WHITE PAPER

The Procrastinator's Guide to Preparing for the GDPR

An Osterman Research White Paper
Published February 2018

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

EXECUTIVE SUMMARY

- **The new European Union (EU)-wide General Data Protection Regulation (GDPR) was signed into law in late April 2016, and comes into effect on May 25, 2018. As of the publication of this paper, that now leaves less than four months to finalize preparations before the GDPR becomes effective.**

- **However, even though the requirement for GDPR compliance commences in May 2018, compliance will be an ongoing effort that will continue indefinitely after May 2018.**

- **The GDPR continues the data protections afforded under the previous Data Protection Directive of 1995, but strengthens the rights of data subjects, harmonizes the approach to data protection across the European Union, and introduces new responsibilities for data controllers and data processors.**

- **GDPR may impose major penalties for organizations that violate the rights of EU data subjects: €20 million or four percent of total global turnover for a list of serious offenses, and €10 million or two percent of total global turnover for less serious ones. Both fine tiers are levied based on whichever is higher.**

- **Despite the GDPR being adopted by the European Council and the European Parliament in April 2016, few organizations are fully prepared for its provisions. Only five percent of the organizations surveyed for this white paper believe they will be "completely ready" for compliance with the GDPR by May 25, 2018.**

- **One of the more significant changes in GDPR is its global applicability. Whereas the earlier directive applied to organizations based on geographical location in one or more EU Member States, the new Regulation applies to any organization – regardless of geographical location – that controls or processes data on EU data subjects.**

- **Complying with the GDPR requires both organizational and technical measures. Organizational measures include documenting data processes that contain personal data, risk assessments, and the appointment of a data protection officer. Technical measures include the appropriate use of tools for classifying personal data, identifying and blocking data breaches, and encrypting or pseudonymizing personal data.**

- **Every communication and collaboration technology and practice will be impacted by the GDPR, including email, storage, managed file transfer, encryption, security, archiving, closed-circuit television, printer solutions, scanning solutions, media, fax processes, photos, paper-based processes, etc. Organizations will need to carefully evaluate each of their current solutions and vendors to ensure that they will be compliant with the GDPR.**

[The GDPR] applies to any organization – regardless of geographical location – that controls or processes data on EU data subjects.

ABOUT THIS WHITE PAPER

This white paper was sponsored by MessageSolution; information about the company is provided at the end of this paper.

WHAT IS THE GDPR AND WHAT ARE ITS IMPLICATIONS?

EXACTLY WHAT IS THE GDPR?

The General Data Protection Regulation (GDPR) is the very-soon-to-be-enforced new data protection law for all 28 Member States in the European Union. While it builds on and extends the principles in the earlier 1995 directive on data protection (Directive 95/46/EC), unlike the directive it applies Europe-wide as a unified regulation. That is, the directive had first to be introduced into each of the member states by national law and thus enabled various nuances in data protection law depending on the member state, but the regulation harmonizes the law across all of Europe to create a unified approach, simplifying the regulatory environment for all organizations doing business with European citizens. While there are a few areas where national law can change the regulation giving a member-state specific interpretation, these are few and far between.
The GDPR:

- Changes the answer to the question of "who owns my personal data?", giving ownership to the individual data subject and not the organization. He or she may give an organization the right to store and use their personal data and sensitive data, but if consent is the legal basis for processing, the data subject has the right to revoke their consent at any time. Organizations need to be explicitly clear what legal basis is relied on for storing and using personal data, and transparency with data subjects regardless of the legal basis.

- Applies not only within the European Union, but extraterritorially. Any organization that controls or processes data on living people in the European Union must comply with the data protection provisions of the GDPR, even if the organization does not have a physical presence in any European Union member state. Such personal data can be related to offering goods and services to data subjects in the European Union, or monitoring the behavior of people that happens within the EU for the purposes of profiling, analyzing and/or predicting preferences, behaviors, and attitudes. Organizations that control what personal data is captured and used are definitely accountable, but new provisions extend certain accountabilities to any organization processing data on behalf of a data controller.

- Requires notification of a data breach to the relevant Supervisory Authority and every affected data subject directly if the breach is likely to result in a risk to data subjects' rights and freedoms. (Breaches that will not result in such a risk generally need not be reported.) If data is breached without adequate protections being in place – a scenario that is becoming increasingly common across the world – organizations need a robust response and mitigation plan for any data breaches if they are likely to result in a risk to data subjects' rights and freedoms.

- Affects global data processes and data transfers, because personal data cannot be transferred outside of the EU to another country or region that lacks equivalent data protections unless Binding Corporate Rules, Model Contracts or other programs like Privacy Shield are in place. For example, although it is leaving the Union, the United Kingdom is adopting the GDPR into its national laws to ensure the same protections and rights apply within the UK and between the UK and EU member states. Creating a harmonized framework with Europe simplifies compliance for everyone involved.

- Excludes protections for personal data of individuals involved in criminal proceedings. Law enforcement agencies and organizations must comply with the data protection requirements in Directive (EU) 2016/680. We do not deal with this issue here, since it's beyond the focus of this paper.)

After years of development, the GDPR was published in the *EU Official Journal* in early May 2016, and will be enforced from May 25, 2018. This means we are already three-quarters through the two-year transitionary period, and the time is rapidly approaching when the full weight of the GDPR will be available to the regulators.

DRIVERS FOR INTRODUCING THE GDPR

The GDPR was developed and introduced for several reasons. The key drivers were:

- To modernize data protection regulations in Europe for new technological and communication advances such as the Internet, digital marketing, social networks, the Internet of Things, and pervasive data tracking capabilities, and to harmonize regulations across Europe to provide a unified pan-European approach. The earlier directive was introduced before the Internet became a mainstream reality, and was thus increasingly out-of-touch with the data challenges of the current age; we live in a different world compared to 1995, and thus the modernization driver. The harmonization driver flows from a European Commission priority of creating a Digital Single Market in Europe, by tearing down regulatory differences between national markets to create one unified market with common and consistent rules for all. Organizations will no longer have a differing set of data protection regulations to comply with per national market, but rather one unified compliance framework.

- To elevate the importance of good data security and data protection for personal and sensitive personal data. Just as new technologies have created digital markets where data can flow quickly and easily, so new technologies have been created to protect that data. Engaging in the first without paying appropriate attention to the second is unjust to data subjects, and hence GDPR mandates many stronger protections both organizationally and technically to restore the balance.

- To create a level playing field for every organization controlling or processing personal and sensitive data on EU data subjects, rather than allowing non-residence in the EU to provide an exemption from good data protection practices, as could happen under the earlier Directive. Since the digital age has spawned a highly connected world with the ability to sell goods and services easily to people everywhere around the world without a local physical presence, the playing field had to be re-defined in terms of where the data subjects, not organizations, are located.

- To re-center the locus of data protection in a global and interconnected world, putting the emphasis on the personal and sensitive data of people located in Europe regardless of where the organization collecting or processing that data is physically located. This change impacts global legal frameworks by demanding that any organization, region or country that wants to trade within the EU market has equivalent or adequate data protection standards, rights, and obligations. Every organization that controls or processes personal data on EU data subjects will need to assess the requirements of GDPR on its data processes, and multi-national firms with a presence in Europe may find it easier to set the core requirements of the GDPR as its data protection standard and best practice everywhere it does business (although clearly regional variations outside of Europe will still exist).

While perhaps not a driver, the GDPR can be viewed negatively as more regulation to comply with, added red tape, and increased cost, or can viewed positively. On the positive side is the view that earning and retaining the trust of customers starts with being good with the data about them, including their past purchases, their preferences, and their willingness to engage with you going forward. A competence in data protection bodes well for competence in other commercial aspects, and organizations thus positioned will earn greater freedoms and privileges in the future to serve customers than those that cannot get their data protection act together.

The playing field had to be re-defined in terms of where the data subjects, not organ-izations, are located.

HISTORY AND BRIEF OVERVIEW

Over the past century in Europe (and undoubtedly before that too), personal data has been used against European citizens – think of secret police organizations in some countries and their meticulous filing system on the activities of millions of citizens at home and abroad. In creating a new standard for a new Europe, the European Convention on Human Rights (1953) guaranteed a right to privacy in Article 8, for private and family life, and correspondence; this right was based on the earlier Article 12 in the Universal Declaration of Human Rights (1948). The more recent EU Charter of Fundamental Rights (2000) carries forward the rights in the 1953 convention, and includes data protection as a fundamental right too.

The pre-GDPR practical outworking of the data protection ethos in Europe was the 1995 Directive on data protection. This, however, was not a common regulation for all of Europe, but a proposed standard from the European Commission that individual Member States should pay attention to and adopt within their own national laws. This created a complex compliance environment for any organization working across member states, as the very definition of personal data could differ by state, notifications of data breaches had to be made separately to the supervisory authority in each state, and data transfers between states had to be undertaken with special care. GDPR solves the variation with a single regulation for all of Europe, and for any organization that controls or processes data on EU data subjects, regardless of where the organization is based.

WHAT IS PERSONAL DATA?

Article 4 defines personal data as "any information related to an identified or identifiable natural person" (called a data subject more generally in the GDPR text). Direct identifiers include name, ID number, and online identifiers such as an email address, and indirect identifiers include location data and various types of identity. The key test is whether a direct or indirect identifier, alone or in combination with others, can be used to uniquely identify a natural person. Article 9 adds a second layer to the definition of personal data, by separating out "special categories" of personal data, including data that reveal racial or ethnic origin, political opinions, and religious or philosophical beliefs, genetic and biometric data for identifying a person, and data about a natural person's sex life or sexual orientation. All personal data must be protected, and special categories of personal data carry additional prohibitions and constraints.

Why these protections are necessary is addressed in Recital 75. The core concern is that processing of personal data can result in "physical, material or non-material damage," such as discrimination, identity theft or fraud, financial loss, and reputational damage, among others. Processing can also result in data subjects being "deprived of their rights and freedoms," or prevented from "exercising control over their personal data." Recital 75 gives other examples as well of where damage can result from processing of personal data.

GDPR introduces new and expanded rights for data subjects, including the right of access (Article 15), right to erasure under specific circumstances (Article 17, also called the right to be forgotten), and the right to data portability (Article 20). These three articles in combination redefine the question of ownership of personal data, putting that power squarely in the hands of individuals and not the organizations that control or process information about them.

GDPR also introduces new and expanded obligations for organizations that both control and process personal data on the behalf of data subjects, including elevated conditions of consent (Article 7, when consent is used as the legal basis for processing), maintaining records of processing activities (Article 30), and notifications of a data breach to a supervisory authority and data subjects (Articles 33-34), among others. Data processors gain specific responsibilities and direct obligations in the GDPR for several significant matters, whereas in the Directive responsibilities and obligations were focused on the data controllers, who could choose to extend these

indirectly through contractual means to processors. Processors now have direct statutory obligations for data protection.

SIGNIFICANT PENALTIES FOR NON-COMPLIANCE

GDPR has two tiers of administrative fines for non-compliance (Article 83), which can be levied by a supervisory authority based on the type of infringement, rather than on a first, second, and subsequent infraction basis. The fine for lower level infringements is up to €10 million or up to two percent of the total worldwide annual turnover from the preceding financial year, whichever is higher. Infringements at this level include failing to enact data protection by design and by default (Article 25), failing to keep adequate records of processing activities (Article 30), and not ensuring appropriate security of processing (Article 32), among others. The higher level of fines is up to €20 million or four percent of total worldwide annual turnover, whichever is higher, and is for infringements such as failing to comply with the basic principles for processing, including conditions for consent (Article 5-7, and 9), not providing data subjects with their rights (Articles 12-22), and unauthorized or inappropriate transfers outside of the EU (Articles 44-49), among others.
These administrative fines do not prevent a data subject from also seeking financial damages through a civil court against any organization that fails to process their personal data properly, does not ensure their rights are met, and fails to ensure adequate organizational and technical safeguards are in place to protect their personal data.

It is important to note, however, that there are also non-financial penalties that can create significant problems for an organization that violates the provisions of the GDPR. For example:

- The GDPR's supervisory authorities have the power to impose restrictions or even stop a particular process, implement a remediation program, and then require frequent audits going forward.

- Investigation by a supervisory authority will cause significant disruption in an organization, creating further financial impact, loss of confidence from customers, stakeholders and employees, and it may also impact shareholders support and the share price for a public company. Moreover, there is the added risk of the auditor finding "other" issues that may require further investigation and remediation.

There are also non-financial penalties that can create significant problems for an organization that violates the provisions of the GDPR.

PENALTIES FOR DATA BREACHES: FIVE EXAMPLES

Failing to have sufficient organizational and technical controls in place to prevent a data breach falls under the lower level of infringement in GDPR; Articles 33 and 34 on data breaches are covered by Article 83(4)(a). Here's the administrative fine these organizations would face if they were subject to GDPR, at two percent of total worldwide annual turnover from the financial year preceding the data breach:

- A large British retail bank was hacked in late 2016, with millions of pounds stolen from thousands of bank accounts as a result, a clear and costly breach of personal data. If subject to GDPR, its breach could incur a fine of up to £901.2 million (€961.5 million), based on 2015 total revenue of £45 billion.[i]

- A large provider of international medical insurance discovered a data breach affecting 108,000 of its current and former customers, due to an employee copying data they should not have. The data included names, date of birth, and contact information, along with nationality (one of the special categories of personal data). If the two percent maximum fine were levied against the whole group, its fine on £11.05 billion annual revenue in 2016 would be £221 million (€235 million).[ii]

- A leading ride-sharing service, whose torrid year has been rocked by scandal and the disclosure of a cover-up of a massive data breach, would be subject to GDPR

since it is operational in the European market. Assuming the two percent maximum fine was applied, the company would face a US$400 million fine (€318.6 million) on US$20 billion of revenue for its 2016 data breach of personal data on 57 million customers that was disclosed only in 2017.[iii]

- A leading web services provider has suffered multiple data breaches in recent years. Its 2013 data breach of one billion accounts included personal data, and on 2012 annual revenue of US$4.9 billion, a two percent fine would be US$99.7 million (€79.4 million). Its 2014 data breach would result in a €74.5 million fine. The interesting question is what would happen in 2017 given that the company recently acknowledged that all of its user accounts were breached in 2013, not "only" one billion as originally supposed.[iv, v]

- A large American credit rating organization's 2017 breach of personal data on 143 million American citizens would attract a maximum fine of US$62.9 million (€50.1 million), based on operating revenue of US$3.145 billion for fiscal year 2016.[vi]

None of these administrative fines would be likely to cause the company in question to go out of business, but it would swiftly spotlight the need to avoid a similar occurrence in the future through the introduction of better organizational and technical controls.

OBLIGATIONS FOR ORGANIZATIONS THAT CONTROL OR PROCESS DATA

The GDPR specifies the responsibilities and obligations held by data controllers and data processors. In this section we briefly review some of these requirements, although this treatment is illustrative and not exhaustive.

DATA MUST BE WELL MANAGED

Sloppy data management practices will prove costly under GDPR. A much higher standard for data management is now required for all organizations controlling or processing personal data on data subjects in the EU. This includes:

- **Being Very Clear on the Legal Basis for Processing Personal Data**
  Data can be processed (which includes just about any action performed on data, including storage) only if there is a legal basis for doing so (Article 6). These include direct consent from the data subject, necessity for performing a contract with the data subject (or getting ready to do so, on request from the data subject), complying with a legal obligation, to protect the vital interests of the data subject or another natural person, and in line with the legitimate interests of the controller or a third party. Clarity on the legal basis for each collection and processing is essential because of flow-on implications and linked requirements. For example, if the data subject requests erasure at some point in the future, this must be complied with unless the legal basis for the original collection and processing overrides the erasure request. Similarly, any additional processing beyond the original purposes requires a contextual balancing of interests between the data subject and data controller.

- **Maintaining Good Records of Data Processing Activities**
  Both data controllers and data processors are required to maintain a record of processing activities under its responsibility (Article 30). Think of this as a data governance blueprint for all data processes that touch personal data. Required information for data controllers include the name and contact details of the controller (and representative and data protection officer), the purpose of the processing, the categories of data subjects and personal data, the categories of recipients who will see the results of the processing, the time limits for erasure of the different categories of data, and a general description of the technical and

organizational measures for protecting personal data. Data processors have a similar but slightly shorter list of requirements. Records must be maintained in written form (electronic is fine), and these records must be made available to the supervisory authority on request. Organizations with fewer than 250 employees are generally excluded from these record-keeping requirements, but there are specific instances where this exclusion does not apply, such as processing special categories of data.

- **Responding to Data Subject Access Requests Appropriately and Promptly**
  Data subjects have the right under Article 15 to ask any data controller for confirmation whether personal data concerning him or her are being processed. If data is being processed, they must be given access to their data plus contextual information such as the purposes of processing, the categories of personal data being processed, the recipients or categories of recipients who have access (especially recipients in third countries or international organizations), the time period of storage, where the data came from if not from the data subject, and the presence of any automated decision making. They must also be notified of their rights of rectification, erasure, restriction of processing, and complaint to a supervisory authority. This must be provided free of charge, and promptly – which Article 12(3) sets as a maximum of one month under normal conditions (under the current Data Protection Act the requirement is 40 days, and so existing processes must now change to meet the new requirements). Recital 63 states data subjects must be able to request access "easily and at reasonable intervals," although a fee may be levied for second and subsequent access requests. Access requests will quickly overwhelm any organization lacking very good data management practices. The ability to effectively see all instances of personal data regarding an individual and know the lineage of each instance will be essential, not only for the ability to fulfill the access requirements of Article 15, but also the flow-on rights of rectification, erasure, and limitation of processing. GDPR attempts to prevent an abuse of the subject access request right by virtue of a fee mechanism for second and subsequent requests from the same data subject, but any organization suddenly facing 1,000 first time access requests will need robust response mechanisms ready to go.

Data protection must be "by design and by default".

- **Approaching Data Protection by Design and by Default**
  In what will create significant challenges for organizations with legacy data systems and legacy data archives, data protection must be "by design and by default" (Article 25). This requirement is in service of the overriding principle of minimizing damage to the rights and freedoms of data subjects, and includes the mandate for both organizational and technical measures. Pseudonymization – one method of obfuscating personal data values – is specifically mentioned, as is the principle of data minimization so that personal data unnecessary to a processing isn't even collected in the first place. The analysis of these measures is to be undertaken when the data processing method is initially designed, and when the processing actually takes place. Other organizational measures include data protection impact assessments (DPIA) (Article 35), appointing a data protection officer (Articles 37-39), and the ability to demonstrate compliance with the core principles of processing personal data (Article 5), among others. Data protection is not just a point-in-time requirement; it is a continual mandate.

  Organizations should carry out a risk assessment of all processes that may process personal data and, if deemed high risk, a DPIA must be conducted every six months, since a DPIA is a per-process evaluation. New processes or changes to existing processes are then evaluated using a DPIA. Unless a formal risk assessment is carried out, it is difficult or impossible for decision makers to know for which processes a DPIA must be carried out. Moreover, without a risk assessment, it is difficult or impossible to know if all processes are captured, documented and understood.

- **Reporting Data Breaches within 72 Hours of Awareness**
  A data controller must notify the supervisory authority of a personal data breach within 72 hours of becoming aware of the breach, and data processors must notify the data controller of a personal data breach "without undue delay" after becoming aware of the breach (Article 33). Data controllers are also required to advise data subjects "without undue delay" if a breach is likely to result in a high risk to the rights and freedoms of natural persons (Article 34). Neither notification is necessary if there is no risk to the rights and freedoms of natural persons, such as when the data was encrypted and unreadable by unauthorized people. Common examples of breaches include loss of unencrypted computers and devices, insecure disposal of information, and malicious actors accessing a database and encrypting it for a ransom. Detecting breaches requires having a very good handle on where personal data exists, and the state of data protection in real-time.

Managing data well is not "an IT job," but one that has implications for the entire organization.

DATA SUBJECTS OWN THEIR PERSONAL DATA

Data subjects, not data controllers or processors, are the owners of their personal data. The GDPR gives data subjects ownership by virtue of the following rights, although note that specific requirements and exclusions apply for each right:

- The right of access (Article 15), as we have discussed above.

- The right to rectification (Article 16), for rectifying incomplete or inaccurate data about a data subject. A data subject has the option of supplying additional information to facilitate this process.

- The right to erasure (Article 17), so a data controller must erase a data subject's personal data on request. For example, if the data subject withdraws their consent for processing, and consent is the only legal basis for the processing, the data controller must remove all instances and copies of the personal data from its systems.

- The right to restriction of processing (Article 18), when the data subject contests the accuracy of their personal data, when the processing is unlawful, or when the controller no longer requires the personal data but the data subject does not want it erased for use in legal claims.

- Data controllers have the responsibility to notify each recipient with copies of personal data when handling a data subject's request to rectify, erase, or restrict the processing of his or her data (Article 19), unless this is impossible or too difficult.

- The right to data portability (Article 20), whereby a data controller must supply a data subject with their personal data, on the condition that they provided it to the controller. This must be delivered in a "structured, commonly used and machine-readable format," and be able to be transferred to another data controller. The data subject can even request the data controller to transmit their data directly to another data controller.

- The right to object to the processing of their personal data in line with specific legal bases, namely the performance of a task carried out in the public interest, in exercising official authority, or necessary for the legitimate interests of the controller or a third party (Article 21). Before the data controller can resume processing of the personal data, they must demonstrate that they have the grounds to continue doing so. This right to object also applies to processing for direct marketing purposes, which the data controller cannot override.

- The right to not be subject to a decision that is based solely on automated processing, including profiling, where that decision creates legal or similarly significant effects for him or her (Article 22). There are some situations where this right is not available, but if these exclusions are used, the data controller must at least offer the ability for human intervention, allow the data subject to express his or her view, and offer the ability to contest the decision.

- Finally, data subjects also have the right to learn if their personal data was breached and is likely to cause them harm (Article 34), although this is not stated as a "right" of the data subject as such, but rather a communication responsibility of the data controller. The effect, however, is the same.

PROVIDING CONSENT IS IMPORTANT

Consent by the data subject is listed as the first of six possible legal bases for processing personal data (Article 6). Article 4(11) defines consent as "any freely given, specific, informed and unambiguous indication of the data subjects' wishes ... by a statement or by a clear affirmative action, [that] signifies agreement to the processing of personal data relating to him or her." Requiring a statement or clear affirmative action by the data subject means that consent cannot be implicit, opt-out, or the result of pre-ticked boxes.

If consent is used for collecting and processing personal data, there are specific requirements the data controller must meet. These include (but are not limited to):

- The ability to prove that the data subject has given consent (Article 7(1)). This requires that you maintain good records on how and where consent was gained.

- The request for consent, if provided as one part of a written document, must be "clearly distinguishable from the other matters" in the document and easy for the data subject to read and understand (Article 7(2)). Consent not gained in this way is invalid.

- The ability for a data subject to withdraw his or her consent at any time, using a process that must be as easy as giving consent (Article 7(3)). Withdrawing consent does not invalidate the lawfulness of any earlier processings that took place while the consent was in place.

- Being very careful to ensure that only the personal data required for performing a contract or providing a service is requested from the data subject where consent is used as the legal basis, otherwise consent could be judged as not freely given (Article 7(4)).

- For children under the age of 16, consent for information society services must be given or authorized by whomever holds parental responsibility for the child (Article 8(1)). Note that Member States have the right to set this age to either 13, 14 or 15 years, one of the few areas where GDPR can vary by state.

Transparency will be an essential element of the GDPR in the context of gaining the consent of data subjects.

It is worth noting that transparency will be an essential element of the GDPR in the context of gaining the consent of data subjects. Privacy notices are a key factor in providing all of the relevant information to the data subject prior to collecting and processing their data, allowing them to make an informed decision and commitment on sharing their information.

Be aware that once the GDPR comes into force in May 2018, these elevated conditions of consent will also apply to any processing of personal data collected prior to the GDPR that will rely on consent as the legal basis. If your pre-GDPR consent process lacked the robustness of the new GDPR-mandated approach, you may need to update the consent you currently hold. However, even requesting an update may itself be illegal – two firms were fined a total of £96,000 ($135,000) for their attempts to become compliant with the GDPR[vii].

DATA CONTROLLERS AND DATA PROCESSORS MUST MAINTAIN DATA SUBJECTS' PRIVACY

Data controllers and data processors hold responsibilities to ensure the rights and freedoms of data subjects are maintained and their privacy respected. Specific responsibilities include:

- Avoiding the processing of special categories of personal data – for determining racial or ethnic origin, understanding political opinions, religious or philosophical beliefs, determining trade union membership, uniquely identifying a natural person through genetic or biometric data, health data, or data about a person's sex life or sexual orientation – unless one of ten exclusions apply to the general prohibition (Article 9). Exclusions include explicit consent, ensuring rights of employees, protecting vital interests, and when the data in question has clearly been made public by the data subject, among others. If any of these special categories of personal data will be processed, a data protection impact assessment is likely to be required (Article 35), the supervisory authority may need to be consulted in advance (Article 36), and the data protection officer for the organization should be explicitly involved (Articles 37-39). In short, the processing of special categories of personal data is prohibited unless an exclusion is used.

- Appointing a data protection officer who has expert knowledge in the field of data protection in order to inform and advise the data controller or processor about their data protection obligations (Articles 37-39). He or she is to be involved in all issues relevant to protecting personal data, be available to data subjects for the exercise of their rights, and be accessible to the supervisory authority as a liaison for the organization. Specific tasks include informing and advising the organization and employees involved in processing of their responsibilities under GDPR, monitoring compliance, providing advice on data protection impact assessments, and cooperating with the supervisory authority (Article 39). The data protection officer must have the freedom to carry out his or her responsibilities without interference, and is to report to the highest management level of the controller or processor (Article 38). He or she must not be dismissed or penalized by the controller or processor for carrying out the required tasks.

- Working jointly and transparently where two or more data controllers are determining the purposes and means of processing. This includes being very clear about which responsibilities each holds under GDPR (Article 26). Data subjects can be informed of any arrangements, but data subjects retain full rights against each controller separately.

- Ensuring that any data processor used by a data controller is compliant with the GDPR (Article 28), and that appropriate technical and organizational measures are implemented by the processor to ensure data protection. Data processors now have direct specific obligations under GDPR, but data controllers cannot avoid liability for their processings if things go awry. A contractual agreement between the data controller and processor must be put in place.

- Protecting personal data using appropriate organizational and technical measures, informed by a risk assessment to the processing of that personal data. Pseudonymization and encryption are two of the explicitly mentioned approaches that offer strong – but not failsafe – data protection methods. These approaches are recommended but not required, along with other measures such as processing system confidentiality, integrity and resilience, and a regular program of testing the designated security measures (Article 32).

DATA CONTROLLERS AND PROCESSORS OUTSIDE THE EU MUST HAVE A REPRESENTATIVE IN THE EU

Every data controller and data processor that is not established in the EU must appoint a representative based in one of the Member States in which relevant data subjects are located (Article 27). This applies when processing activities relate to offering goods or services to data subjects in the EU, or monitoring of data subjects' behavior that takes place within the EU (Article 3(2)). The representative must be designated in writing, and be available for communication and interaction with supervisory authorities and data subjects on issues related to processing in light of the compliance mandates of the GDPR. This role of representation is not the same as a data protection officer; the representative must be based in the European Union, while a data protection officer is best located close to the operations of the data controller. Article 27 lists two exclusions to the need to appoint a representative based in the EU.

THE CURRENT STATE OF READINESS FOR GDPR COMPLIANCE

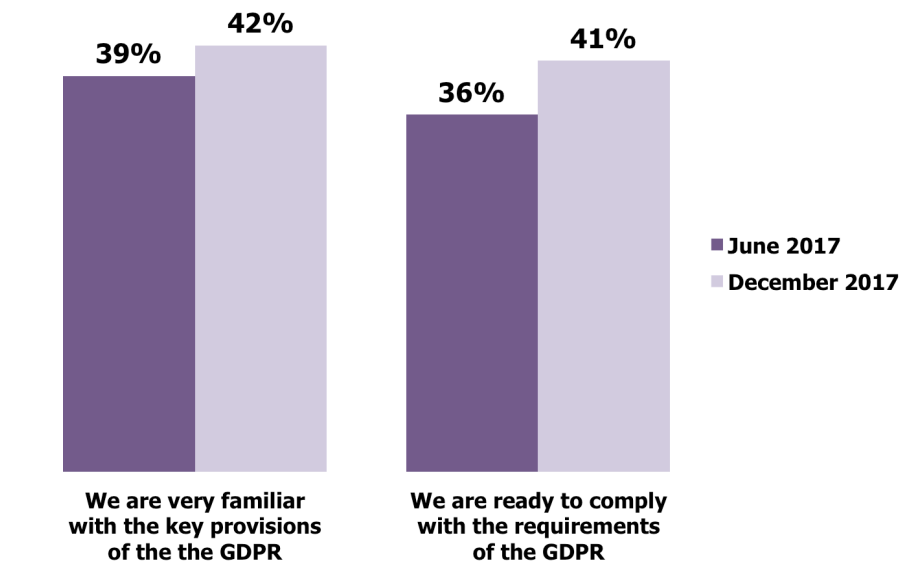
ORGANIZATIONS ARE BECOMING MORE GDPR-READY

Are organizations ready to comply with the GDPR? The surveys conducted for this white paper found that most are not, as shown in Figure 1. Our most recent survey found that roughly two in five decision makers believe they are very familiar with the key provisions of the GDPR and that their organizations are ready to comply with the regulation.

The good news is that things are improving – a bit. A survey that Osterman Research conducted in June 2017 found that strong familiarity and readiness for compliance were 39 percent and 36 percent, respectively. There clearly has been improvement during the last half of 2017, but not much.

Are organizations ready to comply with the GDPR? The good news is that things are improving – a bit.

Figure 1
Familiarity and Readiness With the GDPR
Percentage of Decision Makers Responding "Agree" or "Completely Agree"

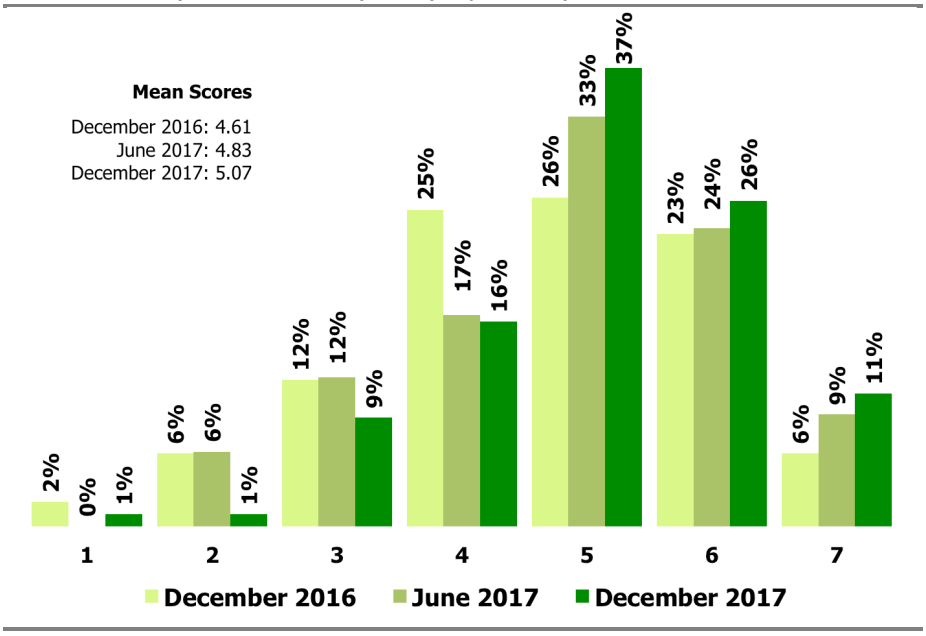


Source: Osterman Research, Inc.

PROCESS MATURITY IS IMPROVING

In the context of improvements to the organizational and technical approaches for data protection that will be required for compliance with the GDPR, things are improving here, as well. As shown in Figure 2, the Osterman Research survey results from December 2016, June 2017 and December 2017 show that organizations' organizational and technical approaches for GDPR compliance are becoming more mature. To be sure, significant improvements are still needed, but the direction of change is positive.

Figure 2
Maturity of Organizational and Technical Approaches to Data Protection
On a scale of 1 (not mature at all) to 7 (very mature)

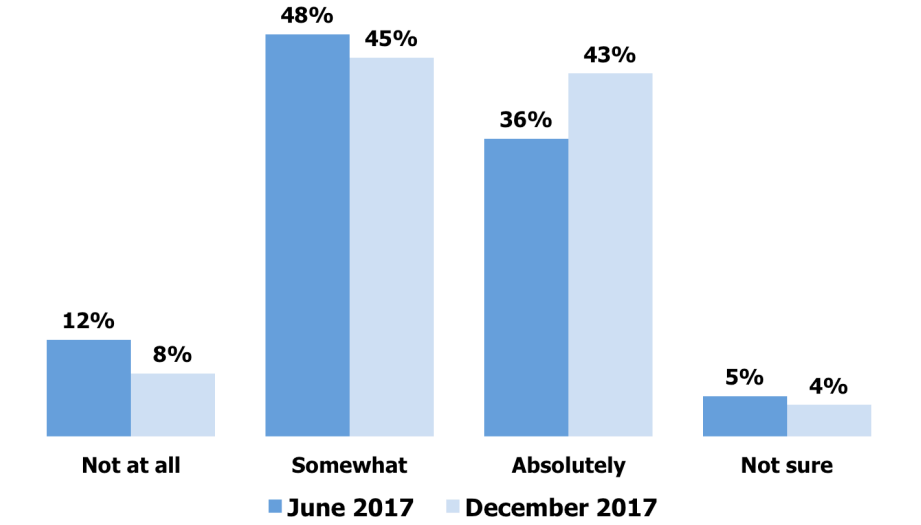


Source: Osterman Research, Inc.

ATTITUDES TOWARD THE GDPR ARE ALSO IMPROVING

Attitudes toward the GDPR are also improving. Figure 3 shows that a growing proportion of decision makers consider that the GDPR will be an opportunity to help improve their security and governance practices. For example, those who believe that the GDPR will in no way help improve security and governance has dropped from 12 percent of respondents in June 2017 to eight percent in December 2017. At the same time, those who completely agree that the GDPR will have this impact have grown from 36 percent to 43 percent.

Figure 3
Is the GDPR an Opportunity for Better Security and Governance?



Source: Osterman Research, Inc.

SOLUTIONS YOU NEED TO IMPLEMENT AND WHY THEY ARE IMPORTANT IN THE CONTEXT OF THE GDPR

GDPR requires that each data controller and processor "implement appropriate technical and organizational measures" to ensure data protection of personal data. These should be done in light of an assessment of the risks to rights and freedoms of natural persons based on the personal data processed. Here is a list of technical measures that you are highly likely to require in your journey of protecting personal data and achieving GDPR compliance:

- **Archiving and backup**
  Archiving tools offload outdated and less frequently used data into secondary systems, reducing the volume of current data in production systems, while still providing a mechanism for authorized individuals to access the relevant data in the context of their day-to-day work. Archiving systems must still be compliant with GDPR, however, including the ability to discover personal data on a data subject under an access request, rectify any data that is incorrect, and erase data under a right to be forgotten request if the conditions for erasure are met.

  Organizations must continue to follow best practices for backup, but the GDPR potentially increases risk depending on how backups are taken. An integrated archive and backup strategy is essential to ensure that only a single instance of data is stored for both. Moreover, cloud-based archiving and backup solutions may offer some advantages here because of their speed of implementation, a particularly important consideration given that the GDPR will implemented soon.

- **Data Classification**
  Mission-critical sanctioned corporate systems that hold personal data in structured formats are much easier to understand in terms of data protection than the mass of unstructured data and unsanctioned applications in use. Data classification tools offer an automated method for analyzing all data stores and sources in the organization, to identify personal data and classify what is discovered. This extends into the usually difficult-to-find data locations like copies, exports, backups, and shadow IT cloud services that employees are

Many current [file transfer] solutions provide inadequate security and other controls and will not be compliant with the GDPR.

using. Data classification tools map what personal data is actually in place across the organization, so that appropriate mitigations can be developed (e.g., protect in place, migrate, delete). Another important consideration is the selection and use of review tools that will help decision makers to sift quickly through large volumes of information.

- **Managed File Transfer Solutions**
  File transfer solutions of various types, from consumer-focused tools to high-level managed file transfer solutions, are commonly used to send and receive information, including personal data. Many current of these solutions provide inadequate security and other controls and will not be compliant with the GDPR. At a minimum, any file transfer solution should:

  - Integrate with identity management solutions
  - Maintain tight user controls
  - Integrate with DLP solutions
  - Encrypt data when it is being transferred and when at rest
  - Enable non-repudiation of data
  - Enable scheduled deletion of data
  - Ensure that data transferred outside the EU fall under an appropriate transfer exception

- **Data Loss Prevention (DLP)**
  DLP tools analyze flows of data in email and other systems to identify the presence of personal data using pattern-matching and other advanced forms of identification and classification. If personal data is identified and appropriate protections are not in place – for example, a spreadsheet attached to an email containing customer names and email addresses that is not encrypted – either the spreadsheet can be automatically encrypted or the message can be blocked or quarantined. DLP tools help prevent the most common and frequent type of data breaches: employees sending data that should be protected in an unprotected form or to people who are not authorized to receive it.

- **Encryption**
  Encrypting personal data adds a strong level of data protection, by using a mathematical code to scramble alphanumeric characters into an unintelligible string that lacks any meaning and cannot be deciphered without the decryption key. Encryption is explicitly mentioned as a data protection safeguard in the GDPR, because most data breaches can be prevented if encryption is used. For example, if a data breach does happen, a controller is excused from the notification requirements if the risks to personal data are low, which would usually be the case if the data was encrypted when breached.

- **Identity Access and Management**
  Personal data is not protected if any employee can access it. Identity access and management tools introduce an identity system so that employees can be uniquely identified, and thus their access to corporate systems – and personal data – be carefully managed. A strong identity and access management system is essential all the time, but is extremely beneficially for preventing access to corporate systems and personal data when off-boarding an employee out of the organization entirely, or when an employee moves to a new role in the organization with a different set of access rights.

- **Pseudonymization**
  Like encryption, pseudonymization obfuscates personal data values by rendering them unintelligible to anyone without access rights. Unlike encryption, pseudonymization achieves this by replacing personal data values with a code that can be used to look up the original values that are stored separately in a secured database. Pseudonymization is also explicitly mentioned in the GDPR, although the approach is not without its own risks, such as the unauthorized reversal of the pseudonymized data. However, in production systems, test and

development environments, and data archives, pseudonymization offers one recommended way of protecting personal data.

- **Security Tools**
  Security tools analyze the integrity of network resources, endpoint devices, and cloud services to identify unauthorized access attempts, unwanted types of data including malicious threats, and the presence of unauthorized and questionable applications when access to a network or data resource are requested. These capabilities work in combination to reduce the likelihood of data breaches due to nefarious applications working quietly in the background to exfiltrate data, and can provide rapid awareness of an active breach attempt. Security tools can also identify out-of-date and unpatched operating systems and applications that are vulnerable to malicious threats.

  Tools to thwart phishing, ransomware, other types of malware and impersonation in email are critical to prevent malicious code from undermining the integrity, availability and resilience of data systems. Advanced capabilities are essential and must go beyond simple spam and virus filtering.

- **Ensuring Safe Cross-Border Transfers**
  It is also essential that organizations implement appropriate safeguards when transferring data to nations outside of the EU. The GDPR allows such data transfers under three conditions:

  - If the European Commission has determined that the level of personal data protection in the country to which information will be sent meets an acceptable standard.

  - If binding corporate rules (discussed in Article 49) or contractual agreements are used to govern the management of the data sent outside of the EU. Moreover, Article 42 allows that "data protection certification mechanisms, seals or marks" may be approved for a maximum of three years "for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation".

  - If an exemption is granted in the event that none of the conditions above can be satisfied (discussed in Article 49).

  Unfortunately, the validity of each of these mechanisms – including the Privacy Shield program which enables many organizations to transfer data to the United States – are under a legal challenge and have the potential to be invalidated. Organizations should consider alternative measures to enable compliance if these mechanism are invalidated, which may include creating or expanding their data center capabilities within the EU.

- **Application Security Testing**
  Data protection must be "by design and by default," and application security testing tools help deliver this mandate by analyzing applications for vulnerabilities. Once identified and catalogued, software developers can rectify or mitigate the weaknesses before damage can be done. Penetration testing, for example, offers a process for analyzing application and system security, in order to elevate the overall security posture of the system.

- **Data Portability Capabilities**
  Data subjects have the right of data portability, where a data controller must supply the personal data the subject has provided in an appropriate format for transfer to another data controller. Tools that enable the export of data provided by data subjects that meet the right conditions will be essential.

- **User Awareness Training**
  Employee training is an organizational measure that has high overlap with the

Employee training is an organizational measure that has high overlap with the technical measures of protecting data.

technical measures of protecting data. Employees should be trained on the requirements of the GDPR, their responsibilities to protect personal data, the risks of unsanctioned tools and applications, and the risky actions they should avoid in order to not fall foul of the data protection mandates. For example, sending a spreadsheet containing an export of personal data from corporate systems to their personal email address is a risky and dangerous proposition, the consequences of which should be explained. Likewise for departing employees, copying data on customers to take to their new place of employment is a breach of GDPR, and should not be done.

- **Other Technologies**
  The above is a list of high-priority technical measures that help with GDPR compliance. Complementary technical measures include:

  - Incident response systems, for quickly being able to contain and respond to a security or data protection incident. We also recommend use of APIs to consolidate logs and forensics from key security systems to help identify, investigate and more quickly remediate threats.

  - The use of data redaction solutions that enable private or sensitive information to be blocked from access when data is transferred to third parties or even when it is stored by a data controller or processor.

  - Mobile device management tools, to remotely wipe or kill a compromised or lost device in order to prevent a breach of data. Such tools also provide a real-time dashboard on the data protection health of the device fleet, and enforce local settings such as encryption and the use of endpoint security software.

  - Behavior analytics to provide early warning of developing patterns that show weird or unsanctioned behavior by employees, that could give early warning signals of a data breach, for example. Such tools can also highlight impossible valid situations, like an employee being logged into two devices simultaneously on opposite sides of the world (this would signal account credential compromise).

  - Privileged account management analysis tools to ensure that only valid actions are undertaken by authorized IT administrators. Privileged accounts often have higher access rights to data systems containing personal data, and are a key attack vector for hackers and other actors with malicious intent.

  - Process mapping tools, to document how processes with personal data work, where the data resides, who interacts with it, and how it is shared.

TECHNOLOGY CHANGES WROUGHT BY THE GDPR

The surveys conducted for this white paper found that, from a technology perspective, the chief beneficiaries of the GDPR will be cloud vendors and technology vendors based in the EU, as shown in Figure 4.

Figure 4
Changes in Use of Various Elements as a Result of the GDPR

	It Will Increase	It Will Decrease	No Change	Don't Know
On-premises technology	28%	20%	47%	5%
Cloud technology	50%	5%	39%	6%
Non-European technology vendors	8%	8%	71%	13%
European technology vendors	23%	8%	59%	10%

Source: Osterman Research, Inc.

In closing, while the above technical measures offer capabilities to greatly enhance the protection of personal data, developing proficiency in their effective use is critical. Proficiency includes developing people across the organization with the knowledge, skills, experience, and aptitude to use the various technical measures deployed, in conjunction with smart organizational measures, to actually protect personal data and safeguard the rights and freedoms of natural persons. Ongoing data protection impact assessments, data protection certifications, and independent audits will enable the perpetual evaluation of compliance with GDPR.

SUMMARY AND CONCLUSIONS

The GDPR is a far-reaching and standard-setting piece of regulation on protecting personal data. Any organization impacted by its mandates needs to take rapid action to ensure they are appropriately ready by May 2018. Equally, however, is the realization that compliance is not a one-time event nor a journey with an easy destination. It is an ongoing process of learning, analysis, mitigation, and improvement.

However, many organizations are not yet ready for the GDPR starting gun in May 2018 and many need to expend significant resources to become compliant.

Compliance is required, but will bring spillover benefits for customer engagement, competitive positioning, eDiscovery, and regulatory compliance more generally.

SPONSOR OF THIS WHITE PAPER

MessageSolution is a private held profitable company with zero debt, with its 100% R&D resources focusing on innovating and developing world-class enterprise compliance archiving and eDiscovery solutions. MessageSolution's team of dedicated professionals comes from a wide array of companies in Silicon Valley, California, including technology veterans from IBM and Sun Microsystems as well as graduates of Stanford University. With more than 20 years of high tech experiences, the MessageSolution team puts everyone's skills to work creating software to solve IT problems for enterprises in various industries across the world. Managed by a team of highly experienced Silicon Valley veterans, MessageSolution is positioned to lead the rapidly growing enterprise information archiving, compliance management and eDiscovery markets.

MessageSolution is headquartered in Silicon Valley, California, with operations in North America, Europe, and mainland China, along with distribution channels in

MessageSolution™
Enterprise Archiving, eDiscovery, Migration

www.messagesolution.com
@GlobalArchiving
+1 408 383 0100

Europe, South Africa, Australia, and Asia Pacific. We are a growing independent software vendor dedicated to providing innovative email, file systems, SharePoint, and archiving for compliance, electronic discovery, storage management, and mail cross-platform migrations.

REFERENCES

[i] https://www.statista.com/statistics/490931/tesco-group-finance-revenue-united-kingdom-uk/

[ii] https://www.bupa.com/~/media/files/site-specificfiles/our%20performance/pdfs/financial%20results%202016/bupa%20ar2016%20-%20financial%20statements.pdf

[iii] https://www.bloomberg.com/news/articles/2017-04-14/embattled-uber-reports-strong-sales-growth-as-losses-continue

[iv] https://www.statista.com/statistics/266253/yahoos-annual-gaap-revenue/

[v] https://www.theverge.com/2017/10/3/16414306/yahoo-security-data-breach-3-billion-verizon

[vi] https://investor.equifax.com/financial-information/fundamentals

[vii] https://www.theregister.co.uk/2017/03/28/ico_fines_flybe_honda/