

Overview of General Data Protection Regulation (GDPR)



An introduction to the GDPR
and why it's important to you
and your business

New data protection requirements (GDPR) are coming

The privacy rights of individuals are safeguarded in relation to the processing of their personal data by organisations.

- **Personal data is any information related to an identified or identifiable natural person ('data subject')**. This definition not only includes names and other factors specific to the identity of the individual but also online identifiers such as an IP address and location data.
- **'Sensitive personal data' are specific categories of personal data related to a person's: race or ethnicity; political, religious or philosophical beliefs; sexual life or sexual orientation; health; genetic or biometric data; criminal record; or trade union membership.** There are additional requirements for the protection of sensitive personal data. **'Processing of personal data' can cover the many different uses of that data**, including: collecting, recording, storing, adapting, using, disclosing and deleting data.
- **The General Data Protection Regulation (GDPR) applies to both 'data controllers' and 'data processors'.** A data controller is a person/company/other body, who either alone or with others, controls the contents and use of personal data. A data processor is a person/company/other body, who processes personal data on behalf of a data controller but does not include an employee of the data controller who processes such data in the course of his/her employment.
- **The rights cover data related to identified or identifiable persons (e.g. customers or employees) held either electronically or physically** – this includes physical files, emails, Customer Relationship Management (CRM) systems, images or recordings of individuals.

The EU has recently reformed its rules on data protection. The GDPR will be directly applicable in all EU Member States, including Ireland, on 25 May 2018. Many existing regulatory concepts on data protection will be retained, but there will be significant changes under the GDPR that require consideration and advance preparation.

Data protection is a key business consideration. In this context Ibec is delivering a series of short guides to help raise awareness and understanding of the GDPR.

The objective of this specific guide is to provide an overview of the GDPR - highlighting some of the key requirements for your business.

These guides are not exhaustive and are not intended as definitive analysis or advice legal or otherwise on compliance with data protection requirements. Ibec reserves the right to update this guidance as the implementation of the GDPR progresses.

Overview of the upcoming GDPR



This guide provides an overview of the GDPR - highlighting some of the key features for your business.



1. Enhanced rights for individuals

Individuals will have a greater say in how their personal data is collected and processed by organisations. They may:

- Request to receive further information within one month on how their data is processed;
- Request that their data be rectified or deleted;
- Object to profiling or automated decision making (automated decision making occurs when decisions are taken solely by automated means involving no human intervention);
- Transfer their data to another organisation.



2. Expanded scope for data protection

Core principles of current EU data protection law are retained, but the GDPR will apply to:

- Both data controllers and data processors;
- Organisations established in the EU; and to
- Organisations outside the EU who offer goods/services to EU residents or monitor their behaviour.



3. Harmonised implementation

- GDPR will be 'directly applicable' across the EU.
- Organisations operating across the EU will be predominantly regulated by the data protection authority (DPA) where they have their main establishment (one-stop-shop mechanism). For example a multinational company whose HQ is in Dublin but also has operations across the EU may choose to be predominantly supervised by the Irish Office of the Data Protection Commissioner.
- Co-operation between relevant DPAs across the EU in providing guidance and addressing cross-border complaints.

4. Risk-based implementation

- Companies, regardless of size, should take into account the nature, scope, context and purposes of their data processing activities in defining the potential level of risk and severity posed to the rights of individuals e.g. is there a potential risk of fraud, financial loss, harm or reputational damage to the individuals.
- Appropriate technical and organisational controls must be adopted to manage the risks posed to individuals by the data processing activities.
- Depending on the level of risk, organisations may need to:
 - Conduct impact assessments.
 - Keep detailed records of data processing and implement measures to ensure and demonstrate compliance.
 - Designate data protection officers (DPOs), who report to top management.



5. Greater accountability for business

- Personal data must be obtained and processed in a lawful, fair and transparent manner. Data processing must have specific, explicit and legitimate purpose(s).
- Businesses must ensure and demonstrate compliance.
- Businesses must consider data protection in the design and development of new products and services, not just in existing activities.
- Businesses must provide accessible information to individuals in their privacy notices.
- Businesses must emphasise that contracts between an organisation and service providers clearly outline the data protection responsibilities of each party.



6. Higher consent threshold for data processing

- Consent from individuals must be “freely given, specific, informed and unambiguous”. Silence, pre-ticked boxes or inactivity will not constitute consent.
- Check age limits for parental consent in certain cases.
- Consent may be withdrawn at any time.



7. Reporting data breaches

- Data processors must report data breaches to data controllers.
- Data controllers must notify their DPA of a data breach within 72 hours. Affected individuals must also be notified in cases where the data breach poses a high risk to their rights.



8. Greater sanctions

- DPAs have wider powers to enforce compliance.
- Significant administrative fines of up to €20 million or 4% of total worldwide annual turnover, whichever is higher, apply.
- Individuals also may sue organisations for material and non-material damage suffered as a result of a breach of the GDPR.
- Depending on their responsibilities, data controllers and processors may be jointly and severally liable for damage caused to individuals by a breach of the GDPR.



9. International data transfers

- Organisations must continue to use appropriate mechanisms if transferring personal data outside the EEA e.g. adequacy decision by the European Commission, binding corporate rules, model clauses or legitimate derogations approved by the relevant DPA. Further information is available from the European Commission.
- Non-EU authorities are prohibited from ordering the disclosure of personal data from EU organisations unless the order is under an international agreement.



10. Further guidance is expected

- Understand your GDPR requirements – one size does not fit all. Educate your organisation about GDPR requirements.
- DPAs (ODPC, the ICO and the Article 29 Working Party) are producing guidance to help your awareness and understanding of data protection and the upcoming GDPR.

About us

Ibec represents Irish business; home grown, multinational, big and small, spanning every sector of the economy. The organisation and its sector associations, work with government and policy makers nationally and internationally, to shape business conditions and drive economic growth. It also provides a wide range of professional services direct to members

Further information

Ibec's digital economy policy committee and GDPR taskforce
www.ibec.ie/digitaleconomy

Ibec's Employer Relations Division
www.ibec.ie/employerservices

© Copyright Ibec, 2017



Ibec

84/86 Lower Baggot Street
Dublin 2
T: + 353 1 605 1500
E: membership@ibec.ie
W: www.ibec.ie

Disclaimer

This publication is for general information purposes only and not intended as detailed legal analysis or advice. Ibec assumes no responsibility for any use to which the information may be put, or for any errors.