

FORTR△

**EU General
Data Protection
Regulation (GDPR)
Compliance Are
You Prepared?**

What You Need to Know
to Make Your Data
Transfers Compliant

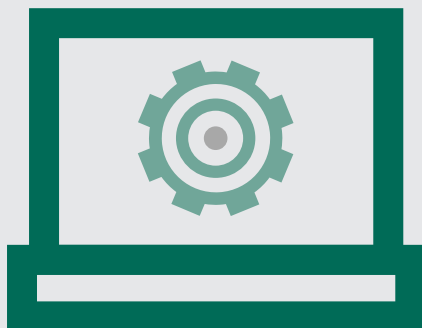




Save The Date

May 25, 2018

The General Data Protection Regulation Goes into Effect



If your organization processes data that pertains to residents of the European Union (EU), then **May 25, 2018** is an important date for you to remember.

And Here's Why

May 25 is the designated day that the EU plans to enforce the General Data Protection Regulation (GDPR).

GDPR applies if the data controller or processor (organization) or the data subject (person) is based in the EU. It also applies to organizations based outside of the EU if they process personal data of EU residents. The new regulation applies to a large number of global organizations or companies that do business globally.

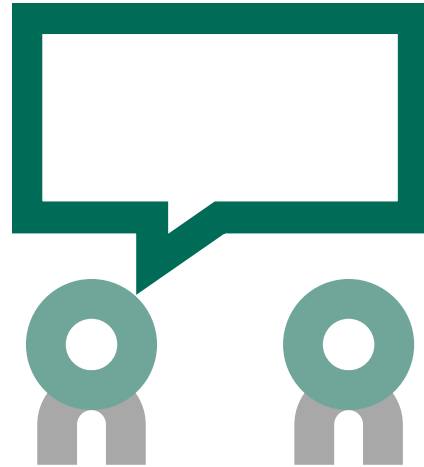


GDPR requires organizations to follow a new set of data protection directives designed to protect the data privacy rights of EU residents. EU's new set of rules intends to, "give citizens back control over their personal data, and to simplify the regulatory environment for business." [\(European Commission\)](#)



What is Personal Data According to GDPR?





According to the European Commission,

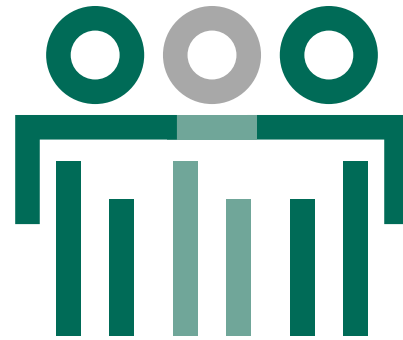
“personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.”

The regulation does not apply to the processing of personal data for national security activities or law enforcement; however, the data protection reform package includes **a separate Data Protection Directive for the police and criminal justice sector that provides robust rules on personal data exchanges at national, European and international level.**





Eighty-one percent of Europeans feel that they do not have complete control over their personal data online. ([European Commission](#))







Does GDPR apply to you?

With any new regulatory framework, it can be hard to understand whether or not your organization needs to comply with the new rules.

Here are few questions to consider





-  Does your business provide goods and services in the EU?
-  Do you have employees in the EU?
-  Are you managing consumer data in or from the EU?
-  Do you move your consumer or employee data outside of the EU?

If you can answer yes to any of the questions listed, then your organization will need to comply with the GDPR.

This guide offers an inside look at the GDPR and how you can make the transition to the security standards outlined within the EU's new regulations.



The Rise of GDPR and Privacy Protections for Citizens

The focus on GDPR is to ensure that companies are doing everything they can to protect the personal data and privacy of EU residents. Establishing these protections has taken a few years to develop, but now that the May 2018 enforcement date is getting close, it makes preparing for GDPR that much more urgent.

In 2012, the European Commission started developing GDPR after recognizing that the previous data privacy and protection legislation was out of date. After countless discussion that spanned more than four years, the **European Commission agreed on the privacy processes and procedures defined in the new regulation.**





Technology, data security, and the way we use data is vastly different compared to the past two decades, which is what the GDPR attempts to rectify in its legislation.





Additionally, the previous policies didn't offer the same standards and protections as an actual law, which meant that the directive only offered the minimum legal standards and **many inconsistencies in data protection laws throughout the EU.**



Once approved by the EU Parliament, the GDPR will provide an actual uniform data security law that all **EU member states would be expected to follow.**

GDPR establishes “**data subject rights**” which ensures that EU residents can retain control of their personal data, including:





Complete access over the information describing in plain language how personal data is used

Full access to personal data

Delete or correct personal data

Rectify and erase personal data (“the right to be forgotten”)

Restrict or object to processing of personal data

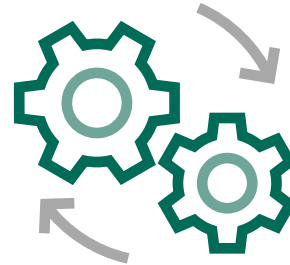
Object to processing of data for specific uses, like marketing or profiling





The Data Privacy Threat Landscape: The Reality of Protecting Personal Data

When critical data protection policies and processes compete with another equally critical set of business and technology requirements, protecting data can become a significant challenge. Managing the balance between the overlapping requirements and meeting compliance will happen in a collaborative environment, and not in an isolated environment of technology, security policies, or workflows.



Compliance will always be a dynamic entity requiring a proactive “all hands on deck” approach; otherwise your quest to protect personal data within GDPR will be a difficult endeavor to manage.

Competing priorities and collaboration are not the only challenges that organizations face when it comes down to protecting personal data in today’s environment.



Protecting personal data can also be challenging when faced with the following situations:





Minimal Awareness



In some cases, employees may not be aware of their own role in helping protect the security of an organization's IT infrastructure and data. They also may not be aware of the financial or legal ramifications that would follow a compliance violation or data breach.



2

High Volume of Data



Visibility over your data activity will always be a concern if you want to meet GDPR compliance. The higher volume of data that you manage, the more challenging it may be for you to track or control.

Ultimately, you can't secure what you don't know about.

3

Minimal Security Hygiene



A lack of security hygiene can lead to compliance security policies not being enforced. Security vulnerabilities should continuously be assessed and remediated. Controlling levels of administrative access to endpoints are also important.



No Accountability



Creating a culture that is conducive to protecting personal data must have the support of leadership or it will be impossible to make changes.



GDPR was created with the goal of protecting data privacy rights of residents within the EU, which means if you're managing the personal data of EU residents, **it's essential to understand the threat landscape and where your IT infrastructure has weaknesses.**

Personal data isn't safe without the right data management strategy, training, policies and tools in place.

At the same time, personal data will not be safe without full participation from your organization. However, should your organization face a data breach, the GDPR includes requirements that allow for information sharing to better inform those whose data you store or share that their information may be compromised or leaked.





The Risks of Non-Compliance Following the Rise of GDPR

Protecting the privacy of EU residents is at the core of GDPR, and the damage that would result in non-compliance can cause **irreparable damage to an organization's reputation.**

From a public relations perspective, non-compliance with GDPR can translate to the general EU public that data security and data privacy is not a top priority to your organization, which can then lead to lost trust and lost business.

If the perception of trust continues to decrease, it will affect your bottom line. In addition to the reputation damage, non-compliance can lead to expensive litigation and fines, which could add up to a €100 million fine or 2 to 4 percent of your annual worldwide revenue, whichever is greater. (PWC) That is a high price tag for non-compliance.



Your GDPR action plan must entail much more than using encryption and firewalls. Meeting and maintaining GDPR beyond their requirements should include a full scale data management strategy that will enable you to protect, manage, and audit any data within your IT infrastructure, specifically when the data you manage was collected or produced from residents of the EU.



May 25, 2018 is just around the corner. With fines climbing up to **4 percent** of global revenue for noncompliance with GDPR, now is the best time to get started on your GDPR action plan.



“More than 75% of surveyed organizations outside of Europe say that they are not or don’t know if they are prepared for GDPR.” ([Help Net Security Survey](#))



4 Steps to Maintaining GDPR Compliance

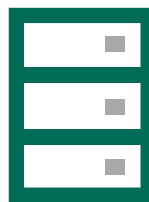
If your organization transfers EU data, you'll need a plan for getting maintaining GDPR compliance.

To maintain compliance you should follow these steps:



1

Identify the Type of Data You Have and its Location



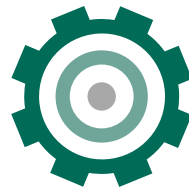
GDPR requires organization to report on not only data that may have been compromised in a data breach or cybersecurity incident, but what kind of data it is. In order for you to properly prepare for the GDPR, you should first figure out where your data is. Once you know where your data is, you should begin a process to classify the data, noting important sensitive details like personally identifiable information, who has access to the data, how it's being used, etc.

Under the GDPR, an organization has 72 hour to report any information that may have been lost or compromised. Classifying your information before May 28, 2018 will allow you to better prepare for potential reporting requirements enforced by the GDPR.



2

Set up a Process to Protect and Manage Your Data



Once you've classified the most important data that's critical to the GDPR, an organization needs to prove that it's doing everything to protect that data and the privacy or legal rights of the individual's information. This might require new security tools like endpoint security, data loss protection or managed file transfer platforms. This may also be a good time to hire or assign a data protection officer or chief data officer to the managing and establishing any processes required for compliance. This individual and their team would work closely with the rest of the organization in the time of data loss or breach.



3

Update All Crisis or Security Plans



If an incident should occur, an organization only has 72 hours to comply with the appropriate policies under the GDPR or risk fines. Plans should be drafted up, that likely could be incorporated into your security response plans, about who needs to be notified, what information they will need and how to access the correct reports or audit information.

4

Conduct a GDPR Readiness Assessment

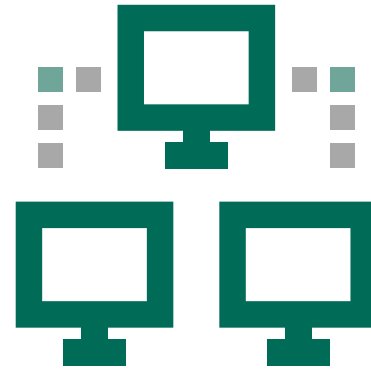
“21% of surveyed organizations said they would face a penalty if GDPR were in place today.” **Help Net Security Survey**



Once you've followed the first three steps, you can test your own readiness before May 28, 2018. If there are any areas of non-compliance, be sure to take the appropriate actions to rectify the issues. It's also important that organizations consider conducting assessments regularly, to ensure there is not a gap in compliance.

Preparing your organization for the regulation change must combine a full scale strategy that involves data management with a proactive and secure solution, like can offered with a managed file transfer (MFT) solution. At the same time, it's important that you consult with an attorney that specializes in international data protection laws.

The **EU GDPR Portal** covers the key regulation changes that will help you further prepare yourself for GDPR readiness.



Facilitating GDPR Compliance with a Managed File Transfer Solution

A managed file transfer (MFT) solution **simplifies and enhances a data management strategy**, helping an organization meet both business and compliance requirements through the secure and reliable exchange of data. With MFT as the data management solution, an organization can maintain full operational visibility and control over all data activity and access. A MFT solution can streamline the process of compliance through a secure system of policies, procedures, and technologies.





"Over half of U.S. multinationals says GDPR is their top data protection priority"

In the past twenty years, the most significant change in global policy came about with the new EU GDPR, which will enforce new obligations on any organization that manages personal data belonging to EU residents, regardless of the business location. If your organization is ready to secure GDPR compliance, then data management will play a crucial role.

Data management is conducive to developing an organization's security and compliance strategy. The methodologies and tools that support the secure management of data—especially when it comes to facilitating GDPR compliance helps organizations enhance their security profile through increased

operational visibility and efficiency. This is where a MFT solution can be a data transfer conduit that supports GDPR compliance, through a secure system of policies, procedures, and technologies. A data management strategy used in conjunction with a MFT solution and its security and visibility enhancing technologies, will enable you to enforce and facilitate compliance mandates, for greater control and transparency over the data and IT infrastructure you want to protect.

Source: [PWC, Pulse Survey: US Companies Ramping Up General Data Protection Regulation \(GDPR\) Budgets](#)

If you are evaluating enterprise data management solutions to help you facilitate GDPR compliance **(including its key changes)**, consider the **following MFT-supported features:**



1 Centralized Control and Visibility

Executives, department heads, and managers need a view of an array of business management-focused insights derived from the movement of files and data.

Not knowing what's happening in your network can be dangerous. Oftentimes, the most pervasive compliance pitfalls stem from a shortage of administrator insight into a sprawling, changing IT infrastructure. With today's network dynamics shifting so rapidly and encompassing new technologies all the time, transparency into these environments is critical if IT teams want to ensure everything checks out with regulatory expectations. Only when IT leaders can see the big picture, investigating and closing compliance gaps in a proactive manner, will a company truly be averse to risk and maintain a clean record.



Under GDPR's key changes, the data subject rights would be impossible to meet without a solution that provides centralized control and visibility. A robust MFT solution offers IT administrators an unprecedented level of transparency into the data in the entire network, empowering strategists with perspective and control that no manual processes could provide.

This top-down view of the infrastructure is a primary component of compliance excellence, and can also alleviate a number of other security and performance risks.

2

Custom Compliance Profiles & Reporting

It's important to understand how data moves throughout your organization. Every organization has its own set of regulatory expectations to uphold.

Therefore, a one-size-fits-all data management solution won't do much for a highly specialized compliance profile. Among the key GDPR changes, the data subject rights that would prove beneficial with the use of MFT's custom compliance profiles and reporting, includes the right to access, data processing notification for data protection officers, the processing of data through the conditions of consent, among many others.

Luckily, today's best solutions offer customized data workflows and configurations that ensure every data transfer is performed and tracked to the highest possible degree of adherence. A tailored MFT solution can simplify and strengthen its data management capabilities, which will better support your GDPR compliance initiatives. With each of these functionalities, an MFT solution simplifies what can easily be a complicated

endeavor when it comes to meeting compliance mandates—including complying with the security standards required from GDPR. The right MFT solution will also go beyond traditional IT considerations to provide real opportunities to achieve greater operational efficiency, enhance your security posture, and provide data management and integration capabilities, producing measurable effects on ROI within your organization.

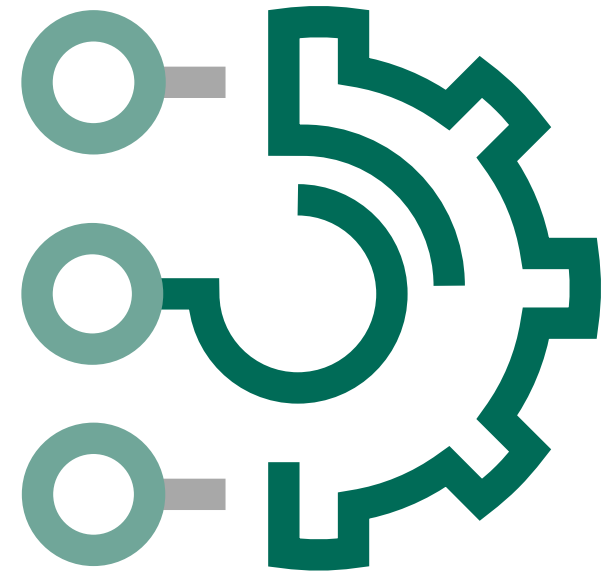
Compliance is undoubtedly a complex and dynamic endeavor. With a secure MFT solution and a strong data management policy, you will be better equipped to help your organization track, monitor, and report on compliance efforts so that you can proactively catch and mitigate any potential risks.

3 Automated Data Workflow and Processes

Today's end users may be aware of the compliance standards to which their organizations are held, but when performing daily tasks such as sharing data, messaging, and email, the need to comply with regulatory measures is not necessarily top of mind.

In fact, employees focused on productivity may take some shortcuts to accomplish more in a given day, circumventing best practices in the process. For profit-minded business leaders, it's hard to enforce data management standards while maximizing user performance.

An MFT solution should automate processes with all key applications and services with appropriate compliance functionality. This lets end users remain at the top of their game while all security and tracking processes are performed automatically in the background.





Achieving Better Data Management in the Age of GDPR



GDPR is undoubtedly a complex set of regulations to implement.

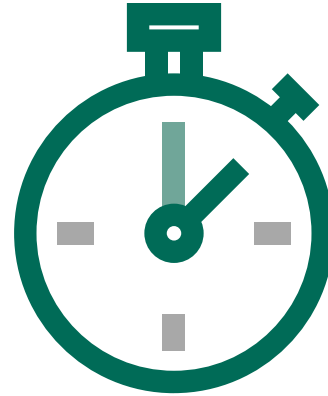
There is a lot involved, so the sooner you get started the better. Failing GDPR compliance will definitely do more harm than good. And if you're still in the non-compliance boat, once GDPR becomes law, you could find your organization facing hefty fines or irreparable reputation damage.

There are requirements defined in GDPR that provide directives on how you will be allowed to manage personal data, this includes everything from how data is collected to how it is store, and how it is used. This is an extremely wide scope, as you can probably see and expect, these

requirements will affect how personal data is identified and secured within your systems, the detection and reporting of breached personal data, and how your organization trains employees on data privacy.



Overcome GDPR Uncertainty with Globalscape



The climate surrounding global data privacy regulations is still extremely heated and uncertain, in spite of GDPR's May 25, 2018 enforcement deadline.



The risk factors are heavy burdens to bear during a time of uncertainty, but it's worth re-evaluating your perspective on data privacy and data security, **not only to meet GDPR regulations, but also to rebuild trust between EU residents and international companies.**



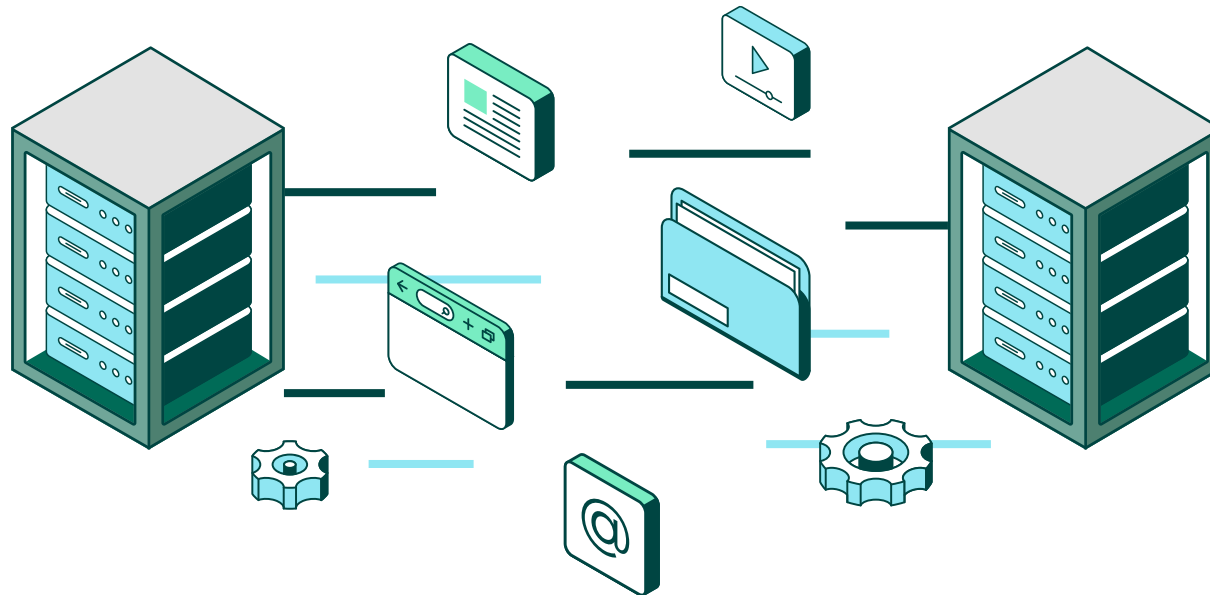
However, there is still time. You can prepare yourself for GDPR and any potential regulatory shifts with **a solution that will not only help you meet compliance, but also give you a competitive edge.**



Globalscape helps organizations **protect their sensitive data and IT infrastructure** in the most transparent and preventative way.



Enhanced File Transfer™ (EFT™) is Globalscape's award-winning MFT platform that was designed to manage data transparently, efficiently, and within the parameters of control and accessibility that you require.



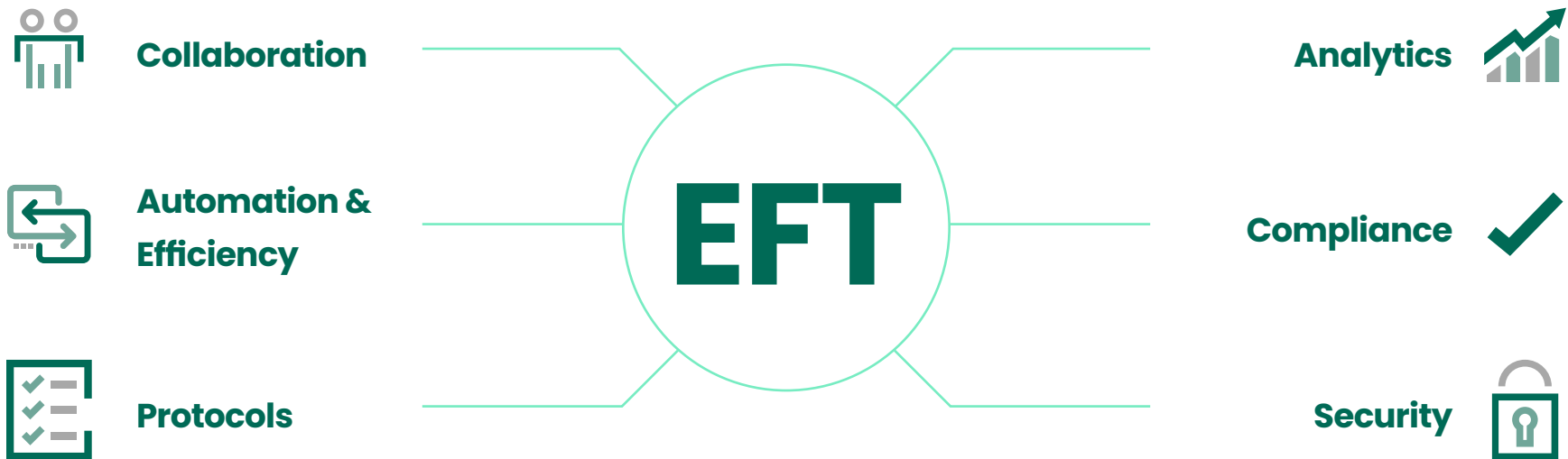


EFT provides enterprise-level security for collaboration with business partners, customers, and employees, while automating the integration of back-end systems.





Built-in regulatory compliance, governance, and visibility controls help keep your data safe, while outstanding performance and scalability help boost operational efficiency and maintain business continuity. Administration is easy, yet granular enough for complete control of your file transfer system.



With EFT, you can

- ✓ Use **industry-standard secure protocols** to secure your file transfers
- ✓ **Monitor** file movement and user activities on your network
- ✓ Create a **multi-layered security** solution for data storage and retrieval, authentication, and firewall traversal **with Globalscape DMZ Gateway®**
- ✓ Use **malware and IDP tools** to prevent malware from entering the network and prevent sensitive data from leaving **the network**
- ✓ Use **data wiping** to thoroughly delete data
- ✓ **Encrypt** stored data
- ✓ Securely access your **data on any device without the cloud**
- ✓ Merge or **replace legacy file transfers systems**
- ✓ **Automate workflows** and integrate systems



Don't be left in the dark, come May 25, 2018.

Globalscape is ready to work with you to develop a proactive data management strategy for securing all of your data transfers from any global location.

Contact us today to get your questions answered on GDPR and on your data management strategy.



Things You Need to Know – GDPR at a Glance



As a replacement to the data protection regulations, the European Commission was focused on developing a set of regulations that would not only simplify the regulatory environment, but also protect the privacy and personal data for all EU residents.

Listed below is a summary of the regulations that are set to replace the data protection directives:



Increased Territorial Scope

This requirement defines the stakeholders as any company that processes the personal data of subject residing within the EU, and extends the jurisdiction of GDPR. Company location does not matter. If your company manages or processes personal data for a resident within the EU, then your company is required to comply.



Penalties

Noncompliance can result in fines up to 4 percent of annual global turnover or €20 million (whichever is greater), which is the maximum fine imposed for a serious compliance violation e.g. not having a sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2 percent for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors —meaning 'clouds' will not be exempt from GDPR enforcement.



Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.



Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to “result in a risk for the rights and freedoms of individuals”. This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.

Data Subject Rights



Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.



Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.



Data Portability

GDPR introduces data portability – the right for a data subject to receive the personal data concerning them, which they have previously provided in a ‘commonly use and machine readable format’ and have the right to transmit that data to another controller.



Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically – ‘The controller shall [...] implement appropriate technical and organizational measures [...] in an effective way [...] in order to meet the requirements of this Regulation and protect the rights of data subjects’. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing.

Data Subject Rights (Continued)



Data Protection Officers

Currently, controllers are required to notify their data processing activities with local Data Protection Administrators (DPAs), which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs).

Instead, there will be internal record keeping requirements, as further explained below, and data protection officer (DPO) appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could result in a conflict of interest

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.