Grant Thornton
An instinct for growth™

Retail Excellence
Empowering an Industry

General Data Protection Regulation (GDPR)

New regulation for the protection of data

Executive summary

This manual has been developed by Retail Excellence in association with Grant Thornton to provide retailers with an overview of the key changes from the General Data Protection Regulation (GDPR) which will come into effect in **May 2018**.

The Grant Thornton team have created a specific retail-focused manual that will ensure Irish retailers are aware of the upcoming changes allowing them to ensure they are compliant with the new Regulation.

It is crucial that retailers have a secure operation in place when handling all customer data to ensure information is only used for its intended purpose. The manual also includes an appendix with commentary and viewpoints from the Data Protection Commission, Ecommerce Europe and the European Consumer Centre on the changes that the GDPR will bring.

From 2018, the cost of a data breach will become more direct and will have greater financial consequences.

General Data Protection Regulation (GDPR)

The GDPR is the latest development in the current EU agenda to safeguard its citizens and their private information. Currently, almost every retailer gathers and stores customer information in some form or another.

The GDPR introduces new rights for individuals and the changes require a review of your current approach and an assessment of the impact to your business and customers. Regulations come into force in the EU in **May 2018** and imposes stricter requirements on all business activities involving data. Whether you are a data controller, own customer data, a data processor or process data on behalf of a client, the GDPR will have a significant impact on your business.

With this we see the data protection legal landscape evolving rapidly. It presents many challenges for businesses and in particular for consumer-facing business with an online offering.

At Grant Thornton we have observed a keen interest from many sectors as businesses prepare for the revised regulations. With this, the profile and extent of activity by the Office of the Data Protection Commissioner in Ireland continues to grow and this activity is expected to further increase under GDPR. It's important to note that maximum fines for data breaches and non-compliance with regulation is €20 million or 4% of group turnover, whichever is greater.

The GDPR supersedes the existing Irish Data Protection Act and expands the obligations already in place. Organisations will have to move quickly to avoid potentially large fines for non-compliance.

As retailers, the pressure to make the most use of your data for marketing, cross-selling, geo-location, etc is only increasing. In some cases, the GDPR will require that you change the way you manage consent, such as prior information and specificity, for customer data processing or it may require that you change the kinds of data you collect and process. Even if you are not collecting and processing large volumes of data, the GDPR necessitates increased accountability.

At Grant Thornton, we can assist with all aspects of GDPR preparation. Our team has a wide range of data protection experience on which to draw, covering the technical, legal and compliance areas.

Key changes under the GDPR

Penalties - €20 million or 4% of turnover

A penalty for a data breach may cost up to €20 million or 4% of your annual turnover. In many cases, this is the difference between profit and loss in a financial year or would at least have a detrimental impact on your annual returns.

Increased territorial scope and cross-border transferral of personal data - new rules now applies to business outside of the EU

If you are transferring data outside of the EU, for any purpose, the terms of the GDPR will still apply. Transfer of data must be in compliance with the GDPR using one of the legal mechanisms provided for in the regulation.

Requirement to maintain internal inventories – need to record what data you store and collect

Although there are some narrows exemptions for smaller organisations, in general you must have and maintain an inventory of all of the data you hold, the reasons for holding it and other attributes, but not limited to retention, safeguards and data types.

Requirement of 'data portability'

Customers will have the right to obtain and use their personal data for their own purposes across different services. You will have to be able to provide customers with a machine readable copy of their data.

Introduction of the 'right to be forgotten'

Customers now have the right, in certain circumstances, to have data about them erased, removed or de-indexed. Are your IT systems and business processes able to take this into account?

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 and specific to the purposes for which it will be used. Consent can no longer be by default or implied.

Appointment of a Data Protection Officer (DPO)

A DPO is a new role established by the GDPR where certain organisations will be required to have depending on the type and volume of data being processed. The DPO must be a competent person, whose role is to promote the GDPR requirements and enforce a system of accountability. There are independence requirements which mean that the DPO may not be in a senior operational role.

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.

Reporting data breaches introduction of data breach reporting within 72 hours

In addition to reporting requirements from other regulations, the GDPR will require communication with the Data Protection Commissioner within 72 hours and/or informing the affected data subjects 'without undue delay' in high risk cases. Your incident response procedure will be key in achieving this tight timeline.

Subject access rights

Data subjects will enjoy stronger access rights. Where an access request is received, you must respond within the shorter time frame of one month and cannot charge a fee unless the request is manifestly unfounded or excessive. If you reject the request, you must reply setting out your grounds for doing so and providing information about the possibility of lodging a complaint with the supervisory authority, the Data Protection Commissioner in Ireland.

Appendices

European Consumer Centre

Information for consumers

The GDPR will impose increased obligations on retailers concerning the manner in which they handle personal data. This will include data collected when making purchases (eg name, address, banking details, etc) and also data collected for other purposes, for example marketing information (eg email address, personal preferences, types of products purchased, brand loyalty, etc). The GDPR will apply to retailers operating in the EU even if the company is registered outside the EU.

Consent

Consumers can allow retailers to process their personal data for many purposes (eg to send information of upcoming offers, for reward schemes, etc). Retailers are required to inform consumers of the purpose for which their data will be processed when obtaining consent for such use. The GDPR will require retailers to obtain multiple consents from a consumer where it is intended that their personal data will be used for more than one purpose (eg to process a transaction and sign up to receive a newsletter).

The GDPR also requires retailers to obtain 'unambiguous' consent from consumers with regard to the use of their personal data, which will assist consumers in retaining control over the use of their personal information.

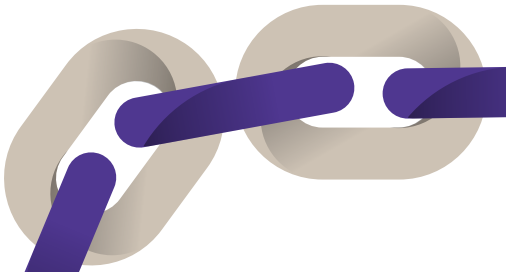
Protection

Consumers will be able to bring claims against retailers who fail to uphold their obligations under GDPR and who infringe their privacy rights. Retailers will be obliged to report any data protection breaches to the office of the Data Protection Commissioner within 72 hours and also to inform consumers of a breach where there is a high risk to their privacy rights.

Practical

The GDPR allows for data portability. This will be of use to consumers who wish to switch providers of goods and services, as it will provide a mechanism for the transfer of information from one company to another, making the process more convenient.

Cabhair agus comhairle do thomhaltóirí san Eoraip
ECC-Net
European Consumer Centre Ireland



Ecommerce Europe

"All web shops process personal data of their clients or persons they would like to become their clients. From **May 2018** all processing of personal data has to be compliant with the GDPR and the trader will be held accountable for compliance. This means that they will be fully responsible and held liable for proper processing of personal data and must be able to document the compliance of their processing with the GDPR.

The risk of non-compliance is very high. Non-compliance will lead to irritation for your clients that expected you to be careful with their personal data and who will have a right of compensation towards you for any material and non-material damages caused by the infringement. Moreover infringements of the GDPR will be subject to administrative fines up to €20 million or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

So better be prepared. Assess thoroughly all the processing of personal data in your web shop and be sure that you meet the conditions for lawful processing of these data and the expectations of your clients."

trust ECOMMERCE EUROPE

Léon Mölenberg
Senior Policy Advisor, Ecommerce Europe and Data Protection Specialist

“The risk of non-compliance is very high”

Léon Mölenberg, Senior Policy Advisor, Ecommerce Europe and Data Protection Specialist

Data Protection Commission

An Coimisinéir Cosanta Sonraí / Data Protection Commissioner

The GDPR takes effect from **May 2018** and will radically change the law on the protection of personal data in the EU. The GDPR strengthens the rights of individuals over their own data and very importantly for the members of Retail Excellence and their peers, increases the obligations on organisations to be transparent and accountable when collecting and processing personal data.

Publications like the one being launched by Retail Excellence and Grant Thornton are both timely and important, as they help bring the message of GDPR readiness to all businesses, large and small, reinforcing the Data Protection Commissioner's call to action that now is the time to prepare for May 2018.

Further guidance from the Data Protection Commissioner on getting ready for GDPR is available on our GDPR website www.GDPRandYou.ie and on twitter @DPCIreland

Retail Excellence

Established in 1995, Retail Excellence is owned by the Members, for the Members. We are an organisation which invests in innovative and exciting learning, market intelligence, human resources services, government representation and member networking initiatives. Retail Excellence has over 1,750 leading retail companies in Ireland. Our Members are the most progressive and innovative retailers. Retail Excellence is by far the largest retail industry body in Ireland.

T +353 (0)65 684 6927
W www.retailexcellence.ie
E info@retailexcellence.ie

Grant Thornton

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

Tommy Maycock
Director, Cyber Security
T +353 (0)1 500 8176
E tommy.maycock@ie.gt.com

Gary McPartland
Associate Director,
Cyber Security
T +353 (0)1 500 8158
E gary.mcpartland@ie.gt.com

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.

 www.grantthornton.ie  @GrantThorntonIE  Grant Thornton Ireland


Grant Thornton
An instinct for growth™

grantthornton.ie