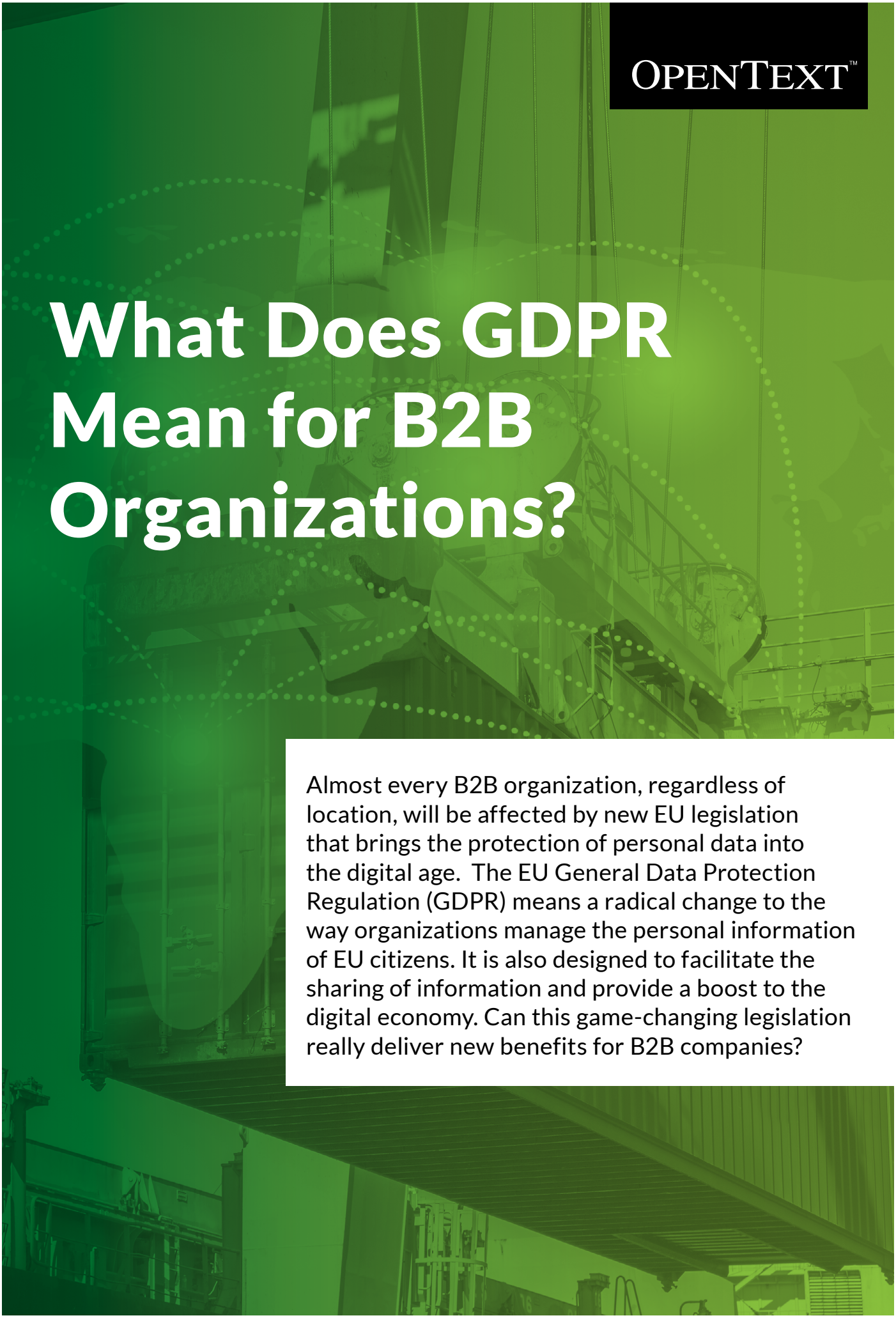
OpenText™

What Does GDPR Mean for B2B Organizations?



Almost every B2B organization, regardless of location, will be affected by new EU legislation that brings the protection of personal data into the digital age. The EU General Data Protection Regulation (GDPR) means a radical change to the way organizations manage the personal information of EU citizens. It is also designed to facilitate the sharing of information and provide a boost to the digital economy. Can this game-changing legislation really deliver new benefits for B2B companies?



OPENTEXT™

Table of Contents

GDPR: Cutting Red Tape 3

The 'Single View of Customer' on Steroids 3

GDPR and Electronic Communication 4

GDPR and the Supply Chain 5

Preparing for the GDPR 5

Introduction



The premise of GDPR is simple: If you collect, manage, store, and share personal data on EU citizens, you now have much greater privacy and data protection obligations. You must ensure – and be able to demonstrate – that you have taken the technical and operational measures necessary to ensure that personal data is completely secure, both at rest and in transit. You must remove personal data from your systems at the earliest possible point or when requested by the person whose data it is, unless there is a legally defensible reason not to comply with their request.

For B2B companies, it becomes essential that you know who owns the data and where it is at all times. Personal data held within your supply chain is likely to remain your responsibility. You need to know if your suppliers and customers have the right to hold the data and if the way they are transmitting and sharing data complies with the regulation. If you are using cloud services, you need to know where data is held and, if not within the EU, that the country's data protection laws are in compliance with GDPR. You need full transparency across the lifecycle of all the personal data for which you have full or partial responsibility.

Meeting the obligations of GDPR is going to be extremely challenging for many organizations. Within the B2B environment, companies that have built up internal information silos over several years and those that do not have visibility across their supply chain must now quickly find a way to organize this data that is sensible, transparent and, most of all, secure.

Or, to put it another way, organizations have until May 28, 2018, to achieve what most have been working towards anyway: Complete control and visibility of the data they hold in a way that allows them to apply greater analytics and deliver the level of insight that leads to better customer experience.

GDPR: Cutting Red Tape

Although the GDPR places data protection obligations on companies, it also reduces a great deal of the administrative burden. The legislation harmonizes the previous laws of all 28 EU member states. An organization now only has one regulation to deal with and a single supervisory authority. This is designed to make it simpler and cheaper to do business within the EU. The European Commission suggests that this one change will bring benefits of saving about 2.3 billion euro per year[1].

The law makers have gone further to suggest that the GDPR provides a platform to boost the 'Digital Single Market' and technical innovation by providing a single technology-neutral set of rules for basing the development of new digital products and services. One example of this is 'data portability,' which makes it easier for customers to move their personal data between service providers[2].

The 'Single View of Customer' on Steroids

To achieve GDPR compliance means extending the concept of the 'single view of customer.' Traditionally, the single view of customer was about bringing all the information an organization held on a customer together. It now requires a complete 360-degree view of all individuals who interact with your company.

That is incredibly valuable. If you can identify and gather all the information you have on each individual, you are able to conduct far deeper analysis. By clearly seeing how and why data is being used – and by being able to examine common traits between data sets – you gain much greater insight into the actions of customers across touch points.

For B2B companies, the challenge is the amount of data and the number of sources with which you are dealing. To gain end-to-end visibility of personal data on any individual you will need to have access to, and be able to bring together, structured data such as product and service information from multiple systems in your organization and beyond. You need to be able to collate unstructured data, such as website behaviours like click through, searches and registrations; social behaviours such as social media interactions; and communications with your organization such as email, fax, call center audio tapes, or mobile app usage.

To comply with the GDPR, large organizations will increasingly need to implement some type of Enterprise Information Management (EIM) solution – such as OpenText™ Content Suite 16. This can allow visibility of all information in whatever format – that is being created, processed, stored, and shared. By delivering transparency across the lifecycle of personal data, EIM can help build customer loyalty and increase revenue by better identifying and managing customer interactions and providing a more personalized customer experience across channels.

GDPR and Electronic Communication

The GDPR imposes the same stringent regulation on data in transit as it does for data at rest. The legislation states: "Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing"[3]. It clarifies the point by saying 'this could, for example, include preventing unauthorized access to electronic communications networks[4]'.

While primarily designed to address the hacking of computer systems, it is clear that this GDPR provision also covers electronic communications in all its formats, including VoIP, fax, and email. It is also important to understand that the GDPR does not stand apart from data protection legislation covering paper-based communications. Wherever personal data is being transmitted or shared, every effort has to be made to ensure that it is completely secure in transit and only available to authorized individuals at either end.

It is also sensible for companies to look for electronic communication systems that minimize the instances of personal data created within the organization. For example, an enterprise, digital fax solution - such as OpenText™ RightFax™ or OpenText™ Fax2Mail™ - enables the end-to-end processing of business documents such as purchase orders and invoices so that data go directly from the company's ERP system to the customer via a secure fax transmission. Inbound faxed documents can be directly ingested into the ERP system for immediate processing, eliminating additional instances of the content in other hands or systems. In addition, organizations may consider bringing voice, messaging, email, and electronic fax together to create an omni-channel communications approach with OpenText™ Notifications, which helps manage messaging and the use of personal data in a single system with a holistic view of business and consumer communications.

GDPR AT A GLANCE

WHAT IS THE GDPR?

The General Data Protection Regulation (GDPR) is EU-wide legislation that covers the management of personal information by private and public companies. It comes into force on May 28, 2018.

WHY WAS IT CREATED?

Previous data protection legislation did not provide the correct level of information security for the new digital economy. The GDPR is designed to address this shortcoming and harmonize the law across all EU countries.

WHAT DOES IT COVER?

It covers all structured and unstructured data that an organization holds on EU citizens. The scope of the legislation includes how the data is managed, stored, and transmitted.

WHO DOES IT AFFECT?

It affects any organization – public or private – that holds or processes personal information on EU citizens.

WHAT ABOUT NON-EU COMPANIES?

The legislation is universal so any company dealing with EU citizens must comply with the GDPR.

WHAT ARE THE PENALTIES?

Fines for non-compliance can be as much as 20 million euro or four percent of turnover – whichever is greater.

GDPR and the Supply Chain

Today, almost every organization has its own – or is part of – extended supply chains. The GDPR places responsibility to ensure that you have considered compliance in everything surrounding the use of personal data both within the organization and beyond. Not only does it contain provisions for the passing of personal data to 'sub-processors,' it requires complete detail and understanding of how data flows across the entire supply chain to ensure organizations are fully accountable for the data in their trading networks.

Companies are now responsible for demonstrating that they have taken all the technical and organizational measures, including how they sign-up new suppliers and connect to new customers, to ensure that personal data is never exposed or misused as it is stored and shared across the supply chain. A common platform for conducting B2B transactions, such as the OpenText™ Trading Grid™, provides secure infrastructure for sharing and managing personal data between trading partners of all technical levels and locations. It is a basis for the supply chain visibility required to ensure you have the transparency of personal data that the GDPR requires.

The GDPR puts a greater emphasis on effective data governance. It promotes a standard approach for the protection of personal data and encourages the adoption of standards and common platforms for the storage, management and transmission of that data. Adopting a B2B integration infrastructure allows an organization to ensure it manages and shares data using industry standards in data structure and security, while delivering visibility across supply chain transactions that facilitate the process of demonstrating compliance.

Preparing for the GDPR

To prepare for the GDPR, organizations must consider every aspect of how they work with personal data. This applies to non-EU companies as much as those within the EU. There are two good reasons for this: First, almost every company will have EU customers or suppliers. Secondly, the GDPR is the most far-reaching piece of data protection ever created. Once you implement it to meet the need of personal data of EU citizens, it is likely to become a template for all personal information. It makes no operational or economic sense to handle personal data for different people and locations differently unless there are good legal or business reasons.

The most important aspect is to introduce Security-by-Design as a foundational element of everything you do. Compliance must be built from the ground up, technically and operationally, rather than thought of as an add-on. The systems you put in place to gain granular control of personal data are going to have to span across your supply chain to connect suppliers and customers. OpenText has had Security-by-Design at the core of the development of its portfolio of solutions for many years, ensuring it can ease the process towards meeting your GDPR obligations.

The key is not to see this as an exercise in regulatory compliance but an investment in digital transformation. The result of your efforts will be the most valuable asset a modern company can have: complete insight into its business operations and the demands and behaviors of its customers.

For more information on how **OpenText** can help, visit www.opentext.com/gdpr

References

1 http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
2 http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
3 http://www.privacy-regulation.eu/en/r39.htm
4 http://www.privacy-regulation.eu/en/r45.htm

SECURITY OBLIGATIONS INCLUDE:

- *Conducting a Privacy Impact Assessment (PIA) to understand the current situation*
- *The pseudonymization and encryption of personal data*
- *The ability to ensure the confidentiality, integrity, availability, and resilience of processing systems and services*
- *The availability and access to personal data in a timely manner*
- *A process of regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing*

www.opentext.com/contact

Copyright ©2017 Open Text. OpenText is a trademark or registered trademark of Open Text. The list of trademarks is not exhaustive of other trademarks. Registered trademarks, product names, company names, brands and service names mentioned herein are property of Open Text. All rights reserved. For more information, visit: http://www.opentext.com/2/global/site-copyright.html (05/2017) 07191EN