White Paper: Global Data Protection Regulation (GDPR)

Key Facts about GDPR

Authors:
Gia Fisher, CISO, Clarus Tech Partners, Inc., Global IT Partner, EMEA & The Americas Cyber Security Solutions/Security Solutions/Analytics

Christine Baird, CEO, Clarus Tech Partners, Inc., International Business Solutions

16 February 2018

White Paper: Global Data Protection Regulation (GDPR)

Key Facts about GDPR

WHAT IS GDPR?

GDPR is the new European Union's (EU) General Data Protection Regulation law and will bring about the greatest change to European data security in 20 years. The GDPR will make major changes to Europe's privacy laws and will replace the outdated Data Protection Directive from 1995.

GDPR preserves many of the principles established in the former Directive; however, GDPR is much stricter and affects organizations on a global scale.

WHEN DOES GDPR TAKE EFFECT?

Companies that collect data on citizens in EU countries will need to comply with the strict new rules that protect consumer data by May 25, 2018.

WHY GDPR?

With the rise of data breaches occurring not only within "Business to Business" but also "Business to Consumer" organizations, this has prompted regulatory entities to revise existing standards in place that would address and expand tighter protection of the organization's data, and their customer's data.

The GDPR gives individuals greater control over their personal data and imposes many new obligations on organizations that collect, handle, and/or analyze personal data.

WHAT CONSTITUTES "PERSONAL DATA"?

Other countries and organizations may define personal data and information in different ways; however, GDPR defines personal data to include any information related to a person that can be used to directly or indirectly identify the person – such as a name, a photo, racial or ethnic data, an email address, bank details, posts on social networking websites, political opinions, health and genetic information, a computer IP address, and more.

GDPR focuses on the collection, processing, and movement of this personal data.

HOW DOES GDPR AFFECT MY ORGANIZATION?

If your company processes personal data or sells goods or services to citizens in EU countries, then you will need to comply with GDPR. The GDPR not only applies to organizations located within the EU but also to organizations outside of the EU if a company offers goods or services to, monitors the behavior of, or holds personal data of EU citizens.

The territorial scope of the new regulation is quite vast, in that GDPR regulations apply to any business that processes personal data on EU residents, regardless of the physical location of the business. So that means you could have no offices or staff in any European Union country, and even no customers in the EU. But, if your business in any way processes and stores personal data on EU residents or customers, it falls under the jurisdiction of GDPR.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

The GDPR penalties for non-compliance are steep – possible audits and fines of up to €20 million (about $24 million USD) or 4 percent of your company's annual global revenue, whichever is greater. This is the maximum fine that can be imposed for the most serious non-compliance and a tiered fine structure will be imposed on companies for lesser non-compliance offenses.

WHAT ARE THE GDPR PERSONAL DATA RIGHTS?

GDPR includes the following Personal Data Rights for EU citizens:

- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object
- not to be subject to automated decision-making including profiling

Organizations will need to have a lawful basis for processing personal data and include this information in Privacy Notices plus have procedures in place when an EU citizen requests access to their data.

WHAT ARE SOME OF THE DETAILS OF THE PERSONAL DATA RIGHTS?

Some of the Personal Data Rights or “Data Subject Rights” include:

- **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. The controller will be required to 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.
- **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 used and machine readable format” and have the right to transmit that data to another controller.
- **Breach Notification** – Under the GDPR, breach notification will become mandatory 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 and controllers will also be required to notify their customers “without undue delay” after first becoming aware of a data breach.

IN WHAT INDUSTRIES DO DATA BREACHES TYPICALLY OCCUR?

Data breaches occur in all industries, including the Real Estate and Financial sectors.

For example, the Real Estate sector needs to address data collected by:

- Landlords of their tenants
- Real Estate companies of their buyers and sellers
- Architects & Developers of their clients & vendors
- Asset & Fund Management companies of their investors
- Hotels of their guests
- Car parking lots of their customers/tenants
- Office/Retail/Industrial buildings of their tenants
- Family Offices of their investors

Financial Services firms, such as mortgage companies, banks, REITs, and financial institutions, also need to address personal data in their:

- **Legacy Systems**
  Financial institutions will need to ensure they have the technical functionality to implement the requirements of GDPR.

- **Financial Services IoT Platforms**
  Connected devices and the data collected through them that generate personal data used to predict personal preferences and behaviors and build customer profiles so that services are tailored to customer demands and needs.

HOW CAN MY ORGANIZATION BE IN GDPR COMPLIANCE?

To be in GDPR compliance, all organizations should implement a GDPR Compliance Readiness Program.

GDPR implementations should focus on having in place the right data governance structures, policies and operational procedures, and monitoring, detection and response processes.

AIM – Assess, Implement, and Maintain

- Assess Your Data
- Implement the GDPR Compliance Program
- Maintain the Data Protection Program

The three key personnel roles for GDPR compliance in every organization, Data Controller, Data Processor and Data Protection Officer (DPO), should be identified and trained.

Many organizations may not reach complete compliance by the May 25, 2018 deadline; however, organizations can start the process now to demonstrate that they are working on reaching a minimum compliance standard.

The organization's board and executive management must make GDPR compliance a top priority and set a sense of urgency.

Since GDPR extends beyond cyber security, it is also important for Legal, IT, Security, Finance, HR, Operations and all the organization to work together to achieve compliance. GDPR is a team effort and everyone within an organization has a responsibility to protect data and understand and get ready for GDPR compliance.

FOR MORE INFORMATION

Clarus Tech Partners and their partner Legal, IT, CyberSecurity and Compliance team offers comprehensive GDPR Compliance Readiness solutions to help your organization assess your current data compliance exposure, build a plan, implement the processes, and maintain and control ongoing GDPR compliance.

For more information, see **www.ClarusTechPartners.com**.

For a full description of the EU GDPR law, see **www.eugdpr.org**.