Wolters Kluwer

CT

ESSENTIAL COMPLIANCE INSIGHTS

The General Data Protection Regulation (GDPR): What Organizations Need to Know

By James Cusick

THE GENERAL DATA PROTECTION REGULATION (GDPR): WHAT ORGANIZATIONS NEED TO KNOW

The General Data Protection Regulation (GDPR) is the result of an effort by the European Parliament and other governmental bodies to strengthen data protection for those living in the EU, while also providing greater uniformity to existing data laws.

Approved in 2016 by the European Union (EU), GDPR overhauls and modernizes existing data laws, many of which date to an era before widespread Internet accessibility. One major change is that the guidelines in the existing data protection directive (Directive 95/46/EC) are non-binding. GDPR is, in fact, a "regulation" which needs to be complied with in certain circumstances.

Now that GDPR is in effect as of May 25, 2018, organizations need to know the impact of these changes and determine how to best navigate the shifting data protection landscape.

> GDPR AND ITS IMPACT

GDPR is the result of an effort by the European Parliament and other governmental bodies to strengthen data protection for those living in the EU, while also providing greater uniformity to existing data laws. Residents of the EU are gaining a greater measure of control over their data (and how it is used), by parties both inside and outside the EU. Meanwhile, the regulations are making data protection more uniform across EU member states, allowing for easier compliance from outside nations.

It should be noted again that GDPR is not a recommendation, but rather a law that governs the data privacy and protection of the EU citizenry.

GDPR stands in contrast to the EU-US Privacy Shield, an agreement between European Commission and the U.S. Government (formally approved in 2016), that set up a system where individual companies could be certified as having adequate data protection measures in place before transferring information. U.S. firms could self-certify (on a voluntary basis) by submitting an application to the Department of Commerce. While this agreement remains in place, the implementation of GDPR essentially renders it obsolete, making it an inadvisable choice for further investment.

CONTENTS

Privacy: a fundamental right for EU citizens

The notion of a right to privacy in the context of data is particularly well-defined in Europe. Unlike other regions where data protection is weaker or virtually non-existent, Europe has remained positioned at the vanguard on this issue. Public sentiment for vigorous data privacy protections is strong, one reason why the EU has moved to modernize and strengthen regulations. The change promises to be profound. Elizabeth Denham, U.K. Information Commissioner, calls GDPR "the biggest change to data protection law for a generation."

While this can be viewed as a net positive for EU citizens, the specter of tightened regulations has presented a whole host of legal and technical challenges for firms doing business in the EU. Effectively complying with these changes is a significant concern for many businesses, as EU leaders have introduced stronger sanctions and stricter enforcement in an effort to encourage close compliance. Should violations occur, regulators can now assess a fine of up to 20 million euros (21.4 million dollars) or four percent of the prior year's global turnover, whichever is higher.

> "Public sentiment for vigorous data privacy protections is strong, one reason why the EU has moved to modernize and strengthen regulations."

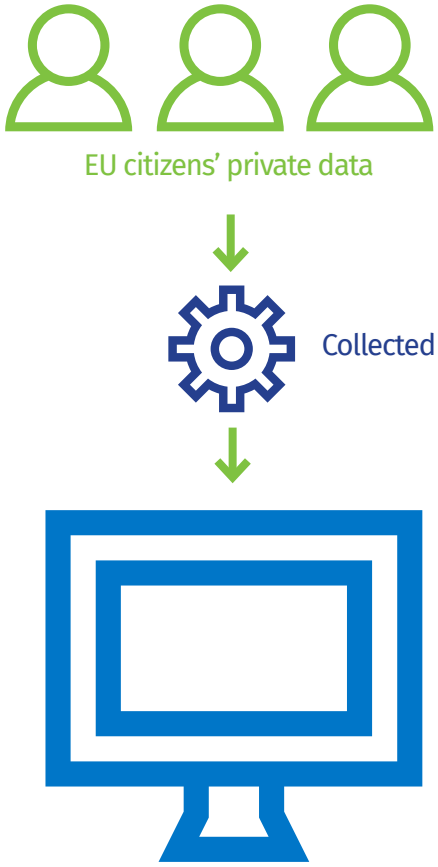
GDPR applies to organizations outside the EU

The legislation applies to any organization that handles, processes, and especially exports EU citizens' data outside the Euro Zone, even if that company is not based in Europe.

> *Example: A U.S.-based company with a website collecting personal data of EU citizens where that website is hosted outside the Euro Zone would be subject to GDPR rules.*

These provisions are uniform across all 28 EU member states and rise to a standard that is exacting enough to require a significant commitment of resources on behalf of compliant companies.

Example of U.S.-based Company Subject to GDPR Rules



Adding to the complexity, all 28 member states retain the power to add localized jurisdictional regulations governing data protection, so long as these regulations do not conflict with GDPR provisions. While this may help EU nations create regulations that are more relevant in home markets, it complicates things considerably from a compliance perspective. Companies need to invest in some form of monitoring or tracking of evolving local data privacy regulations in order to encourage full compliance.

Note: The UK and Switzerland have data protection requirements essentially in line with those found in GDPR.

Businesses, generally speaking, will require board-level support to enact many of these changes. Those firms that fail to address the challenges of GDPR risk not only significantly elevated sanctions but also reputational damage. On the positive side, implementation of GDPR is an opportunity for businesses to demonstrate how seriously they regard the challenge of modern data protection.

> GDPR REQUIREMENTS AND CONSIDERATIONS

Organizations seeking to meet the challenges posed by GDPR should be cognizant of the key changes. These changes include, but are not limited to, the following:

- **How personal data is defined.** The new definition is more comprehensive and can include anything from names, emails, social media posts, medical records, IP addresses or other metadata. This change reflects how modern firms collect information about consumers. Another key distinction: GDPR protects not only personal data attributes but information that can be used to infer attributes. For example, a person's race, gender, union affiliation, or other unique personal characterization are considered as personal data.
- **Profiling usage of personal data.** Under GDPR profiling of users through their interaction with a system or in the way a company analyzes their data comes under regulation. This means if typical user profiling tools are used in a non-anonymized manner, restrictions can apply. This is also true of certain data analysis where aggregation is not used.

GDPR Personal Data Protection Attributes

- **The rules governing consent.** GDPR requires that consent can be withdrawn as easily as it's given, and that requests for consent must be clear, intelligible, delivered in plain language and distinguishable from other materials.
- **The right to be forgotten.** GDPR allows EU residents to request that their data be erased, while also halting the further dissemination of that information. The right to third-party data processing can also be revoked. One caveat: Data controllers must weigh these requests for erasure against "the public's interest in the availability of the data."
- **The right to be informed.** In order to comply with GDPR mandates, businesses must be transparent as to how they use the data they collect. They must also provide fair processing information, typically via use of a privacy notice.
- **Lawful processing.** Businesses must have a lawful basis to process personal data.
- **The right to data access.** EU citizens retain the right to discover how their data is being used, including where and to what purpose. They may also request a copy of stored data, which must be furnished in an electronic form free of charge.
- **The right to data portability.** Citizens may transmit their data between multiple controllers.
- **The right to breach notifications.** Such notifications are now mandatory in EU countries where security lapses could result in "a risk for the rights and freedoms of individuals." This alert must be issued within 72 hours.
- **Transferring data internationally.** Certain conditions must be satisfied before personal information can be transmitted beyond the EU.
- **Privacy by design.** Data protections must now be included during development processes, not tacked on as an afterthought.

Additionally, GDPR introduces several new privacy requirements that depend on certain parameters being met. For example, companies must appoint a Data Protection Officer (DPO) if they are a public authority, if they carry out systematic monitoring on a wide scale, or if they process criminal data on a large scale.

> "Organizations with more than 250 employees must also maintain additional internal documentation of data processing that involves sensitive or high-risk elements. This includes data regarding criminal offenses and other specialized categories."

Organizations with more than 250 employees must also maintain additional internal documentation of data processing that involves sensitive or high-risk elements. This includes data regarding criminal offenses and other specialized categories.

Finally, organizations struggling to meet the new data privacy mandates should be able to conduct Data Protection Impact Assessments. These are tools that help groups identify how to best safeguard information and mitigate any developing problems at an early stage.

› TAKEAWAYS: WHAT COMPANIES NEED TO KNOW ABOUT GDPR IMPLEMENTATION

In order to fully prepare for these most significant changes and compliance challenges related to GDPR, organizations should take note of a few key takeaways.

- First, it must be noted that GDPR applies to any organization (including U.S.-based groups) processing certain types of EU citizen data under specific circumstances, regardless of whether that company has a presence in Europe.
- Next, non-compliance penalties have become much stiffer—up to 20 million euros (24.4 million dollars) or four percent of the previous year's global turnover, whichever figure is higher. Organizations must also demonstrate exactly how they are complying with GDPR mandates.
- Data breaches must be reported within 72 hours if that breach represents a threat to the rights or freedoms of an individual.
- Some companies, depending on classification and other variables, may be required to hire a Data Protection Officer.
- GDPR went into effect on May 25, 2018.

By focusing on these key takeaways, organizations can help ensure that they are well-positioned to meet compliance demands and escape potential financial or reputational damages.

Data breaches must be reported within 72 hours if that breach represents a threat to the rights or freedoms of an individual.

› CONCLUSION: READYING FOR GDPR COMPLIANCE

GDPR represents the single largest shift in data privacy policy in a generation. As such, it presents a significant challenge for organizations seeking to satisfy compliance mandates.

If you haven't already, start planning now and seek to develop "buy-in" from key members of your organization. Because satisfying GDPR's new data protection provisions may require drafting a new set of procedures, large organizations could see significant implications with regard to budgeting, governance, IT, communications, and so on.

You should also be aware that GDPR regulations will not have a uniform impact on all organizations or on every part of an organization, as the type of data that's handled and other variables can change how and when regulations apply. Because of this, map out the areas where GDPR will have the most impact on your organization and dedicate resources accordingly.

With a comprehensive plan, organizational leaders can help ensure they remain compliant with GDPR mandates—while avoiding stiff penalties and reputational harm.

> ABOUT THE AUTHOR

James Cusick

Chief Security Officer & Director of IT Operations

James Cusick is the Chief Security Officer & Director of IT Operations. He is responsible for systems planning, IT Operations, Infrastructure Services, Product Support, and Information Security at CT Corporation. Previously, James led software engineering teams for CT, creating large scale B2B applications. Prior to that, he held various technical leadership roles at AT&T, AT&T Labs, and Lucent's Bell Laboratories' Software Technology Center. He is a member of the IEEE and a current Project Management Professional. James is a graduate of both the University of California at Santa Barbara and of Columbia University in New York City.

LEARN MORE

To learn more about how CT can help you better manage your compliance requirements, contact your CT representative or call 855.316.8948 (toll-free U.S.).

855.316.8948 www.ctcorporation.com