Grant Thornton

An instinct for growth™

General Data Protection Regulation (GDPR)

Should you be worried about GDPR?

General Data Protection Regulation will **affect all companies and every business unit** in your organization that process personal data of European Union citizens.

The new EU General Data Protection Regulation

In a nutshell:

The General Data Protection Regulation (GDPR) comes into force in May 2018.

It is the latest development in the current EU agenda to safeguard its citizens and their private information introducing new rights for individuals and strengthens existing protections. This new regulation imposes stricter requirements on all business activities involving data. Whether you are a data controller or a data processor, the GDPR will have a significant impact on your business and the clock is ticking. The GDPR was implemented through EU Regulation 679/2016 and supersedes EC Directive 46/95.

Regulatory changes require prompt consideration and critical assessment by organisations in order to understand their effects on business operations. Amended business practices, supported by IT systems and operational processes will be required to achieve compliance with this new regulation.

Are you Ready?

Fines for data breaches and non-compliance with EU regulation increased significantly**, up to €20 million or 4% of group turnover**, whichever is greater.

Organisations will have to move quickly to avoid potentially large fines for non-compliance.

Who is affected

The GDPR **will affect every business** and public body that processes the personal data of **EU residents**, including:

- Every Employer
- Every business that process the personal data of EU individuals on behalf of other business.

The new **regulation will impact every organisation and division** of the organisation that holds or process European personal data both inside and outside of Europe.

Indicatively, the GDPR affects the following divisions inside an organisation:

- IT
- Human Resources
- Marketing
- Payroll
- Finance
- Organosis

Key changes under the GDPR

Organisations need to start responding to the new requirements to ensure that they are ready to comply with the new Regulation when it comes into force in the spring of 2018.

Key changes

Imposition of large scale penalties	Data protection authorities will be able to impose substantial fines of **€20 million or up to 4% of global annual turnover** of the respective company, whichever is the greater.
Global Scope Alignment	Adoption of a single set of rules for all on data protection, directly applicable in all EU Member States. There will be **no** opportunity for local transposition. The requirements will attach to the data of EU citizens, not just to companies based in the EU, making it the first global data protection law.
Enhanced Transparency Obligations	Increased transparency obligations. Controllers must inform and remind users of their rights, as well as documenting the fact that they have reminded them of their rights. Customers will now have the right to request a Financial Services institution provide them all the details of all the information held about them.
Data Protection Impact Assessments (DPIAs)	The regulation requires businesses to carry out DPIAs where the processing is likely to result in a high risk to the rights of individuals taking into account the nature, scope, context and purposes of the processing.
Data Protection Officer (DPO) Appointment	Data controllers and processors must appoint a data protection officer. The data protection officer must have expert knowledge of data protection law and practices.
Data Breach Notification Obligation	The regulation introduces requirements to report all personal data breaches falling within the scope of GDPR to the supervisory authorities **within 72 hours** and/or to the affected data subjects without undue delay.
Internal Data Inventories Requirement	The GDPR will require data controllers to maintain a record of all categories of processing activities under their responsibility. This 'inventory' must contain information such as the purpose of processing, the type of data processed, etc.
"Explicit" Data Subject Consent	Businesses must be able to demonstrate that the consent of the data subject was presented in a manner which is clearly distinguishable, in an easily accessible form and using clear and plain language.
New Data Erasure Rights	According to the new regulation, users can also demand that their data be erased. The GDPR 'right to be forgotten' clause will require an institution to remove all relevant Customers' data from all its systems – upon request.
Optimized Governance Structure	Increased responsibility and accountability on organizations to manage how they control and process personal data. The GDPR demands from organizations to implement adequate and tailored Data Protection control frameworks and risk management.
Security by Design & Risk Consideration	The GDPR suggests specific security actions that would be considered appropriate to the risk, such as: encryption of personal data; The ability to maintain confidentiality, and a process for regularly testing, assessing and evaluating the effectiveness of the measures.
Increased Territorial Scope & Cross-Border Transferal	The GDPR will apply to businesses established outside the EU who offer goods, services or monitor the behavior of a subject within the EU. It also applies whether or not the data processing takes place outside the EU.

How Grant Thornton can help you

It's good to know what's just around the corner. At Grant Thornton, we bring you fresh perspectives and insights on the issues facing your organisation tomorrow and today.

We have a strong presence and influence within the market to ensure that the challenges that our clients face are being represented.

Our team can help you navigate the challenge by taking an holistic and integrated approach to a complex issue, working with you to identify and implement practical solutions which are appropriate for your business.

Our services include, but are not limited to:

Preparation Phase

- assessing your current organizational data architecture and GDPR readiness
- assessing your organization's data protection training needs
- building a roadmap for implementation of appropriate regulatory and compliance architecture
- conducting Data Privacy Impact Assessments (DPIAs)
- assessing your remediation activities

Implementation Phase

- assist to draft or update appropriate policies and procedures to ensure compliance with GDPR
- ensuring your data risk management is integrated into your overall risk management structure
- performing data flow mapping
- ensuring the data protection officer is correctly positioned to fulfil the obligations of that role
- helping you develop a data breach response action plan

Permanent Monitoring Phase

- support and guide data protection officer to fulfill his role
- frequently report to management aiming to provide assurance to your key stakeholders, internal and external
- monitoring developments and update top management accordingly

Being ahead of new developments

As one of the major global consulting organisations Grant Thornton is at the leading edge of standards setting and regulation. Grant Thornton services are addressed to all entities regardless of size or activity and are tailored to their specific needs. We have professional experts in several areas and sectors such as Public sector, Financial services sector and Energy Sector who possess knowledge and experience that bring valuable insights to your business.

Contact Us

Our specialised advisory team which combines IT business consulting, Financial services professionals, business risk and cyber-security experts, target in the provision of integrated services in order to create, protect and enhance value in your organisation in line with the new GDPR.

Athina Moustaki
Partner, Financial Services
E athina.moustaki@gr.gt.com

Michalis Rodakis
Partner, Operational Advisory Services
E michalis.rodakis@gr.gt.com

Kostas Poulos
Partner, ITBC Services
E kostas.poulos@gr.gt.com