the end of this paper.

THE REGULATORY IMPERATIVE OF THE GDPR

WHAT IS THE GENERAL DATA PROTECTION REGULATION?

The GDPR is the new regulation on data protection for personal data across the EU. It replaces the earlier 1995 EU Directive on data protection, bringing a newly modernized and harmonized regulation for all EU member states. It raises the game on data protection in some significant areas, while continuing with the foundational principles of the original Directive.

The GDPR is important for two key reasons:

- First, it is likely to apply to all organizations, even those not based in Europe, because it mandates certain protections and provisions for any organization that controls or processes personal data on EU residents where processing is related to offering goods or services ("irrespective of whether a payment of the data subject is required") or monitoring behavior that takes places place within the EU (Article 3). Being located outside of the EU does not grant an exemption to a data controller.

- Second, the cost of non-compliance is significant, with a financial penalties regime of up to a €20 million fine or 4% of total worldwide annual turnover of the preceding financial year, whichever is higher.

PROTECTION OF PERSONAL DATA IN THE EU

In 1995, the EU released a directive on the protection of personal data to be applied across all members of the Union. It enshrined the right of residents within the EU to the protection of their personal data, and imposed certain obligations regarding the handling and processing of personal data on organizations located within the Union. As a directive, however, Member States were free to specify the obligations in different ways, leading to inconsistency in the regulation of data protection across the EU, and a host of negative downstream consequences for organizations doing business across multiple states.

The GDPR… replaces the earlier 1995 EU Directive on data protection, bringing a newly modernized and harmonized regulation for all EU member states.

In May 2016, after four years of exploration, discussion, and negotiation, the 1995 Directive was replaced by a common regulation – Regulation (EU) 2016/679 – commonly called the General Data Protection Regulation (GDPR). Except where permitted in the GDPR, member states are no longer free to add nuances in the implementation of the law because the new law is a common *regulation* instead of a *directive*. The legal framework from the Directive has been carried forward, updated for the current data protection, security and associated technological landscape of 2016, and certain new far-reaching requirements have been introduced. The 1995 Directive is "repealed with effect" from 25 May 2018 (Article 94), the same day the new regulation goes into full effect.

It is worth noting that the GDPR is complemented with a specific directive for the collection and processing of personal data related to criminal proceedings, and while there is commonality between the new Regulation and the new Directive, the specific provisions and requirements under Directive (EU) 2016/680 are not the focus of this white paper.

WHAT IS PERSONAL DATA?

The scope of the GDPR is "personal data", which is defined in Article 4 as "any information relating to an identified or identifiable natural person ... who can be identified, directly or indirectly ... by reference to an identifier." Identifiers listed in Article 4 include name, identification number, location data, and other identifying factors, such as physical, mental, and cultural, among others. While that represents a broad scope of personal data, not all data collected or processed by an organization is personal in nature. Of particular note is that previously collected personal data that has been fully anonymized and cannot be re-identified to an individual is excluded

from the compliance requirements of the GDPR, enabling its use for data analytics, for example.

DRIVERS FOR INTRODUCING THE GDPR

The GDPR is one element of the European Commission's Digital Single Market priority, which is aimed at moving from 28 national markets to a single market that is designed for the digital age. The new regulation makes a contribution toward this priority in a number of ways, two of which are worth calling out:

- Firstly, it both modernizes (takes account of the rapid and significant technological developments of the past two decades) and harmonizes the legal framework for data protection across the EU, removing the nuanced implementation approaches that flourished under the previous Directive. With one law on data protection across all 28 member states, organizations no longer have to manage different data protection approaches per market. The European Commission estimates this will save businesses around €2.3 billion annually.

- Secondly, there is now a level playing field for organizations related to data protection. Essentially, the test of applicability has shifted from whether the organization is domiciled within an EU market to whether the data collected or processed relates to an individual natural person who is domiciled in an EU market. If so, the principles of data protection apply regardless of where the organization is based.

COMPLIANCE REQUIRED BY MAY 2018

The new regulation was published officially in early May 2016, and was effective immediately with implementation required by all affected organizations by May 25, 2018. This means that organizations now have less than 18 months (as of the publication of this white paper) to comply with the data protection provisions of the regulation and, as noted previously, lack of physical presence in the Union is not grounds for exemption. The transition period has already begun and is now one quarter completed.

With one law on data protection across all 28 member states, organizations no longer have to manage different data protection approaches per market.

SIGNIFICANT FINES FOR NON-COMPLIANCE

The regulation has global impacts with a real bite attached. Organizations found in breach of the requirements can be subjected to a range of administrative interventions, as well as a two-tiered financial penalty regime: a €10 million fine or two percent of global revenue (whichever is the highest), or a €20 million fine or four percent of global revenue (whichever is the highest). Those numbers can become quite large, quite quickly. For example, one of the banks in the United Kingdom suffered a data breach of personal data during 2016, and if this had been subjected to the financial penalties regime of the GDPR, could have seen a fine approaching £2 billion, in addition to the indirect financial and non-financial impacts including reputational damage.

In ascertaining the amount of any fine to apply, Article 83 of the GDPR makes clear the intent is that it should "be effective, proportionate and dissuasive." Any fine must be calculated in light of multiple factors, including the nature, gravity and duration of the infringement; the presence of negligence, organizational and technological mitigations in place; the categories of personal data affected; and whether the organization itself notified the supervisory authority of the infringement. Article 83(2) lists 11 separate factors for a supervisory authority to evaluate when setting the level of the fine, with Articles 83(4) and 83(5) specifying the types of infringements that fall into the two-percent and four-percent regimes, with infringements on the basic principles for processing, data subjects' rights, and transfers of personal data falling under the higher fine regime. The four percent/€20 million fines also relate to Article 58(2), whereby the controller/processor is non-compliant with an order by the supervisory authority.

Any organization currently holding personal data on EU residents essentially has one of two choices: cease doing business with EU residents (and permanently delete or fully anonymize all currently held personal data), or proactively comply with the requirements of the GDPR. A third option of doing the bare minimum required will heighten the risk of falling foul of the regulation, and increase the likelihood of being subject to significant fines. Even if your organization can pay any fine levied under the GDPR, doing so does not get you any closer to protecting the personal data of EU residents, and if you want to stay in business after paying the fine you will then need to take the more proactive approach available now.

REQUIREMENTS OF THE GDPR

The GDPR introduces a set of core requirements for organizations controlling or processing personal data for EU residents. The overall intent is to protect the rights of natural people with respect to their personal data, and compliance with the GDPR will require both organizational and technological measures.

Providing an exhaustive summary of the requirements of the GDPR is beyond the scope of this white paper, but relevant provisions are highlighted below. Please note that the purpose of this white paper is not to provide legal advice for specific organizations, and all organizations affected by the GDPR are encouraged to seek competent legal advice from either Corporate Counsel or an external law firm.

ABILITY TO DEMONSTRATE COMPLIANCE

In the final analysis, which is a good place to start, organizations have to be able to demonstrate compliance with the GDPR, a task that covers both organizational and technological measures. Article 24 sets the general obligations for a data controller ("the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary"), and Article 28 for data processors (who must "implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject"). Any measures implemented in line with the GDPR may reduce the severity of any fine levied for non-compliance. For example, supervisory authorities are required to take into account the organizational and technological measures that have been implemented (Article 83(2)(d)), and adherence to "codes of conduct" or "approved certification mechanism" (Article 83(2)(j)).

Organizations have to be able to demonstrate compliance with the GDPR, a task that covers both organizational and techno-logical measures.

LEGAL BASIS FOR PROCESSINGS

The right to process personal data must be lawful, with six categories of lawfulness listed in Article 6, the first of which is that the data subject has "given consent to the processing ... for one or more specific purposes." Other lawful bases include contract performance, compliance with a legal obligation, and protection of the vital interests of the data subject. Among other implications, organizations will need to be explicitly clear on the lawful basis of all processing activities, and have the ability to comply with any request from the data subject to cease processing if consent is withdrawn (where consent was the only lawful basis).

SPECIAL CONDITIONS WHEN PROCESSING SPECIAL CATEGORIES OF DATA

The GDPR has elevated protection for special categories of personal data. Article 9(1) states the general prohibition as such: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." Article 9(2) then lists ten separate exclusions to this general prohibition, including consent from the

data subject, the protection of vital interests of the data subject, and where the data subject has made such information public, among others.

Note that the GDPR extends beyond a general prohibition on the processing of special categories of personal data and enshrines the principle that the use of data itself may be sensitive. For example, examining the name of an employee's partner could be used to reveal sexual orientation, which could be used to cause harm to the data subject, and is thus also prohibited.

RECORDS FOR KEEPING TRACK OF ALL PROCESSING ACTIVITIES

Article 30 requires that controllers "shall maintain a record of processing activities under its responsibility," and lists seven types of information to be maintained, including the purpose of the processing, a description of categories of data subjects and personal data, and who will see the personal data after processing, among others. Processors have a similar requirement to record all categories of processing activities. Both controllers and processors are required to keep these records in written form, with electronic form permitted under Article 30.

INCREASED STANDARD OF CONSENT

Under GDPR, organizations need to know the legal basis of controlling or processing personal data. One such legal basis is the consent of the data subject, but gaining consent has an elevated standard compared with the earlier Directive. Specifically, as defined in Article 4(11), consent must be "by a statement or by a clear affirmative action." This therefore prohibits the use of opt-out consent (assumed consent), and GDPR also prohibits making consent a condition of participation. Note too that the data subject has the right to withdraw their consent to processing of his or her personal data.

Under GDPR, organizations need to know the legal basis of controlling or processing personal data.

NOTIFICATION OF DATA BREACHES WITHIN 72 HOURS

Consider the following:

- An employee loses his or her company-issued computer at the airport, and the information on the drive is not encrypted.
- An employee emails a spreadsheet containing customer names and contact details to the company's marketing agency, but accidentally sends it to the wrong email address.
- An unencrypted USB thumb drive with customer details is dropped at the train station.
- A malware attack uses compromised user credentials to get access to the customer database, laying bare millions of customer records.

What do all four have in common? All are potential data breaches, with a high likelihood of exposing personal data to people who are not authorized to access it. Requirements in the GDPR come into play at two levels in these scenarios:

- Once an organization becomes aware of a data breach of personal or sensitive personal data, it has a 72-hour window to notify the relevant supervisory authority of the breach (Article 33). Article 33(3) specifies four requirements in such a notification: the nature of the personal data breach (including categories of data and approximate number of data subjects impacted), the name and contact details of the firm's data protection officer, an analysis of the likely consequences of the breach, and measures taken or proposed to be taken to mitigate negative effects. The exemption to these requirements is where "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons," by for example, having the data encrypted.

- The second requirement is to notify data subjects individually of any personal data breach that has a high risk to their individual rights and freedoms (Article 34), and must contain similar information to that notified to the supervisory authority. There are some exemptions and exceptions noted in Article 34(3), such as if the organization had "appropriate technical and organizational measures" (e.g. encryption) in place to protect the data.

APPOINTMENT OF A DATA PROTECTION OFFICER (DPO)

Organizations are required to appoint a data protection officer if processing of personal data and/or sensitive personal data is regular and systematic (Article 37), although there are various forms the appointment can take on account of organizational type and size. The data protection officer requires "expert knowledge of data protection law and practices" (Article 37(5)), must have certain freedoms (Article 38), and has a list of prescribed tasks to execute (Article 39). These tasks include informing and advising data controllers, processors, and employees of their obligations under the GDPR, monitoring internal compliance, and cooperating with the supervisory authority, among others.

RIGHT TO DATA PORTABILITY

Data subjects have the right to data portability (Article 20), meaning they can request the personal data they have supplied to a controller in "a structured, commonly used and machine-readable format" in order to give it to another data controller. If technically feasible, the data subject can require the current controller to transmit it directly to the new data controller.

DATA PROTECTION BY DESIGN AND BY DEFAULT

Data controllers are required to design the data protection principles of the GDPR into the very fabric of technical systems and organizational processes (Article 25). This design process is required to consider "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing." Further, this is supposed to happen when deciding how to carry out a processing as well as when the actual processing takes place.

The specific requirements under the GDPR are many and varied.

Article 25 imposes a very high standard on organizations. First, a thoughtful and integrated assessment of four separate factors is required—the state of the art, the cost of implementation, the types of processing, and the associated risk profile. Second, the rights of data subjects per the GDPR need to be understood conceptually and mapped practically to technical capabilities and organizational processes. For example, how will an organization respond to an Article 15 Access request, and how does the technology being used support the access rights of data subjects? This analysis must be executed for the other rights, too, including rectification, erasure, and restriction of processing.

Article 25 has implications for data sovereignty, either when situating data centers in the EU region or by only embracing cloud services that offer jurisdictional assurance of storage, processing, and appropriate security within the EU. Organizations will need to select IT vendors and cloud providers who can demonstrate that the requirements of the GDPR are built-in by design and by default to their respective solutions, not bolted on to legacy architectures that become ever more fragile.

MANY OTHER REQUIREMENTS

The specific requirements under the GDPR are many and varied. Other requirements include, in brief:

- **Article 15. Right of Access by the Data Subject**
  A data subject has the right to ask a data controller whether his or her personal data is being processed, and if so, can request access to both the personal data and information on processing, recipients, data transfers, and subsequent rights (such as the right to complain to a supervisory authority, or the right to request

rectification, erasure, or a restriction on future processing). Data subjects have the right to know if and when their data is transferred to a third country or an international organisation, along with the safeguards in place to ensure ongoing protection of the data after transfer. A data controller must provide a copy of any personal data undergoing processing at no charge the first time it is requested, but has the right to charge "a reasonable fee based on administrative costs" for subsequent requests.

- **Article 16. Right to Rectification**
  If a data controller holds inaccurate personal data about a data subject, the data subject has the right to supply the correct information to get their personal data updated. The data controller is required to rectify the inaccurate information "without undue delay."

- **Article 17. Right to Erasure (Right to be Forgotten)**
  Subject to certain conditions, a data subject has the right to request the erasure of his or her personal data held by a data controller. Conditions include the withdrawal of consent, previous unlawful processing, and other legal compliance erasure mandates. Data controllers, on the other hand, have the ability under the GDPR to decline an erasure request if it falls within one of the several exclusions in Article 17(3), such as compliance with a legal obligation, public interest for public health, and legal claims. Nonetheless this requires that organizations have a very clear legal understanding of why they are processing data, the appropriate legal bases, and when required, a technological ability to erase all affected data promptly.

- **Article 18. Right to Restriction of Processing**
  As with the right to erasure, subject to certain provisions, a data subject also has the right to have his or her personal data excluded from future processing activities - either temporarily or permanently. Conditions include contested data accuracy, unlawful processing, and the desire of the data subject to be excluded from processing activities but to not have their personal data erased for various legal and historical reasons.

Data subjects can object to automated processing and profiling based on their personal data.

- **Article 19. Notification Obligation for Controllers**
  A data controller has the obligation to notify each recipient of any personal data newly impacted by the exercise of a data subject's rights in relation to rectification, erasure, or restriction. If the data subject requests details on recipients, the data controller is required to supply it.

- **Article 21. Right to Object**
  A data subject has the right to object to the processing of his or her personal data at any time where the legal basis is "the performance of a task carried out in the public interest," "the exercise of official authority vested in the controller," or for the purposes of the "legitimate interests" of the controller or a third party (Article 6(e) and (f)). The data subject can also object to processing for the purposes of direct marketing and profiling for direct marketing activities.

- **Article 22. Automated individual decision-making, including profiling**
  Data subjects can object to automated processing and profiling based on their personal data, and at minimum have the right to "obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision." This right is designed to stop data controllers making legal and other significant decisions regarding a data subject purely on an automated basis.

- **Article 28. Processor Requirements**
  If a data controller engages another organization for processing activities, the processor must have implemented "appropriate technical and organizational measures" to meet the requirements of the regulation, and in addition to other specific requirements, must assist the controller in responding to requests related

to the rights of data subjects.

- **Article 30. Records of Processing Activities**
  Data controllers must keep records of the processing activities for which they are responsible, with a list of specific information to be retained for each record.

- **Article 32. Security of Processing**
  Data controllers are required to implement technical and organizational measures to ensure an appropriate level of security is in place for processing activities, such as pseudonymization, encryption, regular testing of organizational and technical measures, and more.

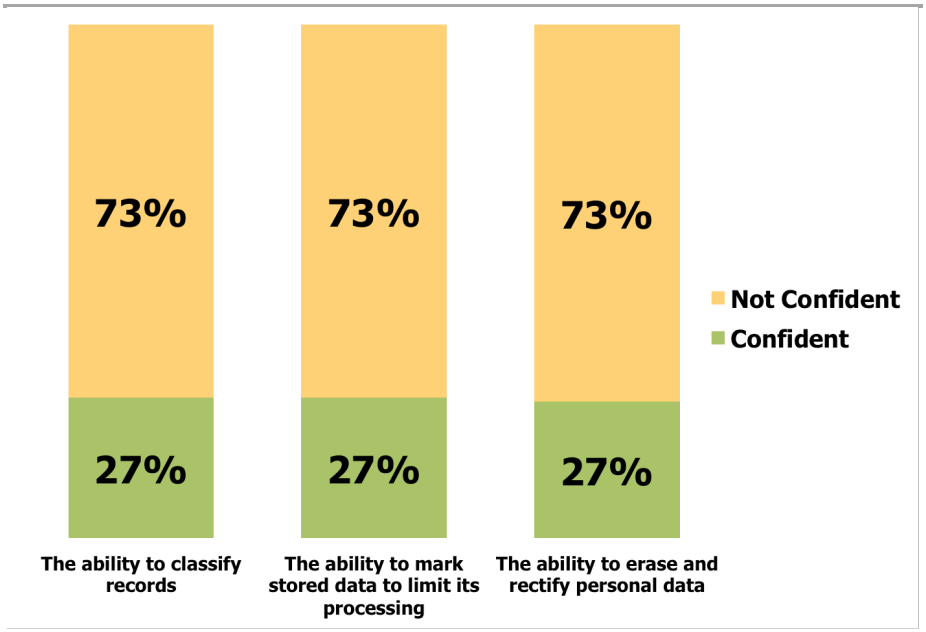
- **Articles 44-50. Transfers of Personal Data to Third Countries or International Organizations**
  The GDPR outlines specific requirements governing when and where personal data can be transferred to third countries or international organizations. While Safe Harbor was determined to be invalid in late 2015, it was replaced by the EU-US Privacy Shield framework as of mid-2016. The goal of the framework is to permit US companies to transfer data on EU residents while still maintaining the protections afforded under the GDPR.

MOST ORGANIZATIONS ARE NOT PREPARED FOR THE GDPR

The survey for this white paper was conducted with mid-sized and large organizations that are already subject to privacy laws and that store and process data for residents of the EU – i.e., organizations that will be subject to the GDPR. However, we found that most organizations are not ready to satisfy the compliance obligations of the GDPR, as shown in Figure 1.

Only 29 percent of organizations believe that their organ-izational and technical approaches to data protection today are "mature".

Figure 1
Organizational Confidence in the Ability to Meet Key Requirements of the GDPR



Source: Osterman Research, Inc.

Moreover, the research found that only 29 percent of organizations believe that their organizational and technical approaches to data protection today are "mature", and

only 38 percent of organizations had allocated budget in 2016 to achieve compliance with the GDPR.

TECHNOLOGIES REQUIRED FOR GDPR COMPLIANCE

With the clear majority of personal data being captured, stored, structured, organized and processed in digital forms across today's digital landscape, compliance with the GDPR is going to require appropriate technological responses. To do otherwise would be foolhardy and out of step with the requirements of the GDPR that specifically call out the need for technological answers. As noted above, complying with the GDPR requires a complementary mix of both organizational and technological responses.

In reviewing the requirements of the GDPR, the following categories of technologies will be essential for every organization controlling or processing data on EU residents.

MODERN APPLICATIONS FOR COLLECTING, STORING, AND PROCESSING PERSONAL DATA

Organizations need to select up-to-date and modern applications to govern the processes of collecting, storing, and processing personal data about EU residents. The rights that EU residents newly have under the GDPR - such as the right to access, the right to rectify, the right to erasure, and the right to the restriction of processing, among others - requires an exceedingly well-governed data management environment that handles both the big picture requirements of GDPR as well as the specific rights across all instances of personal data. Organizations will need to track consent requests and approvals for many different actions, and tie that consent to the specific personal data collected or updated for that purpose. Organizations will need the ability to know when a legal basis other than consent is being used to justify storing and processing personal data, and the specific personal data values to which this applies - and for how long. Organizations must retain records of processing activities, transfer activities, and access or disclosure activities.

Implementing appropriate organizational and techno-logical safeguards on all master production systems that contain personal and sensitive personal data is essential.

Taking this approach is merely an enactment of Article 25, on data protection by design and by default. Organizations without such an applications landscape will be unable to meet even the conceptually simple access, rectification and erasure rights in a timely and cost-efficient manner, let alone address the more complex rights around data portability, objections, and automated decision-making for individuals. Organizations should be challenging their current IT applications providers for details on how these requirements are met in current applications, as well as exploring the options from new generation IT providers.

DATA DISCOVERY, CATALOGUING AND CLASSIFYING

Implementing appropriate organizational and technological safeguards on all master production systems that contain personal and sensitive personal data is essential. But it is not enough. Sufficient controls are required for:

- Copies of production databases containing personal data taken for testing, development, or analytics purposes. Leaving these unprotected or unsecured will place the organization out of compliance with GDPR.

- Spreadsheets and other data sources populated by exporting customer contact and profiling details for a mail merge. Storing this information in a local folder that is synchronized to a cloud storage service like Box, Dropbox, or OneDrive for Business is likely to compromise GDPR mandates.

- Email archives, whether stored on-premises, in cold storage or in the cloud. These are likely to contain personal data that must be protected under the GDPR.

In light of the massive volumes of data that exist in unstructured forms across the organization, a technological response to identify, catalogue, and classify all such data sources is an essential step, laying the foundation for taking appropriate action on any and every form of personal data thereby identified.

DATA LOSS PROTECTION

Data Loss Protection (DLP) capabilities will be required to aid in the prevention of inadvertent data breaches, by blocking outgoing email, other messages and file movements that contain personal data that has not been protected by appropriate safeguards, e.g., data encryption. In some situations encryption can be automatically applied to personal data when it is classified or identified in an email message or document attachment, while in other situations it would make more sense to quarantine the message to enable an organizational response.

DATA ENCRYPTION

Encryption is one of the few specific technologies called out in the text of the GDPR, and its presence there essentially mandates its use by organizations. Encryption of data in systems and applications reduces the potential impacts of a data breach because the data is rendered useless – meaning that data subjects cannot be identified – without the encryption key. For complete protection in all use cases, encryption should protect data at rest and while being used in applications to ensure that if a breach occurs on any system, the information remains confidential and does not trigger the GDPR penalties. Some vendors offer the ability to encrypt personal data within an existing database format, thereby greatly enhancing the level of data protection while not requiring a re-development of current systems and applications. This style of encryption of data enables encryption of data while at rest, in-use or in-motion, because the existing database and applications can continue to function normally without relying on the use of data in the clear. With appropriate organizational safeguards, this can then enable secure data analytics on data in production environments. A related and important consideration is tokenization because of the additional protection it can afford by offering additional data residency assurance.

Encryption is one of the few specific technologies called out in the text of the GDPR, and its presence there essentially mandates its use by organizations.

EMAIL ENCRYPTION

Another important use of encryption technology is the encryption of communications inside and outside the organization, such as via emails. Email remains the main form of collaboration in enterprises, with the average user receiving over 100 emails per day and sending 30. These emails and attachments could represent one of the most vulnerable points in the journey of data inside and outside a company's network. Either by the automated trigger of a DLP and/or by user initiation (classifying or adding classified attachments), sensitive emails must be protected with email encryption. Email encryption needs to be capable of protecting both internal and external sensitive messages and all attachments. Some email encryption solutions can also be used to encrypt all data flowing into a cloud-office application provider, including files used in collaboration. The separation of duties between encryption and storage providers gives end-users peace of mind in the cloud.

DATA BREACH IDENTIFICATION AND BLOCKING

The GDPR requires notification to a supervisory authority within 72 hours of detecting a data breach, as well as notification to individual data subjects if there is a high likelihood that the data breach will have adverse effects for them (for example, because personal or sensitive personal data was breached). By implication, therefore, organizations need the ability to proactively sense that data has been breached, audit the extent of the breach, and create an appropriate organizational response. DLP, as noted above, is an example of a specific technology to aid in this area, along with other relevant technologies, including communications analytics, penetration testing software and services, threat protection, anti-malware, and monitoring of how privileged user accounts are accessing personal and sensitive data sources.

PSEUDONYMIZATION

The GDPR explicitly talks about the use of pseudonymization as a means of protecting personal data. In practice, pseudonymization means separating data elements that can be used to identify a specific person – such as their name or common identification number (e.g., passport number or Social Security number) – from the data being tracked (e.g., the book purchased). It is not a failsafe approach per the data protection requirements of GDPR, however, because pseudonymized data can be re-identified to a specific natural person through various organizational and technological means. Fully anonymized data, on the other hand, is unable to be re-identified to a specific natural person unless new information is supplied to enable the re-identification process.

Various vendors offer means of pseudonymizing or masking data, encrypting identifying data, or even encrypting identifying data inside structured data sources, such as databases. These technological methods can be combined within organizational approaches to greatly reduce the likelihood of personal data being compromised, leaked, or exposed unnecessarily. For example, a common valid use of personal-type data is in software development and testing environments, and also for analytics and reporting purposes. If data is pseudonymized for these purposes, identifying personal data is not disclosed unnecessarily, and is also not left lying around in less protected or unprotected data sources that could be compromised through a targeted attack.

One reason that pseudonymized data is not considered a failsafe approach is that if the lookup source data or encryption keys are compromised through a data breach, personal and potentially personal sensitive data can therefore be exposed too. The GDPR still recommends the use of pseudonymization, but organizations that use products and services to implement this method are not given an automatic exemption to data protection requirements under the Regulation.

DATA PORTABILITY

Data subjects have the right to request an export of their data in a usable format that can be given to another vendor or service provider to import into its service. Data subjects can request that organizations provide this data to them directly or transfer it to the new vendor. Current data schemas and storage methods need to be examined to ensure an export is feasible, economical, and timely, and products and services to facilitate the portability requirement should be explored for implementation. Enabling customers to perform their own export of personal data through a secure, self-service web interface is a good way of balancing access and economics.

Data subjects have the right to request an export of their data in a usable format that can be given to another vendor or service provider to import into its service.

ENDPOINT SECURITY AND MOBILE DEVICE MANAGEMENT

Computing devices need to be protected from loss or theft through mobile device management capabilities, such as remote wipe and kill. A lost device could be the weak link in the data protection chain, leading to a data breach based on information stored on the device or accessible through still active user credentials. Enforcing certain settings in order for a device to connect to the network at all – such as local encryption, password complexity, the presence and currency of security software, and the removal of the local administrator account – will be an essential part of protecting the organization within the GDPR framework.

PERIMETER SECURITY

Perimeter security – erecting defences to keep malicious actors out – was essential when organizations ran data centers and other on-premises infrastructure. In the age of multiple cloud services the "perimeter" is much harder to control, but technologies that monitor perimeter security should still be one element of the security defences maintained by organizations. Security over the data itself is becoming more important (hence the essential requirements around data discovery, classification, and encryption), and perimeter security is less able to dissuade internal malicious actors, such as a disgruntled employee, from doing harm from the inside.

CLOUD STORAGE AND SHARING SERVICES

Cloud storage and sharing services have been widely adopted in recent years, addressing a valid user need for easier access to relevant files and documents across multiple computing devices. Many of these services offer extremely large personal storage footprints, and support the synchronization of files to one or more computing devices. This user bonanza, however, could cause a data protection nightmare under GDPR through the inadvertent sharing of personal data by employees collaborating with others inside and external to the organization, not to mention the prospect of malicious disclosure by disgruntled employees or external actors.

Organizations need to ensure they have selected and deployed appropriate cloud storage and sharing services in the first place, and are actively blocking or discouraging the use of non-authorized services. Proactive monitoring of sharing actions should also be in place to minimize the likelihood of data breaches. A key decision criterion in selecting a cloud storage service is the relentless use of encryption to protect data stored in the cloud service (encrypting data in transit, in use and at rest), either provided directly by the vendor itself or enabled through a third-party service provider to give the right level of risk mitigation.

ANTI-MALWARE

While a successful malware infiltration can render computers unusable – a costly annoyance and interruption that most organizations will want to avoid – of more serious concern under GDPR is the potential for malware to harvest credentials for user and administrator accounts. Harvested credentials can then be used to access data sources across the organization (both on-premises and in cloud services), including those containing personal and sensitive personal data. Preventing a malware infection in the first place requires a multi-faceted technological response, including anti-malware software and services and advanced threat protection. Advanced threat protection services need to become commonplace, in order to deliver capabilities that pre-analyze every click on a URL to ensure it does not contain a malware payload, and likewise protect against email attachments being used as an attack vector.

Blocking malware through technological means is essential for any organization wanting to become GDPR-compliant.

Blocking malware through technological means is essential for any organization wanting to become GDPR-compliant (specifically to reduce the likelihood of data breaches, among other implications), and highlighting dangerous or compromised URLs or attachments helps educate the user population about the security risks facing the modern organization. Moreover, organizations must show that encrypting and tokenizing with format-preserving technologies that also preserve context, logic, relationships and meaning will allow data to be portable and neutralize the effects of the malware that typically goes after data in the clear. Finally, while malware can create havoc as above, organizations will also need to protect against malware-less attacks that use trickery to impersonate a trusted or senior-level executive in order to gain access to sensitive information.

APPLICATION SECURITY TESTING

The GDPR requires that organizations embrace data protection "by design and by default," which means data protection considerations should be an always-on approach, not an afterthought at the tail end of a development job or selection process. Approaches that we have explored above – such as data encryption, classification and pseudonymization – should therefore become initial discussion and design points. Likewise, technologies that proactively test for security vulnerabilities during development and deployment should be evaluated as a way of operationalizing a data protection by design mindset and approach.

EVALUATING CLOUD SERVICE PROVIDERS

Organizations should look for cloud providers that offer specific assurances on the requirements of GDPR. For example, cloud services should be designed to address the access, rectification, and erasure rights of data subjects. Equally, there should be jurisdictional assurance that all EU data is kept solely within the EU, using multiple

data centers within the EU for redundancy and consistent data protection. Multi-national organizations with significant operations outside of the EU will require an appropriate cloud architecture to meet differential data protection requirements in its various markets. Cloud providers that meet GDPR certification standards give good assurance to customers that the technical side of the law is addressed appropriately, although this technical readiness must be met with appropriate organizational measures too.

"WITH DUE REGARD TO THE STATE OF THE ART"

One of the challenges facing lawmakers is how to account for future technological advances that could be used to achieve compliance with certain provisions, without having to re-issue a legal framework every time something new comes to market. Within the GDPR, the phrase "with due regard to the state of the art" is such a future-oriented attempt. While a few specific technological approaches are mentioned in the text of the GDPR – such as encryption and pseudonymization – organizations are given a much broader mandate to ensure the state of the art for data protection is considered when selecting or designing applications, services, and products used for processing personal data (Articles 25 and 32).

For example, new state of the art approaches currently coming to market include behavior analytics, privileged access management and format-preserving encryption (FPE):

- Behavior analytics examines the normal behavior patterns of employees across the organization and, when a divergence is noted – for example, when the user account accesses applications not previously accessed, accesses data at unusual times of the day or night or from foreign locations, or there is a spike in emails with attachments sent to a personal email address – an exception is raised for further investigation. Unusual behavior could signal an employee going rogue or the presence of compromised credentials, thereby enabling early detection and risk mitigation.

- Privileged access management, on the other hand, adds a layer of protection to mitigate against IT administrators with higher access rights to data sources and potentially encryption keys from causing harm, again either through rogue actions or compromised credentials.

- FPE, which encrypts content so that its format is identical to the plain text input, is useful because it helps to overcome the problems associated with the integration of encryption into applications that have well-defined data models. FPE can make encryption easier to implement and to ensure that it is more readily used in existing applications.

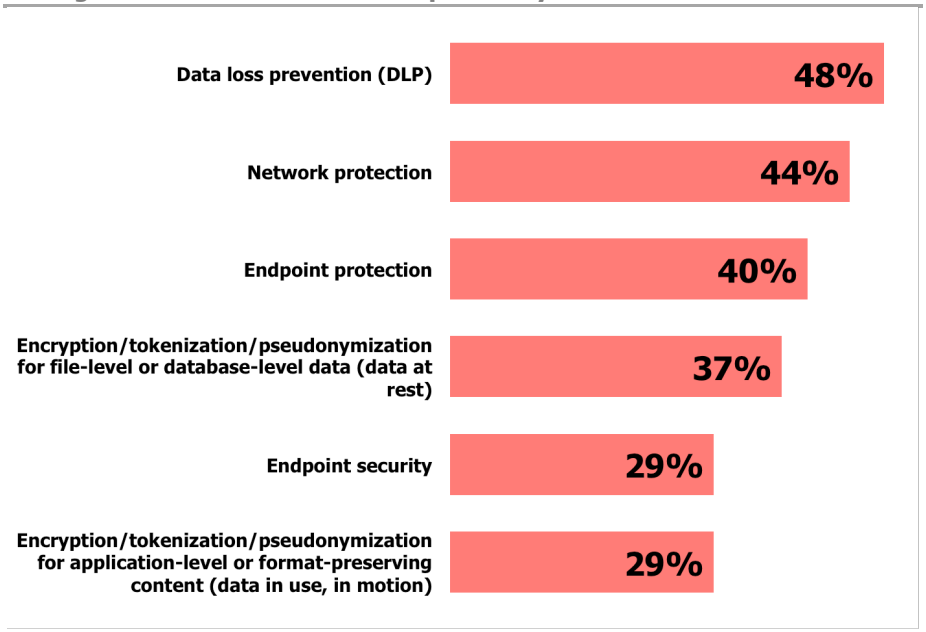
New state of the art approaches currently coming to market include behavior analytics, privileged access management and format-preserving encryption.

In evaluating compliance with the GDPR, organizations should investigate the applicability of these current state of the art offerings.

IDENTITY AND ACCESS MANAGEMENT

Organizations with a myriad of application-specific usernames and passwords for each employee will find it more difficult to map and control access management rights and privileges, and by implication much more difficult to identify non-standard or questionable behavior. A cohesive identity and access management system that seamlessly unifies employee identity across applications is a foundational requirement for GDPR compliance.

Figure 2
Data Protection Technologies That Organizations Will Spend More On During the Next 12-18 Months to Specifically Address the GDPR



Source: Osterman Research, Inc.

The [GDPR] applies to every organization anywhere in the world that controls or processes personal data of EU residents.

CONCLUSION AND SUMMARY

The GDPR – the EU's newly introduced legal framework for the protection of personal data – is now in place, and will be enforced from May 25, 2018. Organizations have less than 18 months (from the publication date of this white paper) to ensure they have appropriate organizational and technological measures in place to ensure compliance. The cost of non-compliance is extremely high in both financial and non-financial terms, making the option of doing nothing in response to GDPR invalid. A few concluding statements and implications follow.

GDPR: "GENERAL" OR "GLOBAL"?

While the word "General" appears in the title of the GDPR – signifying a newly harmonized and unified approach to data protection to be applied across Europe – the "G" could equally stand for "Global." The Regulation applies to every organization anywhere in the world that controls or processes personal data of EU residents, and the financial penalties regime for organizations found in non-compliance is based on total worldwide revenue, not only on revenue earned within EU member states.

THREE IMPLICATIONS

In summarizing this white paper, there are three implications of the GDPR that decision makers must consider:

- **Re-examine your data strategy**
  The implications of the GDPR for organizations can be summarized simply: every affected organization needs to immediately undertake a significant re-examination of its organizational data strategy related to personal and sensitive personal data. Specific requirements in the GDPR need to be planned for, and organizational and technological approaches implemented to resolve problems, strengthen policy and protections, and mitigate against the worst outcomes. In accordance with the general principle of Article 25 of the GDPR, data protection must be "by design and by default." Failure to adequately prepare will push firms

into a compliance quagmire once May 2018 arrives.

- **Non-EU firms have to play rapid catch-up**
  The second major implication of the GDPR is for those organizations that were not subject to the earlier EU data protection directive by virtue of not being based in one of the member states. The new, level playing field introduced by the GDPR applies to all firms everywhere if they control or process personal data on EU residents. Organizations previously subjected to the data protection directive have had a 20-year head start to develop the appropriate organizational and technological approaches to operating successfully in Europe. The GDPR calls for new capabilities for these firms, but the foundation is already in place. For organizations newly impacted by the GDPR, there is a lot of catch-up required.

- **Organizational + technological responses**
  Third, although we have focused mainly on technological responses to the GDPR in this white paper, technology alone is insufficient to comply with its mandates. By all means, every organization should embrace the best technology on offer, but this has to be done as one coordinated element of a wider organizational response. Achieving GDPR compliance is not something the IT department can do alone. Compliance will require a set of coordinated and appropriate responses from the organization as a whole, with strategy, policy, training, and governance processes needed based on expertise from various groups, including Executive Management, Legal, Human Resources, Training, and the IT Department. And finally, since the sanctions regime could threaten the very existence of a firm, Board level visibility will be essential.

SPONSOR OF THIS WHITE PAPER

Smarsh helps financial services organizations get ahead – and stay ahead – of the risk within their electronic communications. Smarsh has established the industry standard for the efficient review and production of content from the diverse range of channels that organizations now use to communicate. With innovative capture, archiving and monitoring solutions that extend across the industry's widest breadth of channels, customers can leverage the productivity benefits of email, social media, mobile/text messaging, instant messaging/collaboration, websites and voice while efficiently strengthening their compliance and e-discovery initiatives.

A global client base, including the top 10 banks in the United States and the largest banks in Europe, Canada and Asia, manages billions of conversations each month with the Smarsh Connected Suite. The company is headquartered in Portland, Ore. with nine offices worldwide, including locations in Silicon Valley, New York, London and Bangalore, India. For more information, visit www.smarsh.com.

www.smarsh.com
@smarshinc
+1 866 762 7741
+1 503 946 5980