ELEMENTS
GLOBAL SERVICES

GENERAL DATA PROTECTION REGULATION:

WHAT IT MEANS FOR U.S. COMPANIES

INTRODUCTION

On April 26, 2016, the European Union (EU) Parliament adopted the General Data Protection Regulation (GDPR), a significant move to unify data protection across all EU member states. GDPR replaces the existing Data Protection Directive, which was enacted in 1995 to protect the privacy of all personal data collected about citizens of the EU.

The GDPR will have a major impact on how companies, regardless of their location, collect, store, and process the personal data of EU citizens. The regulation applies to data for all EU-based customers and employees and requires all businesses to document consent and use of that data.

The purpose of the regulation is to ensure that EU citizens have greater control over how their personal data is used. After GDPR is in effect, EU citizens will have the right to:

- Actively consent to use of their personal data
- Limit the way their personal data is used
- Be forgotten, or to demand that an organization identify and eradicate the data it has about them
- Have their data be portable
- Seek damages in the event their data is misused or breached.

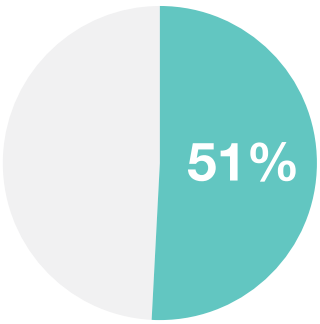
U.S. multinational companies with customers and/or employees in the EU must comply with GDPR. Many U.S. businesses were not affected by previous data protection rules, because those rules only applied to companies with some physical presence in the EU. Now, any company that processes personal data about EU residents, even if it is only online, must comply.

The GDPR takes effect May 25, 2018. After that date, non-compliant companies will face fines of up to 4% of their global annual revenue, or 20 million Euros, whichever is higher. Lesser offenses may result in lesser fines.

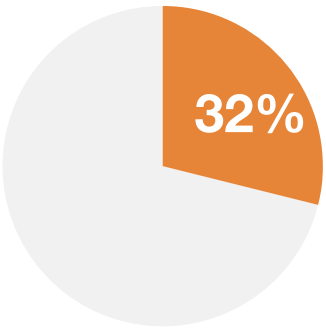
Why Now?

Introduction of the GDPR highlights the importance of effective data management and robust cybersecurity, especially in light of recent devastating cyberattacks. In its 2017 Data Breach Industry Forecast[1], Experian warned that "while companies are better prepared to protect against a data breach, attackers are finding more stealthy ways to get around security measures and seek the information they want."

The recent Equifax data breach, which compromised the personal data of 145.5 million people, or 60% of the adult population in the U.S. provided a stark reminder of the potential threats that exist for all businesses. Compared with data breaches of customer data, data breaches that impact employee records—which often include sensitive information such as health data, home addresses, Social Security and financial account information—can potentially have more significant, long-term effects.



51% of companies report that they experienced a global data breach in the past 5 years



32% reported they do not have a response plan in place

Source: Study by Ponemon Institute sponsored by Experian[2]

INTRODUCTION

Recognizing today's need for greater data security, GDPR goes beyond the previous Directive by including a definition of "personal data breach", requirements and guidelines for data breach notification and other steps needed to improve personal data processing to ensure network security.

Under the GDPR, a personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

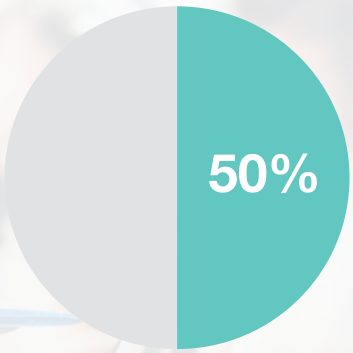
COMPLIANCE COMPLEXITIES **FOR HR DATA**

Unlike customer data, HR data presents additional issues for U.S. businesses seeking to comply with GDPR. Because of the sensitive nature and high volume of personal data they need to process on a regular basis, HR departments will need to find solutions to some special challenges. For example, they may need to:

- Map data from multiple sources. The fact that, unlike customer data, employee data is collected and stored in many locations—including HR information systems, payroll and benefits systems managed by third-party service providers, among others—complicates the process of mapping and providing employees access to their data.
- Meet additional requirements of individual EU member states. In addition to the requirements included in GDPR, there may be additional specific requirements in some EU member states that go beyond the scope of the GDPR regulation. For example, on June 30, 2017, Germany implemented new data protection provisions regarding a number of employee data issues, including creditworthiness and scoring, and video surveillance[3].
- Provide employees with more detailed information in Data Privacy Notices (DPN). In the past, employers provided information about the way their personal information is processed in employment contract clauses. Now, employers will need to provide each employee with a DPN at each point at which the employer collects personal data. As a result, employers will need to determine which employees will need DPNs, update or draft new DPNs, and train HR staff about procedures for processing data with DPNs.
- Comply with new restrictions on background checks. The GDPR includes restrictions on procedures for criminal background checks in situations that meet certain criteria. U.S. companies with EU-based employees will need to take steps to ensure that their procedures comply with the new GDPR requirements.

"When GDPR takes effect, HR departments will be tasked with the challenge to update their procedures for collecting the personal data of applicants and managing the personal data of current employees," says Rick Hammell, CEO at Elements. "That will require careful planning and preparation. It's a daunting prospect, but it can be accomplished by taking a step-by-step approach."

Gartner®



Gartner predicts that, when the GDPR goes into effect, more than 50% of companies affected by the GDPR will not be in full compliance with its requirements.

Source: Gartner[4]

KEY STEPS TO TAKE NOW

With the May 2018 deadline looming, it is imperative that U.S. companies with employees in the EU begin taking steps toward compliance. Working with a consultant throughout the process can save considerable time and money and provide greater assurance that your business is compliant with GDPR requirements.

A consultant with knowledge and expertise about data privacy and the challenges faced by global employers can help you assess your current situation with regard to handling employee data and provide a roadmap to compliance. Here are some recommended steps to take, with the help of a qualified consultant.

1. IDENTIFY THE LOCATIONS WHERE CRITICAL EMPLOYEE DATA SYSTEMS RESIDE.

Cloud-based HR information systems, which most U.S. multinational companies rely on for managing their employee databases, will be the focus of GDPR compliance efforts. However, because GDPR defines "personal data" as "any information relating to an identified or identifiable natural person," attention should be paid to the many other locations where employee data may be stored.

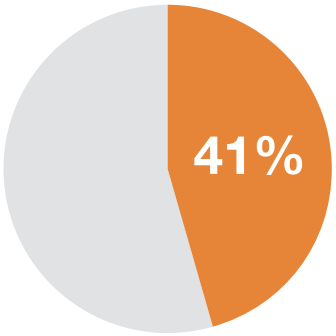
In order for your business to provide employees access to—and obtain permissions for processing—their personal data, you need to know where that data is stored.

> **"An experienced HR consultant can help you conduct a critical review of your existing architecture for storing employee data, help you put policies and procedures in place for GDPR compliance, and train your staff to implement those procedures," says Hammell.**

2. IMPLEMENT A SYSTEM FOR CONTENT CLASSIFICATION.

Any document that includes an employee name, home address, and other personally identifiable information (PII) falls under the jurisdiction of GDPR. Establishing a system for auto-classification of documents and content that include PII can help your business manage access to that data and comply with GDPR requirements.

> **"GDPR expects your business to be able to identify all the types of employee data you collect and store," says Hammell. "A qualified consultant can help you integrate all your data and build a framework for classifying and handling it in compliance with the privacy requirement of GDPR."**



Only 41% of organizations know where their employee data is located.

Source: Forrester[5]

3. REVIEW PRIVACY AND CONSENT POLICIES.

Recognizing the concepts of "privacy by design" and "privacy by default," the GDPR requires businesses to consider data privacy at every stage of a project—from initial design through the lifecycle of relevant data processing. As a result, you and your vendor will need to determine the best way to use HR information systems to comply with the regulation.

> **"A knowledgeable consultant will work with you to update your company's privacy statement to meet the 'say what you do' requirement of GDPR—and help you identify any updates needed in your operations to meet the 'do what you say' requirements," says Hammell.**

KEY STEPS TO TAKE NOW

4. REVIEW YOUR CURRENT EMPLOYMENT DOCUMENTS.

GDPR requires companies to obtain clear records documenting the consent of employees for processing their personal data. As a result, your company will need to reconsider the current consent clauses in employment contracts and implement additional documentation beyond the employment contract that demonstrates employee consent to process personal data.

> **"GDPR expects your business to ensure that any data protection provisions in employment contracts are clear and specific—and to provide opt-out mechanisms for employees," Hammell says. "An HR consultant with expertise in employment documents can help you review your documentation and determine the need for new documents and procedures."**

5. UPDATE VENDOR AGREEMENTS

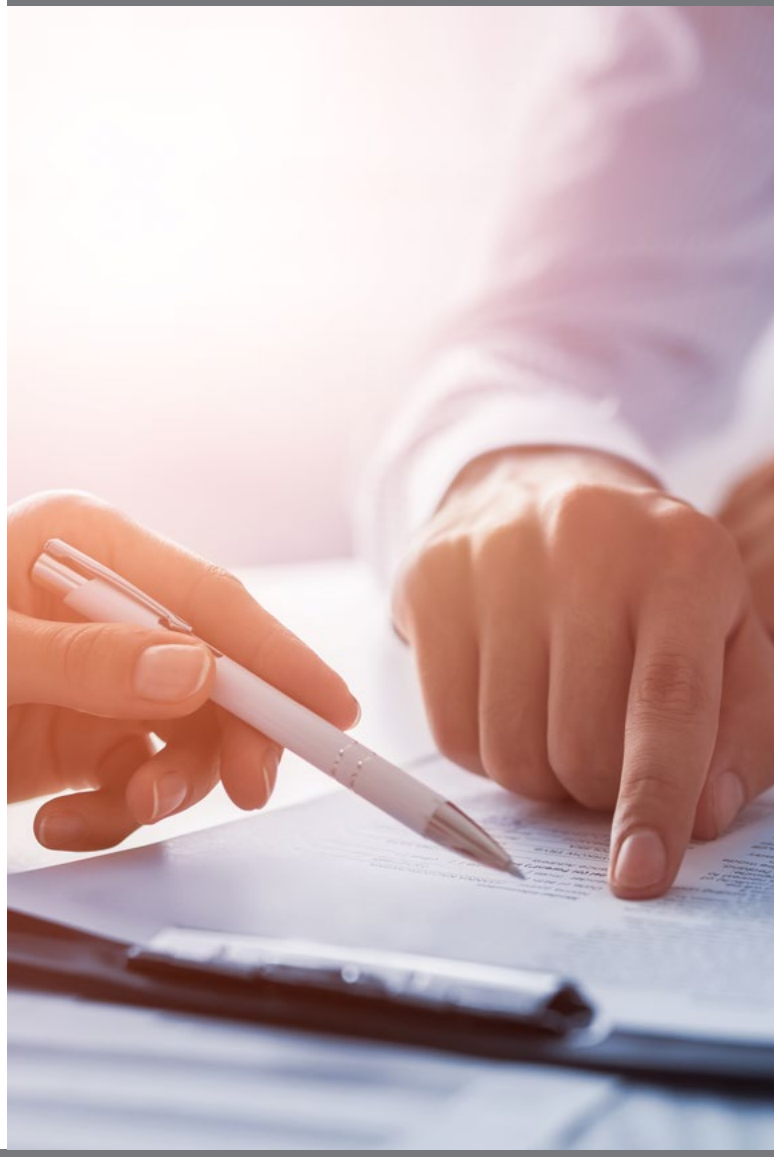
U.S. businesses are required to vet third-party service providers that collect and manage HR data to confirm their ability to comply with GDPR requirements. The regulation includes a long list of requirements for agreements with those vendors. Among other things, vendors located outside the EU must confirm that they are able to provide an "adequate level of protection" for transferred personal data. For this reason, it will be necessary to review current vendor agreements and policies for vetting potential vendors.

> **"The GDPR requires that your company understand how third-party service providers use the employee data that you share with them," says Hammell. "A knowledgeable consultant can help you assess the ways that your current third-party providers store, use, and protect your employees' data. They can also help you conduct due diligence and craft new agreements for potential vendors."**

6. REVIEW YOUR SYSTEMS FOR MANAGING ACCESS TO PERSONAL DATA.

The GDPR places great importance on the rights of employees to access, correct, erase, and object to the use of their personal data. As a result, U.S. companies must provide their EU-based employees with a mechanism to use in exercising those rights—and must respond to any request by an employee without undue delay.

> **"A key GDPR principle is ensuring that companies give the right people access to the appropriate data at the appropriate time," says Hammell. "A qualified consultant can conduct a review of your access management procedures and help you develop an effective strategy for GDPR compliance."**



ABOUT ELEMENTS

Elements Global Services is a leading International Payroll and Employer of Record (EOR)/Professional Employer Organization (PEO) with the expertise and resources needed to make the hiring and employment process as easy as possible.

With our long history of working with U.S.-based multinational businesses, we can provide you with informed and practical support for global payroll, human resources, benefits, and the visa process—and help you build an effective plan for compliance with the GDPR and other global regulations governing data privacy and security.

CONCLUSION

Time is tight for compliance with the new GDPR regulation, due to take effect on May 25, 2018. There are many new requirements that will necessitate review of current systems and the implementation of new policies and procedures. U.S. companies with employees in the EU will need to institute tighter controls on sensitive personal employee data and integrate improved identity and access management into their document and process flows.

U.S. companies and their HR departments will need significant and timely assistance from knowledgeable experts to identify changes that are needed in current processes and determine the best way to achieve those changes on a timely basis for GDPR compliance.

GDPR: Key Provisions

The GDPR goes well beyond the requirements for the existing Data Protection Act covering citizens of the EU. Following are some of the changes in the requirements with which U.S. multinational businesses will need to comply:

HEFTY FINES FOR NON-COMPLIANCE

Non-compliance with GDPR can result in fines of up to 4% of annual global revenue, or 20 million Euros, whichever is higher

GREATER GEOGRAPHIC SCOPE

GDPR applies to all businesses that employ residents of the EU, even those without a physical presence in the EU

EMPLOYEE CONSENT

Employees must give consent for processing of their personal data—and that consent must be easy to withdraw

DATA ACCESS AND PORTABILITY

Employees must be able to confirm whether—and where and why—their personal data is being processed and be able to obtain and reuse their personal data for their own purposes

BREACH NOTIFICATIONS

Companies must report any personal data breach within 72 hours

RIGHT TO BE FORGOTTEN

Employees must be able to have the company erase their personal data, discontinue any dissemination, and have third parties stop processing the data

PLANNING FOR GDPR: WHAT U.S. BUSINESSES ARE DOING NOW

According to a GDPR Preparedness Pulse Survey published by PwC[6] :

- Nearly all (92%) of U.S. businesses consider compliance with GDPR a top priority on their data privacy and security agenda in 2017
- Most (77%) of U.S. companies plan to allocate $1 million or more on GDPR readiness and compliance efforts

Steps they're taking

- More than half (58%) say they're adopting model clauses in their contracts to help ensure that certain data protection standards are met when working with a vendor
- Most (77%) are joining the EU-US Privacy Shield, a self-certification program of the U.S. Department of Commerce and Federal Trade Commission

Looking for more efficient ways to operate in Europe

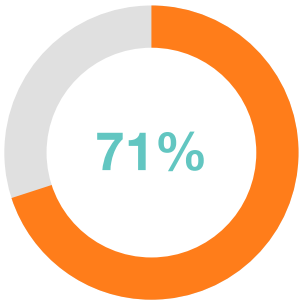
- 64% are considering centralizing their data center in Europe
- 54% plan to anonymize European data across the board

Some are backing away

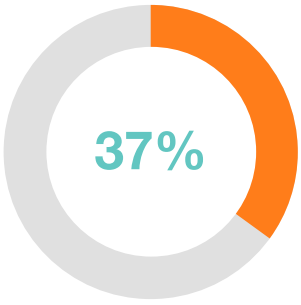
- 32% are thinking about reducing their presence in Europe
- 26% might leave the European market

How GDPR Compliance Could Benefit Your Company

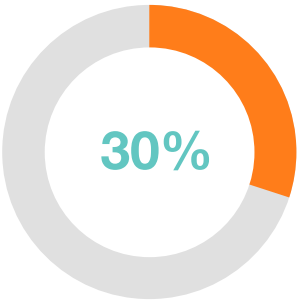
Even though new GDPR requirements present daunting challenges, many businesses are optimistic about the potential benefits they offer. A recent survey by SAS®[7] of 340 global business executives found that:



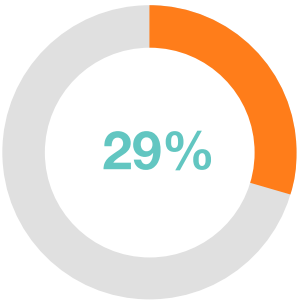
71% of businesses believe their data governance will improve



37% think their general IT capabilities will improve



30% agree that GDPR compliance will improve their image



29% think customer satisfaction will be higher

Resources

[1]*"2017 Data Breach Industry Forecast," Experian, https://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf*

[2]*"Data Protection Risks & Regulations in the Global Economy," Experian Data Breach Resolution and Ponemon Institute, http://www.experian.com/blogs/data-breach/2017/06/27/survey-companies-ill-prepared-global-data-breach/*

[3]*"Germany Publishes English Version of its National GDPR Implementation Act," Hogan Lovells, 2017, https://iapp.org/news/a/germany-publishes-english-translation-of-the-federal-data-protection-act/*

[4]*Gartner. (May 3, 2017). Gartner Says Organization Are Unprepared for the 2018 European Data Protection Regulation [Press release]. Retrieved from https://www.gartner.com/newsroom/id/3701117*

[5]*"The Data Security Money Pit," Forrester, 2017, https://info.varonis.com/hubfs/docs/research_reports/Varonis_TLP.pdf*

[6]*"Pulse Survey: US Companies Ramping Up General Data Protection Regulation (GDPR) Budgets," PwC, https://www.pwc.com/us/en/increasing-it-effectiveness/publications/gdpr-readiness.html*

[7]*"Working Toward GDPR Compliance," SAS, 2017, https://info.varonis.com/hubfs/docs/research_reports/Varonis_TLP.pdf*

Chicago | Barcelona | London | Hong Kong | Singapore

ELEMENTS
GLOBAL SERVICES

800-827-4660 | inquiries@elementsgs.com | elementsgs.com