Grant Thornton
An instinct for growth™

General Data Protection Regulation

March 2017

Creating, protecting and enhancing value in your business

The new GDPR and the possible impact on your business

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 by introducing new rights for individuals and strengthening existing protections, while imposing 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 EC Directive 46/95 currently in force, implemented in Italy through Legislative Decree 196/03 (Data Protection Law) and expands existing obligations.

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, the GDPR presents many challenges for businesses, government and public authorities, in particular for consumer facing businesses, online businesses, those in the financial services industry or organisations in possession of sensitive personal data.

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

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

At Grant Thornton Financial Advisory Services, our business risk and cyber-security experts offer an integrated service to create, protect and enhance value in your organisation in line with the new GDPR.

Key changes under the GDPR

Accountability

Accountability is a key concept within the new GDPR. The data controller is accountable for ensuring compliance with the GDPR with respect to all legal, organisational and technical matters; the data controller must actually be able to demonstrate compliance with the provisions of the EU Regulation.

Increased territorial scope and cross-border transferral of personal data

The GDPR will apply also to businesses established outside the EU which offer goods or services or which 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.

Security of processing

The data controller must carry out a Risk Assessment on personal data processing to guarantee compliance with the GDPR and be able to demonstrate that depending on the "risks (accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data)", the most "appropriate technical and organisational measures" to ensure an appropriate level of security have been implemented.

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.

Privacy by default and Privacy by design

The data controller must adopt appropriate technical and organisational measures to ensure that, by default, only personal data needed for each specific purpose are treated (amount of personal data collected, extent of their processing, period of their storage and accessibility limited to a specific number of individuals).

Both at the time of the determination of the means for processing (by design) and at the time of the processing itself, the data controller must implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the regulation and protect the rights of data subjects.

Requirement to maintain internal records

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, the categories of subjects involved and a general description of the technical and operational security measures (security of processing).

Data Protection Impact Assessments (DPIAs)

The regulation requires businesses to carry out a data protection impact assessment 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. The impact assessment must be carried out prior to the actual data processing.

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.

Data subjects' rights

Data subjects have the right to obtain additional information on the treatment of personal data, e.g. the recipients (or categories) to whom the data will be disclosed, the existence of automated decision-making (including profiling), as well as the right to request amendment or completion of personal data and, where provided for, the right to obtain the deletion of personal data without undue delay (right to be forgotten).

Data subjects also have the right to transmit personal data to another controller without hindrance from the controller to which they had been previously provided, upon condition that the processing is based on consent or on a contract and is carried out by automated means.

Data subjects also have the right to have personal data transmitted directly from one controller to another, where technically feasible.

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 (calculated at a group level, not by subsidiary), whichever is greater.

In short

Alignment with the new GDPR requires a multi disciplinary approach involving legal, organisational and technical skills, which takes into account the peculiarities of the personal data treatment and services offered, the territorial scope and the technological infrastructures used for the development and the provision of services, leading to a Privacy Governance framework with defined roles, responsibilities and management processes.

This will be critical when certification schemes will be defined; the application of an approved certification mechanism, could actually be used to demonstrate compliance with the data controller obligations under the GDPR.

How Grant Thornton Financial Advisory Services can help

Our multi-disciplinary team, with legal, organisational and IT skills, has a wide range of experience in data protection and privacy assignments.

We believe that the management of your organisation's data is a business risk like any other. Our team of experts can help you navigate this challenge, taking a holistic and integrated approach to a multidimensional issue, working with you to identify and implement practical solutions tailored on your business. We can help you with:

- understanding the key GDPR changes;
- assessing your current organisational data architecture and level of compliance with the GDPR and building a roadmap for the implementation of an appropriate regulatory and compliance structure (GDPR Check-up);
- devising solutions to ensure data risk management is integrated into your overall risk management structure;
- building an maintaining a personal data flow mapping;
- developing governance models and procedures to manage personal data;
- supporting the Data Protection Officer in fulfilling the obligations of his/her role and monitoring internal and external factors which may have an impact on the defined governance model;
- conducting data privacy impact assessments;
- evaluating your alignment with the new regulation;
- developing a data breach response action plan;
- assessing your organisation's data protection training needs.

Contacts

Stefano Salvadeo

CEO, Head of Growth and Advisory Services

T +39 02 783 351
M +39 347 83 95 792
E stefano.salvadeo@bgt.it.gt.com

Alessandro Leone

Partner
T +39 02 783 351
M +39 347 72 35 017
E alessandro.leone@bgt.it.gt.com

Renato Sesana

Partner
T +39 02 783 351
M +39 347 98 39 309
E renato.sesana@bgt.it.gt.com

Grant Thornton
An instinct for growth™

www.bgt-grantthornton.it

Offices

Milan

Via Melchiorre Gioia, 8
20124 Milano
T +39 02 783 351

Rome

Lungotevere Michelangelo, 9
00192 Roma
T +39 06 397 344 95

Padua

Galleria Europa, 4
35137 Padova
T +39 049 738 8290

Brescia

Piazza Paolo VI, 21 (Piazza Duomo)
25121 Brescia
T +39 030 240 4798

Staff locations

Trento

Via Brennero, 139
38121 Trento
T +39 0461 828 368

Trieste

Piazza Silvio Benco, 1
34122 Trieste
T +39 040 363 006

Turin

Corso Re Umberto, 2
10121 Torino
T +39 011 071 2899