GDPR COMPLIANCE:

Preparing Your Organization

GUIDANCE SOFTWARE is now

opentext™

The European Union's General Data Protection Regulation (GDPR), set to go into effect on May 25, 2018, was approved with the intention of creating uniform laws to regulate data privacy across the EU. Through the introduction of new safeguards protecting the data privacy rights of EU citizens, GDPR requires organizations doing business with individuals located in EU member countries to adapt their data handling practices in order to meet these new standards for compliance.

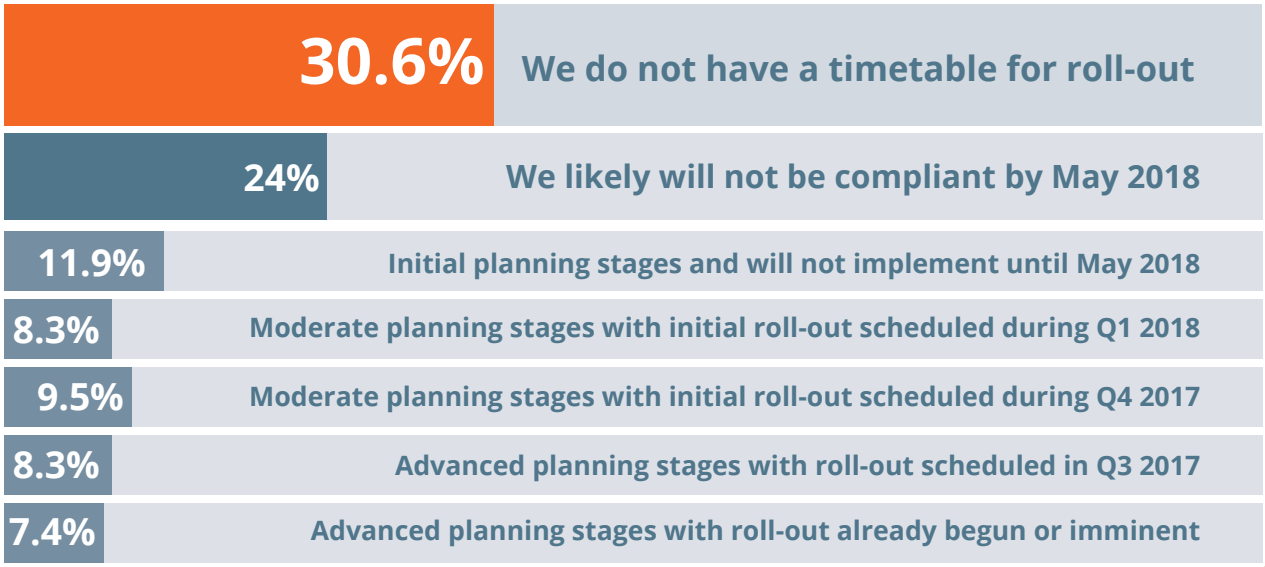
For organizations with operations spanning multiple nations, today's digital economy provides advantages that make entering new geographical markets easier than ever before. At the same time, legislators worldwide are acting to sate a growing public appetite for greater individual data privacy. Because of its potential as a seminal influence on how data privacy considerations are implemented, GDPR is a key point of interest, especially for multinational businesses. As organizations augment and refine their solutions for sharing data across borders and safeguarding the privacy of their customers, the ramifications of this upcoming regulation are top of mind.

Organizations stand to benefit from the standard approaches to privacy that GDPR will bring to business conducted across EU member states, ensuring that the same legal processes and rules apply across organizations, no matter where they are headquartered. On the other hand, the GDPR's requirements vastly increase the responsibilities that an organization handling EU citizen personal data must now thoughtfully address, as well as the penalties inflicted on organizations that fail to comply. The stakes of GDPR compliance are such that data protection processes are a topic for discussion at the highest levels of leadership.

IDC reports that the threat of immense fines due to non-compliance with GDPR will push businesses to invest $3.5 billion in additional data security and storage solutions. Investments in security software alone will more than double as the start date for GDPR enforcement arrives, jumping from $811 million in 2016 to an anticipated $1.8 billion in 2019. GDPR expands the scope of the guaranteed data subject rights to include breach notification, the right to access personal data, the right to be forgotten, data portability rights, systems that provide privacy by design, and the requirement that Data Protection Officers (for organizations over 500 employees) be empowered to add efficiency to data-related requests. Under GDPR, organizations must also develop a comprehensive data privacy strategy that features a 360-degree view of their data — meaning full insight into where data is located, precise details of what is occurring during any data breach incidents, and the capabilities to rapidly remediate both threats and errant PII. Considering these requirements, organizations that have not already done so ought to begin embarking down the path of implementing the data privacy solutions needed to achieve full compliance ahead of the May 2018 enforcement date. However, per a recent study conducted by Guidance and SC Magazine, many organizations have yet to really begin compliance work.

GDPR COMPLIANCE BEGINS IN MAY 2018.

WHERE IS YOUR COMPANY OVERALL IN PLANNING AND IMPLEMENTING GDPR? (Q6)



This paper will address specific challenges highlighted in our research, outline the process of becoming GDPR compliant, and delineate the ways in which the forensic security suite of products from Guidance Software – EnCase Endpoint Security, EnCase Risk Manager, and EnCase Endpoint Investigator – can deliver key capabilities for GDPR compliance.

CHALLENGES TO ACHIEVING GDPR COMPLIANCE

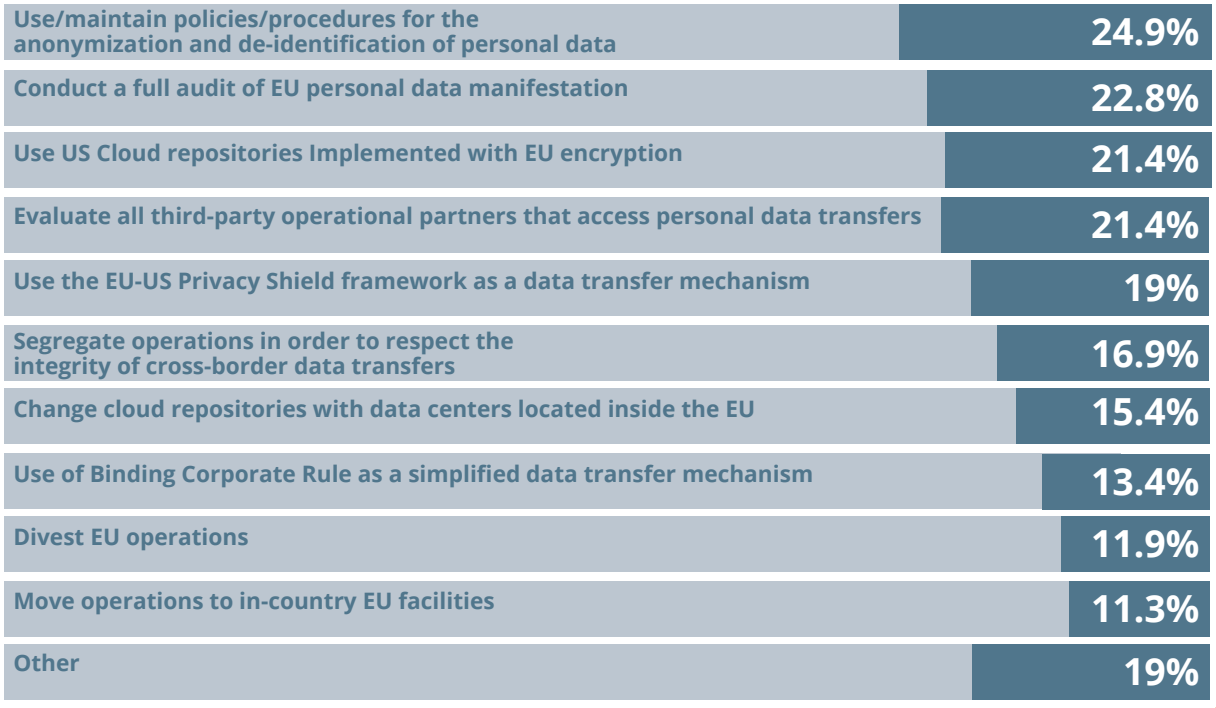
The incentives for organizations to be aggressive in addressing their GDPR compliance needs are clear: where compliance is required, the EU can and will use heavy fines to enforce regulation. Severe non-compliance can result in a fine of up to 20 million Euros or four percent of the organization's total worldwide revenue for the previous financial year (whichever is greater). Even cases of non-compliance with GDPR that are less severe can still lead to fines totaling the greater of 10 million Euros or two percent of total worldwide revenue over the previous financial year.

For most organizations, the challenge of complying with GDPR is successfully executing strong policies that define the careful methods with which data must be governed and retained. Achieving strict and dexterous control over all GDPR-covered data often requires investing in employee training, process development, and more capable technology solutions than organizations currently possess. However, the benefit can and should extend beyond simply "proving compliance." Such investments are necessary from a legal perspective, and valuable from a security ROI viewpoint. The Ponemon Institute finds that technology investments that result in effective compliance pay for themselves and then some, with non-compliance actually costing 2.65 times more than compliance.

An additional challenge comes with the fact that each affected organization likely has a significantly different profile when it comes to what sensitive data is retained, where it is stored, how it is used, and where it might be transmitted. Different organizations will naturally have different priorities; customer-facing businesses will possess personal financial data and information associated with marketing, B2B companies may have sensitive data from fewer clients stored in a very different set of systems, etc. Understanding the full inventory and usage of data within an organization may be a somewhat unexpected challenge, but it is a real difficulty faced by many sprawling multinational organizations – and one crucial to securing data privacy. If the first step to any solution is admitting you have a problem, the first step to data security is understanding the data that needs to be secured.

A final wrinkle is the reality that commercial organizations are dynamic, ever-changing entities with many moving parts, partnerships, policies, and goals. Given the complexity of such environments, data secured at one moment might be due for transfer to a third party via an unsecure channel the next. Preparing to implement effective data privacy requires examining all business relationships and auditing transfers to understand the movement and retention of data, wherever it may go.

IN ORDER TO BE OPERATIONALLY COMPLIANT WITH GDPR, WE PLAN TO DO THE FOLLOWING:



PREPARING A FOUNDATION FOR ACHIEVING GDPR COMPLIANCE (IN 5 STEPS)

Before an organization selects vendors to provide any required technologies in alignment with GDPR, it's necessary to execute groundwork. Existing data stores, new processes, and new responsibilities must be well understood, so solutions can be applied effectively.

Here is a 5-step process for completing these preparations:

1. To begin, the organization needs to fully understand and acknowledge the requirements of GDPR as they pertain to that business' specific situation. Importantly, GDPR does not necessarily apply solely to European organizations – it affects any organization operating in any country that has data pertaining to EU citizens, no matter where it is stored.

2. Next, conduct an audit of existing processes and a gap analysis against GDPR requirements to determine the people and processes necessary to transform internal practices in support of the new regulation.

3. Determine technology requirements that will be needed to fit these new processes. If existing systems used by legal, HR, information security, or other departments are moving protected data between countries, those data transfers need to be well understood. If there has been technology implemented to support the needs of other regulatory mandates such as PCI DSS (PCI Data Security Standard) evaluate if and how they may be leverages to support GDPR compliance. Know the business processes in play, including all data sources, the locations where data resides, and how that data is used by various business units – defining these processes will help determine where gaps exist in the next step, and how technology will be applied.

4. Now, map people to processes and recognize your security, data audit, and privacy needs by performing a gap analysis. Achieving full compliance with GDPR will require multiple technology solutions in accordance with both data discovery requirements and incident detection/response requirements. It's important to understand the full risks inherent within complex business processes (hint: cross-functional communication and coordination, technology integration), and to bolster data visibility and security where you have identified blind spots. For example, a company may have robust security in place to handle credit card processing, but the human element within internal operations – where data is copied, printed, or transferred – may represent a weak point that needs securing. Organizations often lack visibility into these types of risks to their sensitive data, which is why process mapping and a gap analysis are especially valuable exercises.

5. Implement a routine of regularly updating the organization's knowledge of the above to achieve ongoing insight of the data on hand and the processes that utilize it. Make it a goal to constantly verify that sensitive data isn't leaking into unauthorized, less secure systems. Test your incident response process before a breach occurs and periodically thereafter. Require ongoing internal reporting to ensure effectiveness in this effort.

Guidance Software Forensic Security Solutions

Guidance Software offers a suite of best-of-breed forensic security solutions – including EnCase Risk Manager, EnCase Endpoint Security and EnCase Endpoint Investigator – to help organizations manage, protect, and investigate their most critical business data and threats to that data. While there is no single tool that allows companies to become GDPR compliant, Guidance Software provides the technology to help organizations discover and secure sensitive unstructured endpoint data, and manage this data in a manner that is in line with the specific requirements of GDPR

HOW GUIDANCE SOFTWARE ASSISTS WITH GDPR COMPLIANCE

ARTICLE 33 – BREACH NOTIFICATION:

GDPR requires that any data breach that may "result in a risk for the rights and freedoms on individuals" be reported within 72 hours of its discovery. EnCase Endpoint Security is designed to help security teams quickly validate which alerts are real and require further analysis. It also provides a complete set of capabilities designed to rapidly triage threats, determine scope and impact, and apply a suite of remediation options to both isolate the endpoint and eradicate the threat. EnCase Risk Manager allows organizations to quickly "describe… categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned" per article 33 of GDPR. Finally, EnCase Endpoint Investigator provides post-mortem, root-cause analysis to ensure the team understands at the deepest level how a threat got in and how that threat interacted with patient-zero to deliver a payload and spread through the network. Automated incident response capabilities further ensure that potential threats to the endpoint can be identified and dealt with in a minimal amount of time.

PRIVACY BY DESIGN:

Guidance helps implement an architecture across all products that is naturally supportive of data security and privacy by assisting organizations with building data protection into the core design of data systems, minimizing risk profiles by holding and processing as little sensitive data as necessary, and limiting data access to ensure the least possible exposure. As required by the GDPR, data processing is performed without cross-border transfers, while providing dashboard level visibility into potential risk and the ability to escalate to in country data owners for review and decision making.

RIGHT TO ACCESS:

GDPR calls for data subjects to be able to request information from organizations to know if personal data about them is being processed, where the data is, and why it is being collected. When asked, the organization must also provide a free electronic copy of the personal data. EnCase Risk Manager is built to help organizations achieve this transparency by easily recognizing, locating, and controlling all unstructured sensitive data relating to a particular individual.

RIGHT TO BE FORGOTTEN:

In addition to the right to access, GDPR also grants data subjects the right to request that an organization erase all personal data pertaining to them, as well as to cease processing and sharing such data. GDPR requires that personal data be deleted when an individual's consent is withdrawn, or once it is no longer relevant to the original purposes for which it had been collected. Just as with the right to access, EnCase Risk Manager offers an effective means of quickly identifying and securely deleting an individual's data when appropriate — no matter where it is or how it is stored, even in the cloud.

DATA PORTABILITY:

GDPR gives data subjects the right to request that all data concerning them be transmitted to another organization, as they might find convenient. Again, EnCase Risk Manager's facility with searching for, collecting, and securely packaging data can assist organizations in completing these processes.

ACCOUNTABILITY:

Lastly, organizations under GDPR are required to put in place technical and operational processes by which they can demonstrate their compliance. Guidance Software's solution can clearly and ably provide this accountability through robust auditing and reporting.

ENCASE: DESIGNED TO MEET THE NEEDS OF GLOBAL ORGANIZATIONS

Guidance Software is the only cybersecurity company with a forensic security technology stack that provides 360° visibility into all stages of a security breach.

STEP 1: FLEXIBLE DEPLOYMENT

As pertaining to GDPR compliance, EnCase solutions can be deployed within centralized in-country regions to meet data privacy requirements. For instance, site servers and examiners can be installed in-country to ensure all data is processed and either stored locally or to a UNC path in the region, which is configurable by the owner. Once the data is stored locally, remote viewing and analysis of segregated data can be conducted in-country as well. For multinational organizations with footprints in two or more countries, a centralized console with data-minimization features can be deployed to report on aggregate sensitive data without transferring any files across borders while masking export-controlled content. This enables organizations to segregate roles and permissions by country, create baseline reporting, and demonstrate regulatory compliance. It is important to note that some competitors to EnCase Endpoint Security rely on peer-to-peer networking – doing so completely neglects in-country data segregation and integrity.

STEP 2: SECURITY BY DESIGN

Guidance Software provides market-leading forensic security applications to FTSE and Fortune 100 companies and hundreds of government agencies worldwide. Accordingly, deep forensic visibility and advanced security features are inherently built into each of Guidance's solutions by design. Whether searching for private or sensitive data that may be encrypted, deleted, hidden, locked, or otherwise hard to find – while ensuring that any visibility into the disk is strictly controlled using Public Key Infrastructure (PKI) handshakes – customers are able to maintain a high degree of confidence that their country-specific data is not seen by unauthorized parties.

EnCase products also utilize a patented optimized distributed search to scan enterprise endpoints prior to collections. This ensures only relevant files are collected and processed; once collected, they can only be reviewed and accessed by administrators. If the decision is made to delete select files, they can never be retrieved or restored by unauthorized parties.

STEP 3: SINGLE UNIFIED AND TRUSTED AGENT

EnCase products utilize a single unified agent that is proven and trusted internationally, with over 35 million deployments globally. This agent, which is universal across all of Guidance's security solutions, allows for an efficient eco-system of proactive sensitive data management, endpoint detection and response, and in-depth investigations. Time-tested and court-approved with the highest levels of security and reliability, the unified agent sits at the kernel-level and has complete yet controlled forensic access to all users, systems, and communications.

When agents are deployed, they are created in real-time, making them unique to your organization and cryptographically keyed to an on-premises authentication server within a given geographic location. This helps ensure both the inherent security of the system and that the physical location of endpoints will not violate cross-border data privacy restrictions. If sensitive data is suspected to have been manually transferred from one in-country network to another, the target network can be subsequently scanned to identify that information. Again, only the agents tied to an in-country server will be scanned, ensuring compliance with data privacy regulations.

CONCLUSION

Given the fast-approaching enforcement date of GDPR – and the potentially devastating penalties for non-compliance with the regulation – organizations cannot afford to ignore the need for appropriate data security and data privacy capabilities. GDPR requires organizations to execute a comprehensive strategy for data privacy. The Guidance Software forensic security suite can help. EnCase Risk Manager assists businesses in finding, categorizing, and when needed, remediating sensitive data. EnCase Endpoint Security and Endpoint Investigator deliver solutions to rapidly find, respond to, and report on security incidents and breaches.

GDPR is coming into effect at a time when the volume and sophistication of attacks is increasing. Many organizations experience tens of thousands of alerts requiring validation and assessment per day, with some attacks demonstrating sophistication equal to that of nation-state actors. This coincides with the continual arrival of new Internet of Things (IoT) devices, which often have very minimal built-in security. Attacks on these edge devices have increased with their influx.

Considering these realities, it is imperative that organizations dedicate adequate focus and resources to implement data security and privacy measures that are up to the task of meeting GDPR's standards, protecting customers, and shielding themselves from damaging fines. If you have not already begun to prepare, the time to start is now. May 2018 is just around the corner.

For more information regarding how Guidance Software can provide your organization with a data risk assessment and help with your GDPR compliance needs, contact us at (888) 999-9712 or visit guidancesoftware.com.

GUIDANCE SOFTWARE

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 35 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.