WHITE PAPER

A Practical Guide for GDPR Compliance

An Osterman Research White Paper

Published July 2017

RSA®

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

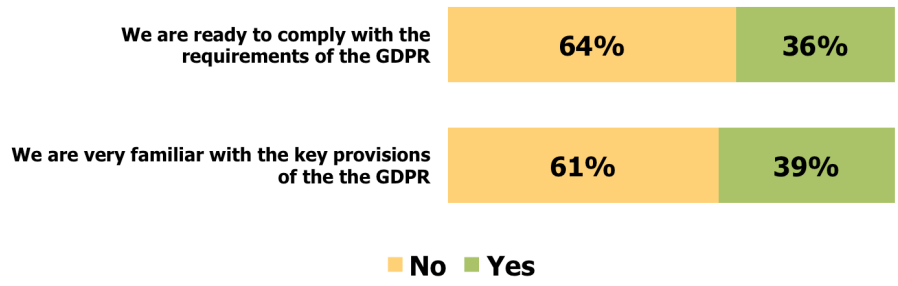
EXECUTIVE SUMMARY

The General Data Protection Regulation (GDPR) has been approved by the European Union and, once it comes into force in May 2018, will give data subjects significant new rights over how their personal data is collected, processed, and transferred by data controllers and processors. It demands significant data protection safeguards to be implemented by organizations. The time to get ready is now, as the consequences of getting it wrong are significant.

KEY TAKEAWAYS

- Most organizations are not yet adequately prepared for compliance with the GDPR, as shown in Figure 1.

Figure 1
Organizational Preparedness for the GDPR



Source: Osterman Research, Inc.

Most organizations are not yet adequately prepared for compliance with the GDPR.

- The GDPR is a sweeping and far-reaching update to the European Directive on Data Privacy from 1995. It harmonizes data protection requirements across all 28 Member States, introduces new rights for data subjects, and applies extra-territorially to any organization controlling or processing data on natural persons in the European Union.

- Complying with GDPR is not optional. If your organization controls or processes personal data on natural persons in the European Union, GDPR almost certainly applies to you. There are a whole host of requirements and mandates that need to be in place when GDPR comes into force, not least of which is that when a data breach occurs, the local data protection authority and all affected data subjects[i] must be notified within 72 hours.

- GDPR requires data controllers and processors to implement both organizational and technical safeguards to ensure the rights and freedoms of data subjects are not compromised. Organizational safeguards include data protection impact assessments, data protection by design for both structured and unstructured data, and the appointment of a data protection officer who reports to the highest level of the organization.

- Technical safeguards include pseudonymization, encryption, and various capabilities for identifying and blocking data breaches, ensuring data security, and automatically identifying and classifying personal data, among others. It is important to note that a "data breach" according to the GDPR also includes "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed", and so preventing unauthorized use or access must also be considered as a key element of GDPR compliance.

- The deadline for being compliant with GDPR is rapidly approaching, and the transitionary period between the earlier Directive and the new Regulation is on now. Once the Regulation goes into force on May 25, 2018, organizations will be expected to comply immediately from that date.

- Being non-compliant with GDPR will be very expensive. In addition to other financial consequences, there are two tiers of regulatory fines, the more expensive of which is a fine of up to €20 million or four percent of the annual worldwide turnover for the organization, whichever is higher. However, there is a need for continual compliance with the GDPR, since a failed audit can have damaging financial consequences. Consult Hyperion has estimated that European financial firms alone may face GDPR-related fines of $5.3 billion in the first three years after the GDPR becomes effective[ii].

ABOUT THIS WHITE PAPER

This white paper was sponsored by RSA. Information about the company is provided at the end of this paper.

WHY IS THE GDPR IMPORTANT?

The General Data Protection Regulation (GDPR) is the newly harmonized European-wide regulation that mandates the protection of data about people living in the European Union, by every organization that controls or processes data on people in the EU, regardless of where that organization is located around the world. Its correct name is Regulation (EU) 2016/689, and it updates, replaces, and extends the protections previously afforded through the earlier 1995 directive on data privacy (Directive 95/46/EC). Protections for personal data of individuals involved in criminal proceedings are excluded from the GDPR; the protection regime for such circumstances are outlined in a complementary directive (Directive (EU) 2016/680), and is beyond the scope of this paper.

If your organization controls or processes data on people living in the European Union – even if your organization is not located in the EU – [the GDPR] applies.

The new GDPR is important, for several reasons:

- It almost certainly applies to you. If your organization controls or processes data on people living in the European Union – even if your organization is not located in the EU – it applies.
- It has a significant bite, in the form of sky-high regulatory fines for non-compliance. If you meet the test of applicability for the GDPR, you cannot opt out of complying.
- It touches every data process in organizations that collects or processes personal data on people, and it covers both direct and indirect data identifiers in every data system.
- It forces organizations to know and understand their data from a 360-degree perspective. Organizations that process EU citizen data will need to know where it is being processed, who is processing and storing it, and demonstrate the ability of "erasure" on it no matter where it lives.
- It demands greater transparency with people on how their data is collected and processed, and introduces notification requirements when personal data is breached. There are reputational consequences of getting this wrong, particularly in light of the fact that during the previous 12 months, 47 percent of the organizations surveyed for this white paper have suffered a breach of customers' or other personal data, employees' personal data, corporate intellectual property, or other sensitive or confidential information.
- There is now no cost associated with requests from data subjects, which means that it is now more likely that many more individuals will be making demands about the information that is held about them.
- You are running out of time. GDPR was signed into law just over a year ago (via publication in the EU Official Journal in early May 2016), and will be enforced starting May 25, 2018.

The earlier Directive on data privacy came into force in 1995, just as the Internet was beginning its adoption trajectory. One of the driving reasons for the new GDPR was to strengthen data protection requirements in light of an increasingly global and interconnected

world, and the regulators took an interesting path. Instead of regulating territorially on organizations within the EU, it shifted the focus to where data subjects reside. This subtle shift means GDPR applies to the personal data of data subjects in the EU (territorially), but has borderless applicability to organizations. The test is no longer whether your organization is in the EU, but rather whether your organizations collects or processes the personal data of people who are in the EU. Specifically:

- Article 23 lists key tests of applicability for organizations not located in the EU. The primary test is that "the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment." However, "mere accessibility" to an organization's website or email address is not sufficient to establish the intent of offering goods or services; whereas factors such as the use of a currency generally used in a member state, and listing customers located in the Union on your website, does ascertain that intention.

- Article 24 offers a second key test of applicability: when an organization controls or processes data for monitoring the behavior of people that happens within the EU. Specific actions include tracking on the internet, "profiling" based on past actions, and "analyzing or predicting ... personal preferences, behaviors and attitudes." If your organization does this for people within the EU, GDPR applies regardless of where you are located.

- With the UK's vote in 2016 to leave the European Union, there has been some discussion about the applicability of GDPR. There are two answers. First, the Data Protection Act is the UK law for data protection, and if the UK does leave the Union, the GDPR will not apply to data subjects and personal data within the UK. Second, the GDPR does apply to Europe, and any UK firm that wants to sell into the EU Single Market will have to comply with GDPR requirements. Individual firms can upgrade their data protection approaches to the GDPR mandates, in addition to whatever regulatory reform is undertaken in the UK to provide equivalent data protection standards.

In closing, GDPR is coming fast, it almost certainly applies to your organization, and the consequences of getting it wrong are severe. Equally, however, are the positive consequences of getting it right, including a strong foundation for working with businesses in Europe, a clear understanding of consumer preferences, and strong internal data protection and security controls that foster trust with customers and partners alike.

GDPR is coming fast, it almost certainly applies to your organization, and the consequences of getting it wrong are severe.

ON THE PRIVACY OF PERSONAL DATA IN THE EU

"Privacy" of personal data has been an essential concept in European law since 1995, when the Directive on data privacy was introduced. As a directive, however, it did not directly mandate data privacy protections for EU Member States, as each State had the freedom to include the recommended privacy protections in their own laws. This freedom led to nuances and differences in data privacy regulations across Member States, making it complex for firms to meet compliance requirements.

The new GDPR is different. First, it is a regulation - and not a directive - for all EU Member States. Member States don't have to enshrine GDPR into their own laws; it already applies to all of them. Second, the more limited focus on "data privacy" in the earlier directive has given way to a broader emphasis on "data protection" in GDPR; this higher standard demands more of organizations everywhere.

The question as to "why" privacy and protection of personal data is necessary is addressed in Article 75 of GDPR. The view is that lack of privacy and protection increases "risks to the rights and freedoms of natural persons ... which could lead to physical, material or non-material damage." Specific examples listed include discrimination, identity theft, fraud, financial loss, and loss of confidentiality of personal data, among others.

WHAT IS "PERSONAL DATA" ANYWAY?

Personal data is the first definition given in Article 4: "any information related to an identified or identifiable natural person" (called a data subject throughout the GDPR). Direct identifiers include name, ID number, and online identifiers (e.g., email address), and indirect identifiers

include location data and various types of identity. The personally identifiable information (PII) that will be relevant in the context of the GDPR includes data subjects' biometric data, network identifiers, images, hobbies, political preferences, religious preferences, sexual orientation and other information about EU residents.

The key test is whether direct and indirect personal data can be used to uniquely identify a natural person: while the person's name obviously can, so can the combination of indirect identifiers. For example, a study in the United States found that date of birth, zip code, and gender allowed for the unique identification of 87 percent of Americans, hence the need to afford indirect identifiers the same level of protection as direct ones.[iii]

The Directive of 1995 and the Regulation of 2016 are directionally the same, but the Regulation demands a significant uplift in data protection. For example:

- Data subjects acquire many new rights, including the right to be forgotten, the right to move their data to another provider, and the right of access to verify data correctness and the processing activities his or her data are subjected to.

- Organizations that control or process personal data must meet elevated protection mandates, including gaining specific consent from data subjects, record keeping, notification of data breaches, and having the organizational and technical means to respond to the rights of data subjects in a timely manner.

- Under the Directive, data processors only had responsibilities insofar as they were demanded through contractual agreements with data controllers. Under GDPR, processors now have direct obligations to implement appropriate security measures, maintain records of processing activities, and meet data breach notification requirements.

DRIVERS FOR INTRODUCING THE GDPR

Several factors drove the development of the GDPR for Europe, including:

- Modernizing the data protection laws to take account of the Internet, digital marketing, social networks, and the whole plethora of data tracking capabilities currently on offer and coming due to technological advances since the Directive was introduced in 1995.

- Harmonizing the legal framework for data protection across Europe, moving from separate regulations in Member States to a Digital Single Market with common standards and rules for all. The European-wide regulation simplifies compliance for organizations operating in multiple States.

- Driving a stronger culture of data protection and security into the heart of organizational data processes. The regulation makes clear the requirements on organizations controlling or processing personal data, and demands stronger measures to protect data subjects and reduce mistakes in handling personal data.

- Leveling the playing field so organizations outside of the Union can't claim immunity from data protection requirements when handling personal data of EU natural persons. The Directive applied territorially to organizations; the Regulation applies territorially to the personal data of data subjects, and to organizations regardless of location.

- Impacting global legal frameworks on data protection, by making GDPR apply to any organization controlling or processing personal data on data subjects in the EU, and by demanding equivalent data protection standards from other countries and jurisdictions wanting to trade with the EU single market. We have previously commented that the GDPR should be more appropriately called the "Global" Data Protection Regulation, given its legal impacts.

COMPLIANCE TIMEFRAME

The European Commission introduced its data protection reform in early 2012, and after four years of negotiations the GDPR was adopted by the European Council and European Parliament in April 2016. It was published in the EU Official Journal in early May last year, and comes into force on May 24, 2018. It will apply from May 25, 2018. There is no transitionary period as such after coming into force; that time is the two-years between May 2016 and May 2018, of which we are already more than half way through.

BREXIT AND THE GDPR

It is important to note that regardless of the implementation of Brexit (the UK's exit from the EU), the GDPR will continue to apply to subjects and organizations within the UK. The UK's Information Commissioner's Office (ICO) has clearly stated that the GDPR will be the minimum standard of protection for personal data. Specifically, the ICO has stated that[iv]:

- "The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR."

- The GDPR applies to "controllers" and "processors". The definitions are broadly the same as under the [UK Data Protection Act] – i.e., the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR."

- "If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR."

It is important to note that regardless of the imple-mentation of Brexit, the GDPR will continue to apply to subjects and organizations within the UK.

NON-COMPLIANCE PENALTIES

There are major penalties for non-compliance with GDPR, and these are set in two tiers (Article 83). Administrative fines of up to €10 million or two percent of the total worldwide annual turnover (that's revenue, not profit) for the organization can be levied for various infringements, such as not enacting 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 many others. The failure of an audit of GDPR compliance, which will be a more common event than a violation of the GDPR itself, can also result in penalties.

The higher tier of fines – which are up to €20 million or four percent of total worldwide annual turnover – is for more serious wrongdoing, such as not following the basic principles of collecting and processing data (Article 6), failing to acquire adequate consent from a data subject (Article 7), and not providing data subjects with their rights (Articles 12 to 22).

Both penalty level are "whichever is higher" between the Euro figure and the percentage amount, so an organization with a worldwide turnover of €10 billion could face a fine of €400 million under the second tier. Note that data subjects themselves also have the right to seek damages through a civil court from an organization that fails to protect their personal data.

THE ESSENTIAL REQUIREMENTS OF THE GDPR

Let's briefly review the essential requirements of the GDPR. You must:

- Have a legal basis for controlling and processing personal data (Article 6). Legal grounds include direct consent from the data subject, for performance of a contract with the data subject, compliance with a legal obligation of the controller, protecting the vital interests of a data subject, and the legitimate interests of the controller. It is essential to be very clear on the specific legal basis for collecting and processing personal data, because some rights held by data subjects apply only to data held under one or two legal grounds, for example. While the "legitimate interests" basis appears to give wide sway to

organizations, there are various provisions that limit its applicability, such as taking into account the context in which the data was collected and the relationship between the data subject and the controller.

- Collect and process personal data only for lawful purposes, and protect it at all times. Required protections include preventing accidental or unlawful destruction, loss, processing, disclosure, access, and alteration. Data subjects have significant rights and freedoms under GDPR, and these must be upheld through appropriate organizational and technological measures.

- Maintain documentation of all data processing activities (Article 30). Required details include the purposes of the processing, categories of data subjects and personal data involved, categories of recipients, safeguards on any data transfers, and if possible, time limits for erasure. A description of technical and organizational security measures is also required. These records are to be kept in writing or electronic form, and available for audit and review by the supervisory authority on request. Organizations with fewer than 250 employees are excluded from these documentation requirements, with some provisos.

- Perform an assessment on the risks to the rights and freedoms of controlling and processing personal data, and develop organizational and technological mitigations for the identified risks. The risk assessment has to include any third-party relationships for data held and processed on your behalf.

- Be able to demonstrate compliance with the GDPR, through organizational and technical measures, and the on-going assessment of the strength and suitability of these measures (Article 25). Demonstrating compliance includes having policies on how to protect data under your control, an up-to-date assessment of risks to personal data (e.g., unauthorized or overprivileged access), workable technical measures that enforce protection (such as encryption), rules on transferring data to other countries, a staff training and awareness program, the means to identify and investigate data breaches, and the means to respond promptly to data access requests by data subjects, among others. All of these measures are on-going: they need to work at all times, and having the means to verify the effectiveness of implemented measures is essential. Certification mechanisms are mentioned throughout the GDPR as well, highlighting the on-going nature of compliance. Overall, the clear intent of the GDPR is that personal data is actually protected, not merely that organizations implement data protection tools.

- Meet the elevated standard of consent, anytime consent is the legal basis for processing data (Article 7). Consent means "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" (as defined in Article 4(11)). Consent cannot be implicit, the result of pre-ticked boxes, or silence. Consent must be documented (which means the data controller must be able to produce evidence that consent was given). And among other stipulations, consent cannot be bundled (it must be given for each specific processing operation and purpose), and the data subject must be able to withdraw consent just as easily as they gave it. This elevated standard of consent applies to consent gained after GDPR comes into force in late May 2018, as well as to any pre-GDPR consent indications that will be used after GDPR goes live.

- Minimize the amount of personal data processed, a principle called data minimization (Article 5(c)). The intent of this requirement is that superfluous or extraneous personal data that is not required for a specific processing activity are not collected or processed. Article 25 takes this requirement further, in addressing the requirement of "data protection by design and by default." Once personal data is no longer required for current data processing activities, it should be minimized through pseudonymization (a process of replacing direct and indirect identifiers with near-meaningless values, although these can be reidentified through specific means) or the data should be erased.

- Notify the supervisory authority of a data breach within 72 hours of becoming aware of the breach (Article 33), and under certain circumstances, notify every data subject whose data was breached as well (Article 34). A breach notification is not required to the supervisory authority if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons," nor to data subjects if the breach won't result in a "high risk" to their rights and freedoms. For example, if the breached data was encrypted with a sufficiently strong encryption mechanism, data breach notifications are not required.

- Appoint a data protection officer (Article 37), who can be an employee for one organization, a representative for a group of organizations, or an external consultant. This is mandatory for public authorities, and for organizations that meet one or both of two tests: core activities "consist of processing operations which ... require regular and systematic monitoring of data subjects on a large scale," or that special categories of data are processed on a large scale. The data protection officer (DPO) must have "professional qualities," "expert knowledge of data protection law and practices," and the ability to perform the tasks detailed in Article 39. Such obligations include informing and advising the controller and processor (and employees) of their obligations under GDPR, monitoring compliance, and being the liaison person with the supervisory authority. The DPO must "directly report to the highest management level" (Article 38), and is to be afforded independence in carrying out his or her tasks.

- Carry out a data protection impact assessment (DPIA) for envisaged processings that are "likely to result in a high risk to the rights and freedoms" of data subjects, and secure the participation of the designated data protection officer in the assessment (Article 35). High risks cover activities like automated processing and profiling, decisions that produce legal effects for people, large scale processing of "special categories of data," and the "systematic monitoring of a publicly accessible area on a large scale." The intent of such assessments is to force the pre-processing evaluation of what is actually necessary, how the processing activity could harm data subjects, and how to develop organizational and technical mitigations to reduce any foreseen harm. Under some circumstances, organizations must consult with the supervisory authority prior to undertaking the processing itself, and wait until the supervisory authority has ruled the processing activity to be lawful (Article 36).

- Ensure the protection of data during processing activities, through the implementation of "appropriate technical and organizational measures" (Article 25). These protection safeguards are to be implemented when determining how to carry out a processing, and at the actual time of carrying out the processing activity. The safeguards required are to be in proportion to the risks to the rights and freedoms of data subjects. Article 32 lists technical and organizational security measures such as pseudonymization, encryption, processing system confidentiality, integrity and resilience, and a regular testing process for ensuring the security measures actually work.

- Abide by specific conditions when processing special categories of data. Article 9(1) states the general prohibition: "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 10 exclusions to the general rule. Given the elevated harm that can accrue to individuals based on these special categories of data, greater protections are mandated. GDPR recognizes that the use of data may be sensitive, and hence seeks to limit such usage, which is why data protection impact assessments are generally necessary for processing special categories of data, the data protection officer must be across such processing, and consultation with the supervisory authority is required.

- Respond promptly to requests from data subjects about the personal data you control, process, or transfer about him or her (Article 15). The data subject has the right of access to know the purposes of the processing, categories of personal data processed, recipients or categories of recipients the data will or have been disclosed to, how long the data will be stored, their right to rectification or erasure, and more. If the personal data is

Once personal data is no longer required for current data processing activities, it should be minimized through pseudo-nymization.

subjected to automated decision-making and profiling, you have to provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." The first request from a data subject must be fulfilled free of charge, although "a reasonable fee based on administrative costs" can be levied for "further copies." Article 63 adds that the data subject should be able to "exercise [this] right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing." Article 63 goes on to suggest the use of a "secure system" that gives the data subject direct access to his or her personal data.

- Update and correct any inaccurate personal data held about a data subject, by various means including a supplementary disclosure from the data subject (Article 16). This is the flip side of the data subjects' right to rectification. Organizations will need tight integration across all data systems and processes to ensure data updated in one system is automatically and correctly updated across all other locations too.

- Permanently erase any personal data about a data subject under specified conditions (Article 17). These include the withdrawal of consent by the data subject (where consent was the original lawful basis for collection and processing), the data has been unlawfully processed, and the data subject objects to the processing of their personal data and there are no other legitimate grounds for continuing to process the data. If the data has been made public by the controller or processor, "reasonable steps" need to be taken to inform other controllers and processors of the erasure request.

- Be able to temporarily restrict the processing of personal data on request from the data subject under certain conditions (Article 18). These include contested accuracy, unlawful processing but erasure is not requested, and the data subject's need for the personal data for legal claims but where further processing is not necessary. Article 67 outlines several methods for restricting processing, and requires that this fact "should be clearly indicated in the system."

- Supply personal data concerning a data subject in a "structured, commonly used and machine-readable format" in response to a request for data portability (Article 20). This requirement is limited to the personal data the data subject "has provided to a controller," and the data subject can request the controller to transmit the data to a new data controller "without hindrance" or in good faith. There are various exclusions noted in Article 20, such as where other lawful grounds apply to future processing activities.

- Have alternative methods available for making decisions about people rather than just automated processing and profiling, such as human intervention (Article 22). There are several exceptions to this mandate, such as the necessity of processing related to contractual matters, exemptions under Union or Member State law, and where the data subject's explicit consent has been given (and not withdrawn). Article 22 makes it clear, however, that whatever happens, the data subject's rights and freedoms must be safeguarded.

- Prevent data from being transferred outside of the EU to "a third country or to an international organization" unless specific protections are in place (Article 44). These protections can be either an adequacy decision by the European Commission (the target recipients have an adequate level of data protection; Article 45), or the controller or processor has appropriate safeguards in place and legal remedies available (Article 46), such as Binding Corporate Rules (Article 47), among others.

- Ensure additional restrictions are in place to safeguard the handling of personal data of children when services are offered directly to children (Article 38). Language aimed directly at children must be "in such a clear and plain language that the child can easily understand," (Article 58) and consent is required from "the holder of parental responsibility over the child" for children under the age of 16 (Article 8), although Member States can lower this to 13 years. One strong implication of this requirement is the ability to verify proof of age.

It should be clear from the above "brief review" that the GDPR demands many significant undertakings from all organizations controlling or processing personal data on natural persons in the European Union.

A CHECKLIST FOR GDPR COMPLIANCE

Use the following checklist to gauge your readiness for GDPR compliance, starting May 25, 2018.

Item	Description of Task	NC	CC
1	Elevate the importance of the GDPR to the highest level in your organization Definitely: CEO and Senior Management Team Most Likely: Board of Directors	☐	☐
1.1	Educate key decision makers on the GDPR and its impacts for your organization Impact: Appoint a Data Protection Officer, who must report directly to the highest level of management in the organization. Impact: Execute GDPR requirements within an overall framework of data protection compliance. GDPR isn't the only regulation your organization is subject to. Impact: Create a cross-organizational task force to ensure GDPR compliance by May 2018 at the latest; this is not the job for any group working alone.	☐	☐
1.2	Understand the two levels of penalties for non-compliance with GDPR and the causes for each tier of fines, as well as bad PR through failed audits, data breaches, higher data processing costs, etc. Tier 1: €10 million or 2% worldwide turnover Tier 2: 20 million EUR or 4% worldwide turnover Idea: Calculate the fine for your organization at 2% and 4% of annual worldwide turnover for the previous year. Compare this cost in light of the cost of becoming compliant. Mitigation: The supervisory authority will evaluate evidence of action toward protecting the rights and freedoms of data subjects when setting a fine. It will go much better for an out-of-compliance organization that has a comprehensive program underway to develop a data protection system and culture, compared with one that does not. Mitigation: Evaluate cyber-insurance options.	☐	☐

NC = Not Compliant, CC = Completed and Compliant

Item	Description of Task	NC	CC
1.3	Develop and implement employee training on data protection, the GDPR, and the rights and freedoms of data subjects Topic to Cover: What employees must do Topic to Cover: What employees must not do Topic to Cover: Tasks and responsibilities in ensuring data protection for data subjects	☐	☐
1.4	Assess the principle of data protection by design and by default against your current systems and processes Include: Assess current systems that hold personal data on customers for the risks they create to the rights and freedoms to data subjects Include: Assess current systems that hold personal data on employees for the risks they create Include: Public facing websites, customer relationship management systems, direct marketing systems, the corporate intranet, employee profiles, Active Directory and other directory solutions that provide authentication to various data sources, HR systems, custom internal applications, and more. Warning: Many of your existing systems were probably developed prior to GDPR, so data privacy and protection may be viewed as add-ons rather than integral design choices. That philosophy needs to change under GDPR.	☐	☐
1.5	Evaluate whether personal data on EU data subjects will be transferred outside of the EU, and if so, what safeguards will be enacted to protect personal data Options: An adequacy finding by the European Commission and the use of Binding Corporate Rules are two possible options, among others. Task: Considering the risks to personal data, develop appropriate organizational and technical measures for data transfers.	☐	☐
1.6	Review data sharing and processing agreements with other organizations, and evaluate their compliance with the provisions of the GDPR. Include: Review contracts and agreements with business partners, cloud service providers, and other third-parties that can access personal data under your control. Include: Review the organizational and technical measures embraced by third-parties to protect personal data, and the efficacy of such approaches. Include: Develop or adopt certification mechanisms or codes of conduct to govern data protection by third-party organizations.	☐	☐

Item	Description of Task	NC	CC
1.7	Look for associations and other bodies that represent your type of business and are working actively on industry-wide approaches to GDPR compliance Benefit: GDPR is a major change for all organizations. Developing shared best practice helps to ensure that GDPR compliance is effective for all industry players, and active involvement in industry efforts signals a serious-minded approach to developing your GDPR approach. Benefit: The data subject's right to data portability requires the development of interoperable data formats. Associations and other bodies can champion such work.	☐	☐
1.8	Get started immediately, and allow sufficient time for the process. Don't wait until the last moment. Consider: Engage early and directly with your supervisory authority. Consider: Engage early and directly with external legal and professional services firms with a specialization in GDPR compliance. Leverage their wider experiences in your GDPR roadmap.	☐	☐
2	Evaluate current industry standards and certifications that provide a structured framework to guide compliance with GDPR (and similar obligations), both for your organization and any third-parties. Benefit: You can use commonly accepted marks and seals to signal your data protection standards to data subjects, the supervisory authority, prospective business partners, and other interested parties. Example: ISO 27001 is an international information security standard that can help with GDPR compliance initially and ongoing. It offers independent certification, and provides an overall framework for information security. Note that it does not give 100% GDPR compliance (for example, responding to the rights of data subjects). Example: ISO 27018 is the international standard for protecting personal data stored in public cloud services, adding a substantial set of controls for operational security.	☐	☐

Item	Description of Task	NC	CC
3	Conduct an end-to-end data inventory and audit, so as to know every location where personal and sensitive personal data is located, processed, stored, or transmitted. Evaluate your ability to identify, analyze in place, and classify personal information. Apply remediation policies to different categories of data and delete unneeded data (and thus minimize regulatory exposure). Include in this effort appropriate management of access privileges, and the ability to search across systems to respond to subject access requests by gathering and remediating personal data (producing, deleting, etc.) Include: Data systems under the control of your organization, such as email systems, databases and applications, file servers, file shares, SharePoint, cloud share and sync services, SharePoint and other collaboration systems, and email archives. Include: Data stored in authoritative sources, as well as data that is stored on endpoint devices (as opposed to being merely accessed). Include: Data flows to and from countries outside of the European Union, considering the lawfulness of such transfers under GDPR. Include: Ensure that third party data processors will be compliant, able to offer all the functionality required, and have effective audit and reporting processes in place to protect data and respond in time.	☐	☐
3.1	Identify and catalog data systems and assets outside of the organization's direct control Example: Non-sanctioned use of cloud storage services such as Dropbox, Box, and other similar services. Example: Synchronization of corporate data to cloud services that is then synced and accessed from non-corporate devices (e.g., personal mobile devices and home computers)	☐	☐
3.2	Evaluate data sovereignty and data residency obligations under GDPR, and how these are enforced by cloud service providers used across your organization	☐	☐

Item	Description of Task	NC	CC
3.3	Identify organizational and technical measures that make personal and sensitive personal data inaccessible to the organization, to protect the rights and freedoms of data subjects Example: Identity management and access control, to ensure only the right people have access to data at the right time Example: Encryption at rest, in use, and in motion Example: Pseudonymization Example: Data protection by design and by default Recommendation: Keep good records of the organizational and technical measures evaluated and implemented. You will need to be able to demonstrate actions and mitigations aligned with GDPR compliance when being audited or monitored by a supervisory authority	☐	☐
4	Classify current data appropriately to determine specific categories of data that will be subject to the GDPR Remember: Both direct and indirect identifiers must be protected, and the use of data can be sensitive, not just the data value itself	☐	☐
4.1	Determine the categories of data that would trigger a data breach notification, and note the breadth of where such data could be breached from Include: Authoritative sources such as databases, directories, and customer relationship management systems Include: Ad-hoc data sources, such as file servers, SharePoint sites, and email Include: Test and development environments that have working copies of production systems (and therefore could have valid personal data too) Include: Endpoint devices that have synchronized copies of personal data	☐	☐
4.2	Establish the lawful basis for each category of data held and associated processing undertaken on such data Remember: All processing activities require a lawful basis, and these are specified in the GDPR Warning: While consent is the broadest lawful basis, there is an elevated standard of consent required, and consent can be withdrawn at any time	☐	☐

Item	Description of Task	NC	CC
5	Review and update current privacy and data protection policies to ensure conformance with GDPR Remember: Existing policies will probably have to be updated to conform with GDPR Example: How to protect personal data Example: How to limit access to personal data Example: How to ensure international transfers are lawful Warning: While policies are essential, as they create the "internal legal framework" for how work is supposed to be done, policies alone are insufficient. These organizational measures must be complemented by technical measures to ensure adherence.	☐	☐
5.1	Implement appropriate mechanisms for establishing and receiving consent from data subjects, reflecting the elevated conditions on consent Include: Update existing consent for personal data, as this will be required after GDPR comes into force Include: Determine how to collect and store evidence of elevated consent Include: A method of withdrawing consent, that is just as simple as giving consent Remember: Consent must be given specifically for each processing activity. Bundled consent is not allowed	☐	☐
5.2	Develop capabilities for responding to data access requests by data subjects. Include: The processing activities their data are subject to, and for the duration of time data will be retained and processed Include: Notification of the right to object to processing, as well as rights of rectification and erasure (under specified conditions)	☐	☐
6	Implement policies and processes for the new requirements under GDPR, such as the rights of data subjects Example: Responding to the right of access, rectification, or erasure within the allocated timeframe, and without onerous and expensive manual processing requirements Example: Responding to data portability requests, using an appropriate digital format, and when required, transmitting the requested data directly to the new provider. Remember: The right of erasure, for example, applies to all instances of personal data, not just data in the authoritative system. Ensure you can catch all copies and extracts Warning: Failure to address the rights of data subjects is a Tier 2 offence, attracting a possible fine of 20 million EUR or 4% of worldwide annual turnover, whichever is higher. It is worth getting it right.	☐	☐

Item	Description of Task	NC	CC
6.1	Document all data processes and bring them into alignment with GDPR requirements. Keep accurate records of all data processing activities Remember: Processing in core systems is relatively easy to safeguard, by data protection for exported data and data in test systems is also essential Warning: Failure to have an accurate register of data processing activities is a Tier 1 offence, attracting a possible fine of 10 million EUR or 2% of worldwide annual turnover, whichever is higher. It is worth doing it properly.	☐	☐
6.2	Modify or disestablish any data processes that are not compliant with GDPR requirements and are no longer necessary Example: Use pseudonymization or full anonymization to remove personal data from data processes that are no longer required Warning: Ensure that you have the lawful basis for deleting personal data, and that such personal data is not going to be required in the future for legitimate purposes, such as establishing or defending legal claims	☐	☐
6.3	For services targeted directly at children, establish appropriate practices for verifying data subjects' age, and where necessary, for gaining parental or guardian consent Remember: GDPR sets the age of a child as less than 16 years, but Member States have the right to reduce it to 13 years. Beware regional variations in different Member States	☐	☐
6.4	Develop and implement the data protection impact assessment process, for use when necessary Include: Prior consultation with the supervisory authority when the impact assessment reveals high risks to the rights and freedoms of data subjects Remember: Your data protection officer must be involved in this process Recommendation: Make this an auditable process, to create a trail of evidence of good practice in data protection	☐	☐

Item	Description of Task	NC	CC
6.5	Implement appropriate policies and notification schemes that will be triggered in the event of a data breach Include: real-time, continuous monitoring of suspicious or unauthorized changes to detect suspicious changes or unauthorized access to files or systems that contain personal data. Remember: Notification is not required if there is no risk to the rights and freedoms of data subjects as a consequence of the breach Remember: If there is a risk to the rights and freedoms of data subjects, notification is always required to the supervisory authority, and to data subjects under some conditions Warning: The common view is that a data breach is a matter of "when" not "if." Don't wait until a breach has occurred to get this process working Consider: Have a standing agreement with a public relations firm, to be activated in the event of a breach Consider: Have a similar standing agreement with a specialist incident response partner, to be activated as required. Or build (and regularly test) incident response capabilities internally	☐	☐
7	Establish the role of the Data Protection Officer, either as an internal role for one organization, a shared role across a group of organizations, or through a services engagement Remember: The contact details of the DPO must be accessible to data subjects, and the contact process simple and appropriate Remember: The DPO must report directly to the highest level of the organization, and his or her duties must not be interfered with Ensure: Your selected DPO has the required professional capabilities and expert knowledge in data protection	☐	☐
8	Implement appropriate technical measures to safeguard the rights and freedoms of data subjects, informed by an assessment of the risks to these rights and freedoms. The GDPR specifically mandates both organizational and technical measures, because people get it wrong sometimes, whether intentionally or by accident. Point of View: The European Regulators are concerned that companies not paying sufficient attention to the technology tools available to protect personal and sensitive personal data, and are thus using a legal framework to force adoption and uptake	☐	☐

Item	Description of Task	NC	CC
8.1	Automated tools for discovering, cataloging and classifying personal and sensitive personal data across your organization Why Necessary? Protecting data in sanctioned systems is relatively easy. The much harder task is ensuring any copies, exports, backups, and shadow IT systems that contain such data are made visible and protected. Automated means of discovering, cataloguing and classifying data offer an excellent safeguard against missing something important	☐	☐
8.2	Data Loss Prevention (DLP) capabilities to examine data flows and identify personal data that is not subject to adequate safeguards or authorizations. DLP tools can block or quarantine such data flows, pending suitable rectification Why Necessary? An employee that emails a mail merge spreadsheet containing personal data to an external marketing firm may have just caused a data breach, thus triggering the data breach notification requirement. DLP tools can identify and stop the breach before it happens.	☐	☐
8.3	Encryption of data in use, at rest, and in transit. Along with pseudonymization, encryption is explicitly mentioned as a safeguard in the GDPR Why Necessary? Encryption is one of the most potent data protection measures an organization can deploy. It renders personal data unintelligible to anyone without the decryption key. Most data breaches can be prevented if encryption is used	☐	☐
8.4	Data breach identification, blocking and forensic investigation capabilities for rapid awareness of active breach attempts by malicious actors, such as through compromised credentials, unauthorized network access, and active advanced persistent threats. Why Necessary? It will not look good for you if you don't know you have been breached, and another party makes it publicly known that you were. This will signal incompetence, and you will become a target for punitive regulatory fines. Forewarned is forearmed.	☐	☐
8.5	Pseudonymization to replace direct and indirect personal data identifiers in data systems with meaningless data values that can be reversed under the right conditions. This approach is explicitly championed in the GDPR, although there are some risks. Why Necessary? Pseudonymization safeguards personal data by removing it from production systems, enabling employees and others to work within the production system without actually having access to personal data. When necessary, the data values can be reidentified.	☐	☐

Item	Description of Task	NC	CC
8.6	Data export capabilities for complying with a data portability request from a data subject. Supplying data in the most appropriate format is essential. Why Necessary? To be able to respond promptly to data portability requests, without relying on manual export processes.	☐	☐
8.7	Network perimeter and endpoint security tools, for preventing unauthorized access into the network, preventing the entry of unwanted data types and malicious threats, and ensuring endpoints have not been compromised when requesting network, system, and data access. Why Necessary? To reduce the risk of malicious threats from taking root in network devices and endpoints, leading to data breaches and other threats. Such security capabilities can also highlight any unpatched or out-of-date operating systems or applications that could be vulnerable to malicious threats.	☐	☐
8.8	Mobile device management capabilities that can remotely wipe and kill devices that are lost, stolen, or otherwise compromised, as well as enforcing certain settings such as local encryption and security software currency. Why Necessary? Loss of unencrypted devices is one of the top causes of data breaches, and are relatively easy to overcome with mobile device management capabilities	☐	☐
8.9	File sharing protection and file sharing technologies that meet the requirements of data protection. Minimizing the duration of open sharing links, for example, can reduce data breach possibilities. Why Necessary? Using authorized file sharing services ensures compliance mandates are met for data protection, data transfers, and data residency.	☐	☐
8.10	Behavior analytics uses machine intelligence to identify people doing weird things on the network, in order to give early visibility and warning of employees starting to go rogue. Such tools can also highlight weird activities, such as employees logged in on devices in two different countries, which almost certainly means compromised accounts. Why Necessary? Early warning of out-of-normal behavior allows for quick rectification actions to prevent unauthorized access, data breaches, and other negative outcomes.	☐	☐
8.11	Privileged account management tools keep a close eye on the actions undertaken by administrators using privileged account credentials. Why Necessary? Privileged accounts are a key target for hackers, as they give widespread access to the most data. Alerting on out-of-the-ordinary behaviors by privileged accounts gives early warning of possible malicious intent.	☐	☐

Item	Description of Task	NC	CC
8.12	Anti-malware and anti-ransomware to ensure the integrity, availability, and resilience of data systems, by blocking and preventing malware and ransomware threats from gaining a foothold on devices. Why Necessary? To prevent malicious software from compromising organizational data systems and devices.	☐	☐

SUMMARY

The GDPR will be enforced beginning in less than 11 months from the publication date of this white paper. Every organization that maintains data on EU residents will need to ensure that they have the appropriate capabilities in place to ensure compliance with the varied aspects of the GDPR. Not complying will be potentially very damaging and, if the EU follows through on its promised fine structure, very expensive.

There are three primary imperatives that should drive decision makers to give the GDPR an extremely high priority until compliance has been assured:

- **Get your data ducks in a row**
  Every organization that maintains data on EU residents must undertake a significant re-examination of its data strategy with regard to its personal and sensitive data on these individuals. The specific requirements must be understood, planned for, and technology approaches implemented to address problems, strengthen policies and protections, and protect against things like data breaches and an inability to comply with the provisions of the GDPR. Data protection must be "by design and by default."

- **Many firms will have to play catch up**
  Organizations in the EU have lived with the general notion of the GDPR for more than two decades, but non-EU firms are largely unprepared for the implications of such a rigorous approach to data protection. Consequently, non-EU firms will need to come up to speed rapidly in order to protect against the consequences of non-compliance with the GDPR.

- **Focus on technology**
  Technology is essential in enabling organizations to be compliant with the GDPR, but it is only one element of a comprehensive approach to compliance, which includes robust and detailed policies, training, governance processes, and appropriate strategies that cut across not only IT, but also legal, risk management, compliance, senior management, HR and finance.

SPONSOR OF THIS WHITE PAPER

More than 30,000 customers worldwide – including more than 90 percent of the global Fortune 500 – rely on RSA Business-Driven Security™ solutions for cyber threat detection and response, identity and access management, online fraud prevention, and GRC and business risk management. Armed with the industry's most powerful tools, enterprises can better focus on growth, innovation and transformation in today's volatile business environment.

For more information and to see how RSA can help your organization address GDPR compliance, go to www.rsa.com/gdpr.

www.rsa.com
@RSAsecurity
+1 781 515 5000

REFERENCES

[i] If the "data breach is likely to result in a high risk to the(ir) rights and freedoms" as noted in Article 33 of the GDPR.

[ii] http://www.bbc.com/news/business-40441434

[iii] https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/

[iv] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/