



Grant Thornton

An instinct for growth™

General Data Protection Regulation requirements

Creating, protecting and enhancing value
in your business



Are you prepared for GDPR?

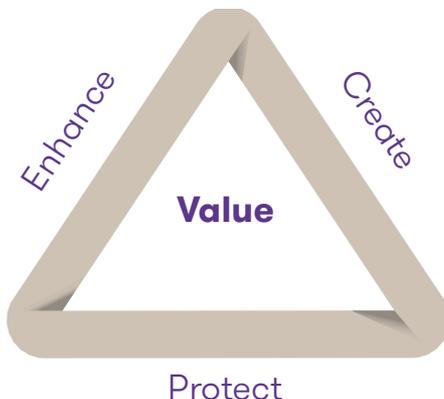
The General Data Protection Regulation (GDPR) comes into force in **May 2018**. It is the latest development in the current EU agenda to safeguard its citizens and their private information. The GDPR introduces new rights for individuals and strengthens existing protections. This new regulation imposes 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 supersedes the existing Irish Data Protection Acts and expands the obligations already in place. 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.

With the data protection legal landscape evolving rapidly it presents many challenges for businesses, government and public authorities, in particular for consumer facing businesses, online businesses, those in the financial services sector or organisations in possession of sensitive personal data. The potential severity of fines for data breaches and non-compliance with regulation was significantly increased 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.

At Grant Thornton our specialised IT consulting, business risk services and cyber teams offer an integrated service to create, protect and enhance value in your organisation in line with the new GDPR.



Key changes under the GDPR



Penalties

Under the GDPR, the Data Protection Commissioner may levy increased fines in the event of a data breach. Fines may be up to €20 million or 4% of annual turnover, whichever is greater. The 4% turnover is calculated at a group level, not by subsidiary.

Increased territorial scope and cross-border transferral of personal data

The GDPR will apply to businesses established outside the EU who offer goods or services or who monitor the behaviour of a data subject within the EU. It also applies whether or not the data processing takes place outside the EU. If your business is transferring data outside the EU, it must do so under an appropriate mechanism. All data controllers should review the basis under which such data is transferred and satisfy themselves that appropriate protections are in place.



Requirement to maintain internal inventories

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.

Appointment of a data protection officer

Data controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, must appoint a data protection officer. The data protection officer must have expert knowledge of data protection law and practices.



Regulation applies to both the data controller and the processor

Data processors may now be held liable for a breach if they have not complied with their contractual and statutory obligations. Data controllers must review and ensure that all contracts contain appropriate terms and data processors should review their contractual obligations to ensure that they are meeting requirements.

Reporting data breaches

The regulation introduces requirements to report all high risk data breaches to the Data Protection Commissioner within 72 hours and/or to the affected data subjects without undue delay. Businesses should be prepared for such an event by ensuring that a data breach response policy and procedure is in place.



Requirement of data portability

Data subjects will have the right to obtain and use their personal data for their own purposes across different services, where the processing of such data is based on consent and is carried out by automated means. The data should be easy to move, copy and transfer.



Introduction of the 'right to be forgotten'

The data subject will have the right to request the deletion or removal of personal data where there is no persuasive reason for its continued processing. Refusal to comply may only happen in a number of limited circumstances where the data is legally required to be maintained.



Data subject 'consent' requires clear affirmative action

Businesses must be able to demonstrate that the consent of the data subject was presented in a manner which is clearly distinguishable, in an intelligible and easily accessible form and using clear and plain language.



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 and particularly when using new technologies, taking into account the nature, scope, context and purposes of the processing.



Practical, real-world answers

Our multi-disciplinary team has a wide range of experience in data privacy assignments spanning regulatory and compliance, data and IT governance and technical reviews. We believe that GDPR compliance and the management of your firm's data is a business risk like any other. Our team can help you navigate the challenge without the jargon, taking an holistic and integrated approach to a multidimensional issue, working with you to identify and implement practical solutions which are appropriate for your business. We can help you with the following:

- understanding the key GDPR changes;
- assessing your current organisational data architecture and GDPR readiness;
- building a roadmap for implementation of appropriate regulatory and compliance architecture;
- ensuring your data risk management is integrated into your overall risk management structure;
- performing data flow mapping;
- building compliance and notification processes;
- conducting Data Privacy Impact Assessments (DPIAs);
- assessing your remediation activities;
- providing assurance to your key stakeholders, internal and external;
- helping you develop a data breach response action plan; and
- assessing your organisation's data protection training needs.

Why choose Grant Thornton?

Our culture is built on a genuine interest in our clients – their challenges, growth ambitions and wider commercial context. You get the attention you deserve from approachable, like-minded senior professionals who ask the right questions, listen and provide real insight and a clear point of view to guide you through all your GDPR concerns. We pride ourselves on being open, accessible and easy to work with. We work through the issues alongside you, always with an independent perspective and challenging where necessary. Our collaborative style also enables us to assemble teams with a broader perspective – working across service lines, industry teams and geographies to tailor our capabilities for you. We deliver a service that results in an entirely different experience – one that is driven by real, practical, informed insight. All of this helps organisations realise the benefits of their business, while mitigating its risks, to enhance value.



We are Grant Thornton

Grant Thornton is Ireland's fastest growing professional services firm. We deliver solutions to all business challenges. Clients choose us because the breadth of financial and business services they need is available, delivered innovatively and always to the highest standards. At Grant Thornton we are committed to long term relationships. We are different. We are Grant Thornton.

If you would like further information please contact:



Mike Harris
Partner
T +353 (0)1 436 6503
E mike.harris@ie.gt.com



Sheila Duignan
Partner
T +353 (0)1 680 5620
E sheila.duignan@ie.gt.com



Ian Cahill
Director
T +353 (0)1 680 5950
E ian.cahill@ie.gt.com

Offices in Dublin, Belfast, Cork, Galway, Kildare, Limerick and Longford.



www.grantthornton.ie



[@GrantThorntonIE](https://twitter.com/GrantThorntonIE)



[Grant Thornton Ireland](https://www.linkedin.com/company/grant-thornton-ireland)



Grant Thornton

An instinct for growth™

grantthornton.ie

© 2017 Grant Thornton Ireland. All rights reserved. Authorised by Chartered Accountants Ireland ("CAI") to carry on investment business.

'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 International Ltd (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. This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.