Grant Thornton

Risk

Regulation

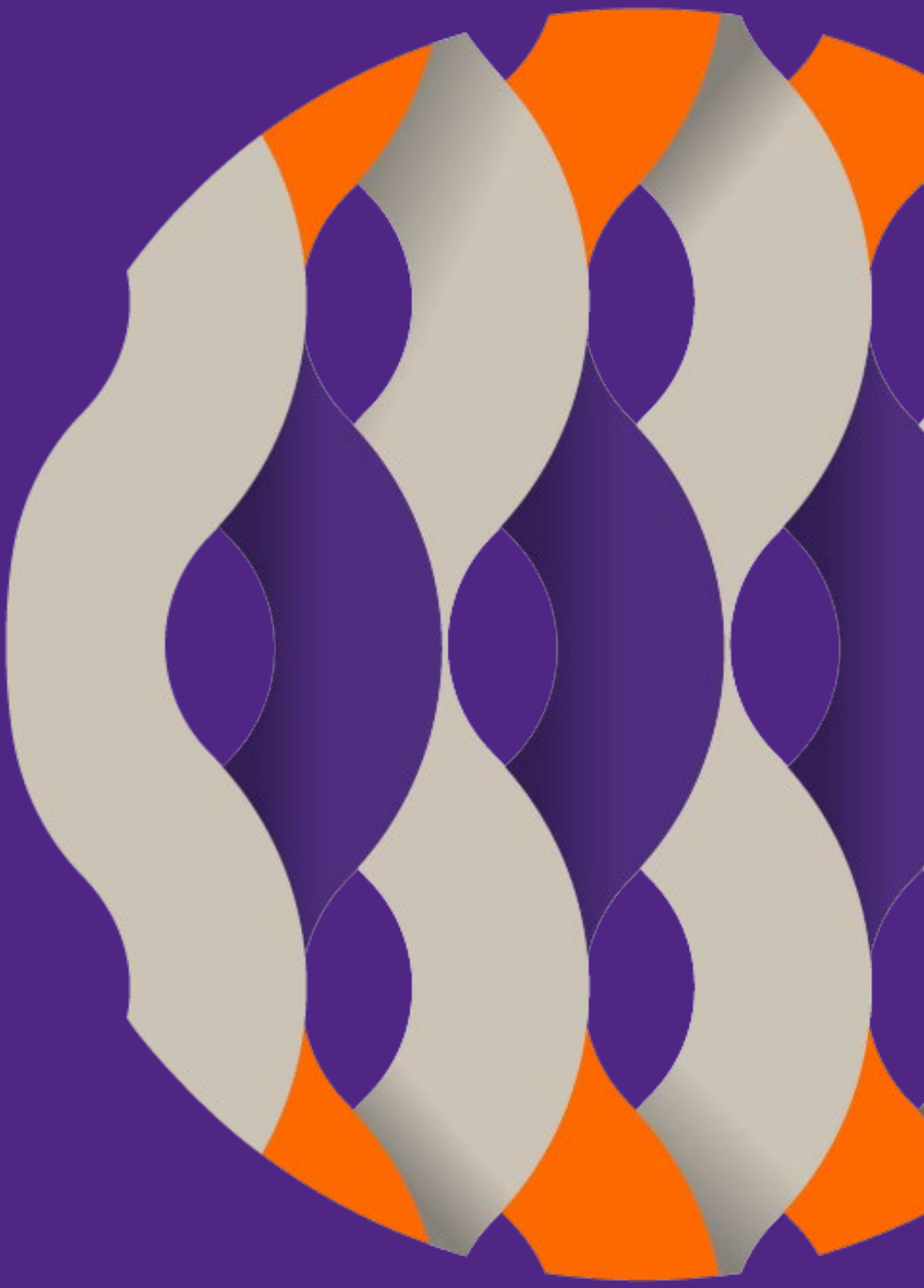
Cyber security

The General Data Protection Regulation (GDPR)

Preparing your business for the GDPR

Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules - not just for governments but for private companies.

- Bill Gates



What is the GDPR and what does it change?

The General Data Protection Regulation (GDPR) is the European Union's (EU) new data protection law came into effect on 25 May 2018.

Implemented throughout the EU, it governs all businesses operating within the union and embeds a more consistent approach to data protection. Companies that trade with EU-based businesses are also being impacted and need to know what's has changed and how to comply.

Penalties for non-compliance can now be up to €20 million or 4% of annual global turnover – whichever is greater.

So why is data protection legislation transforming?

Since 1995, the Data Protection Directive (Directive 95/46/EC) has determined how individuals' personal data is protected within the EU. However, since its inception there have been vast developments in the sophistication and scale of data creation and gathering – for example through the emergence of social media, cloud computing and geolocation services. As the directive predated these developments, it was no longer suitable to govern the current data landscape; in fact it has been refreshed to address modern privacy concerns and to facilitate consistency across the EU. This is why the GDPR was set up.

The new regulation introduced a huge range of changes. Underlying this shift is the EU's ongoing agenda to safeguard its citizens and their private information. The GDPR has now established new rights for individuals, strengthening current protections by applying stricter requirements to the way businesses use personal data. If they fail to comply, the sanctions will be significantly large.

What this means for your business

The GDPR is a valuable opportunity to understand your business' data and use it more effectively. However, it requires strict adherence to new regulations and a clear understanding of the changes made in order to avoid large penalties.

First, it's critical to be aware that the GDPR supersedes all other data protection acts, and that it increases businesses' obligations around data protection and their accountability for failure. It also applies across the full spectrum of data engagement – from the collection of personal data through to its use and disposal. Your organisation needs to embed policies and procedures to ensure that it monitors its GDPR controls and documents its compliance.

The GDPR applies to organisations of any size that process personal data. Whatever the nature of your organisation, the GDPR surely has a substantial impact.

All global organisations, both those in the EU and those that trade with EU companies, are required to comply with the GDPR, since its implementation in May 2018.

Understanding the core changes

The GDPR has introduced wide-ranging changes that require thorough understanding, internal stakeholder acceptance, appropriate preparation and implementation across the whole business. To provide an overview, we've addressed some of the key changes here.

Better rights for data subjects
The largest shift is that individuals are benefitting from greatly enhanced rights, for example, the right to object to certain types of profiling and automated decision-making. Consent requirements have also become more stringent. Consent must be explicit and affirmative, it must be given for a specific purpose and it must be easy to retract. Individuals can also request that personal data is deleted or removed if there isn't a persuasive reason for its continued processing.

Increased accountability
Organisations have far more responsibility and obligation. They need to publish more detailed fair processing notices – informing individuals of their data protection rights, explaining how their information is being used and specifying for how long. The new regulation also embeds the concept of privacy by design, meaning organisations must design data protection into new business processes and systems.

Formal risk management processes
Organisations must formally identify emerging privacy risks, particularly those associated with new projects, or where there are significant data processing activities. They must also maintain registers of their processing activities and create internal inventories. For high-risk data processing activities, Data Protection Impact Assessments (DPIAs) are mandatory and it is also compulsory to appoint a Data Protection Officer (DPO).

Reporting data breaches
As part of the drive for greater accountability, data breach reporting has become stricter. If a significant data breach occurs, it must be reported to the Data Protection Commissioner within 72 hours and, in some cases, to the individual affected without undue delay.

Significant sanctions
Penalties for non-compliance with the GDPR have increased considerably, up to €10 million or 2% of annual global turnover (whichever is greater) for minor or technical breaches, and €20 million or 4% of turnover for more serious operational failures.

Data processing requirements
The regulation also imposes new requirements on data processors, and includes elements that should be addressed contractually between data processors and data controllers.

Key features of the GDPR:

Enhanced rights for data subjects – the right to object to certain types of profiling and automated decision-making, and to request that unnecessary personal data is deleted.

Enhanced obligations for organisations – such as publishing detailed fair processing notices to inform individuals of their data protection rights, the way their information is used and for how long.

Stringent consent requirements – consent must be explicit, freely given for a specific purpose and easy to retract.

Stricter breach reporting – significant data breaches must be reported to regulators within 72 hours and sometimes the individual, too.

Increased privacy impact assessments – organisations must formally identify emerging privacy risks, particularly for new projects.

Privacy by design – organisations must design data protection into new and existing business processes and systems.

Increased record keeping – organisations must maintain registers of the processing activities they carry out, with mandatory DPIAs for high-risk data processing.

Significant penalties – the potential size of fines for non-compliance will be considerable, reaching €20million or up to 4% of turnover, whichever is greater.

Appointing DPOs – appointing a data protection officer is mandatory for many organisations.

Wider regulatory scope – the new regulation applo both the data controller and the data processies tor.

How to prepare your business

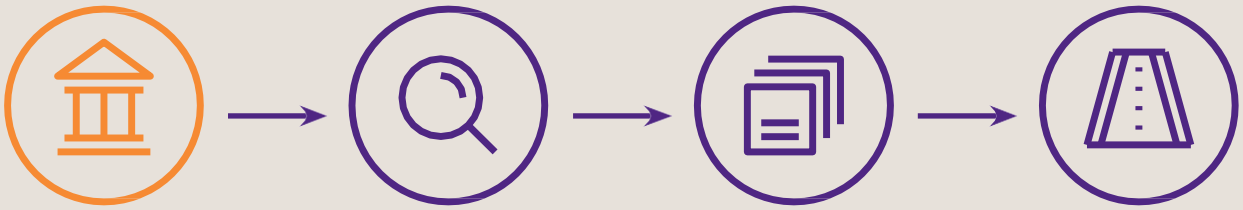
The legal landscape of data protection is evolving rapidly, and presenting challenges for businesses, government and public authorities. If your organisation is consumer-facing, online, in the financial services sector or in possession of sensitive personal data it may be particularly affected.

Businesses need to scrutinise the regulatorions and understand how they shall be affecting your business operations. Bear in mind that the impact of GDPR isn't confined to a specific area of your business – it will require business-wide adoption of a more process-orientated approach.

It's likely you'll need to continously amend your business practices to be compliant with this regulation, and implement new controls.

So where should you start?

We've created a simple visual, below, to help structure your approach to achieve compliance.



GDPR

- Understand the key changes this legislation will bring

Data protection quick check

- Assess your organisation's current data architecture, processes, and risk and compliance controls

Audit results and analysis

- Identify the current data risks in your business
- Review how well equipped your business is for the GDPR

Implementation roadmap

- Develop an implementation roadmap that embeds suitable regulatory and compliance architecture
- Ensure the plan is realistic and achievable for your organisation

Implementation

- Appoint a trusted advisor to:
  - identify and document data processing activities
  - carry out data impact assessments
  - develop a data breach response action plan
  - implement ongoing data protection processes.
- Write a detailed data protection policy and define a standard that ensures your business will meet the GDPR
- Where necessary, appoint a data protection officer and/or a data protection management system for ongoing control

Measure data protection effectiveness

- Undertake a GDPR FIT/GAP analysis or ISO 27001 FIT/GAP analysis – this is an assessment of the effectiveness of your GDPR efforts

Continuous improvement

- Hold regular GDPR audits and Data Privacy Impact Assessments
- Ensure data risk management is integrated into your overall risk management structure
- Regularly review your organisation's data protection training needs

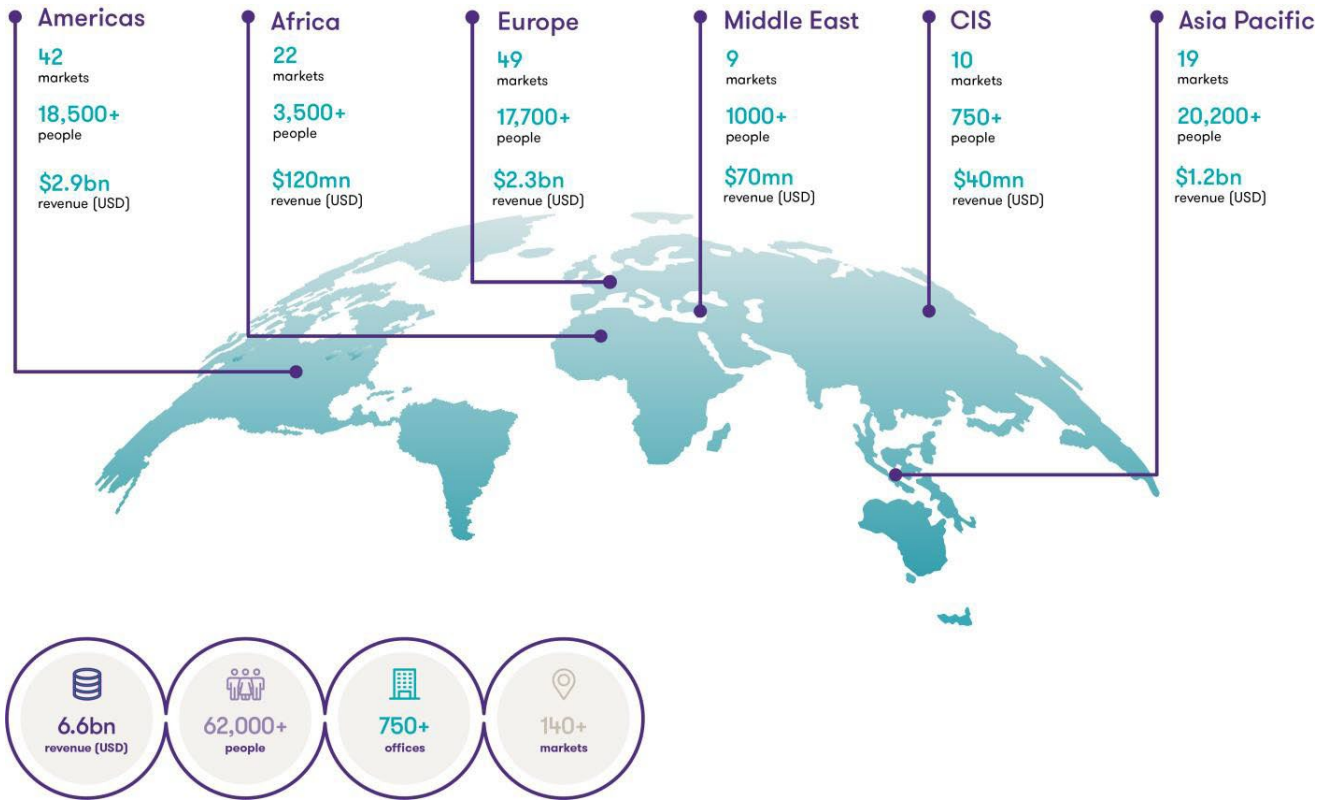
Grant Thornton International

Grant Thornton Malta is a member firm of Grant Thornton International

Grant Thornton International Ltd is a not-for-profit, non-practising, international umbrella membership entity. It is organised as a private company limited by guarantee, not having a share capital, incorporated in England and Wales and does not provide services to clients. Services are delivered independently by the Grant Thornton firms.

Grant Thornton International is an organisation of independently owned and managed accounting and consulting firms. Each member firm within Grant Thornton International is a separate national firm. These firms are not members of one international partnership or otherwise legal partners with each other, nor does membership within Grant Thornton International thereby make any firm responsible for the services or activities of any other. Each firm governs itself and handles its administrative matters on a local basis. Most of the member firms carry the Grant Thornton name, either exclusively or in their national practice names, facilitated by a name use agreement.

Grant Thornton has more than 62,000 people in its member firms in 140 countries.



Related Experts

Wayne Pisani
Partner – Head of regulatory and compliance | Tax and regulatory - Corporate & Financial Services
E: wayne.pisani@mt.gt.com
M: +356 9942 3253
D: +356 2093 1602
T: +356 2093 1000

Wayne Pisani heads the tax, regulatory and compliance practice within Grant Thornton and leads the financial services tax and regulatory team.

He advises an extensive client base ranging from private clients, including family offices and high-net-worth individuals, to NASDAQ listed companies. Working across several industry sectors, he deals with a wide range of cross-border regulatory, compliance and tax planning engagements involving both local and international financial institutions, asset protection, M&A and project finance transactions, driving the development of innovative solutions that support clients in their transition to more sustainable outcomes.

Wayne chairs the Financial Services Regulated Business Committee of the Institute of Financial Services Practitioners having been the president of the Institute and a member of the board of governors of FinanceMalta between 2018 and 2021. He is presently a member of the Malta Financial Services Advisory Council set up by the Minister for Finance and Employment and tasked with setting out a ten-year strategic plan for the Maltese financial services industry and is also a member of the International Fiscal Association, the International Bar Association and the Maltese Chamber of Advocates.

He was admitted to the Bar in 2001 following a Bachelor of Arts degree in Law and International Relations, and a Doctorate in legal studies from the University of Malta in 2001 after researching and submitting a thesis on "Merger control: a comparative study of regulatory systems for potential implementation into the Maltese legal system." Wayne also read for a Master of Arts degree in Financial Services at the University of Malta, graduating in 2003 after submission of a thesis entitled "The Impact of Information Technology on Financial Services". In 2018, having successfully submitted a research project on "Tax arbitrage in ICOs: a European perspective", published in the EC Tax Journal, he was awarded an Advanced Diploma in International Taxation by the Chartered Institute of Taxation.

Wayne is a published author and an experienced and passionate digital finance specialist embracing the mantra to pursue “development that meets the needs of the present without compromising the ability of future generations to meet their own needs”. He is an active thought leader in the financial technology space, proactively exploring digitalisation opportunities to transition to more sustainable finance, aspiring for net zero and a more sustainable way of living. He is a lecturer with a number of institutes and the University of Malta, makes regular contributions at fintech conferences, and has a passion for the security and technological aspects of distributed ledger technology, sustainable development and the collaborative economy. He is also a joint contributing author to "European Competition Laws: A Guide to the EC and its Member States, the leading legal compendium with respect to Competition law in Europe", published by Lexis Nexis and revised annually.

Joseph Pullicino
Partner | Head of Information Technology
E: joe.pullicino@mt.gt.com
M: +356 9949 9660

Joseph (Joe) joined the firm in 1988, after many years at the Central Bank of Malta where he gained extensive experience in banking, foreign exchange and information technology, and was admitted partner at Grant Thornton in 1993.

Joseph's expertise centres around computer security and audit procedures. As partner responsible for the Business Risk and Outsourcing Services Division of Grant Thornton, Joseph is heavily involved in computer systems consultancy for Government and other major clients of the firm and also internal and online-gaming audits.

He has accumulated extensive experience in the analysis, design and implementation of integrated accounting systems for corporate customers of varying size, including the Departmental Accounting System (DAS) for the Government of Malta, and for a number of Government entities, manufacturing concerns and service companies.

Grant Thornton
Fort Business Centre, Level 2
Triq l-Intornjatur, Zone 1
Central Business District
Birkirkara CBD1050,
Malta

T +356 2093 1000
E grantthornton@mt.gt.com

©2022 Grant Thornton (Malta). All rights reserved.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton (Malta) is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

Grant Thornton