Ibec
For Irish Business

02 Mind your business | Prepare for GDPR

How employers should comply with GDPR

Recommendations for employer compliance with GDPR

“ The scope of the impact of the GDPR cannot be overstated. The GDPR will impact most if not all areas of your business. Key employees and decision makers across your business must be aware of and trained on the GDPR so that they can consider how to ensure compliance and appropriately allocate resources.”

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 recommendations to assist employers as they begin their preparations for the arrival of GDPR in May 2018.

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.

How employers should prepare for GDPR

10/Keep abreast of developments between now and May 2018

09/Consider whether you will need to appoint a DPO

08/Consider whether you will need to carry out data protection impact assessments

07/Review your data security procedures

06/Review your data access request procedures

01/Spread awareness of the GDPR within your organisation

02/Conduct a data protection audit

03/Consider the basis on which you have collected personal data

04/Review your data protection notices

05/Review your data protection policies

Recommendations for employer compliance with GDPR

Recommendation 1

Spread awareness of the GDPR within your organisation

The first step is to understand the scope of the GDPR and the extent to which it will impact your organisation. For example:

- Are you a data controller or a data processor?
- Where is your 'main establishment' for the purposes of GDPR compliance?

The scope of the impact of the GDPR cannot be overstated. The GDPR will impact most if not all areas of your business with such impact likely having budgetary implications for various parts of the business.

The GDPR provides for fines of up to €20 million or 4% of annual global turnover and permits individuals to sue for both material and non-material damage. Key employees and decision makers across your business must, therefore, be aware of and trained on the GDPR so that they can consider how to ensure compliance and appropriately allocate resources.

As the business progresses with its preparations, all staff training workshops should be organised so that employees are aware of the main effects of the GDPR on their work. For example:

- Staff should understand how to respond to requests from data subjects and Data Protection Authorities (DPAs) in relation to GDPR requirements;
- Data processing contracts should meet the requirements of the GDPR. The scope and allocation of risk between processors and controllers in such contracts should be appropriate and understood.

Recommendation 2

Conduct a data protection audit

As a first step, employers should review all personal data they hold, whether that data relates to current or former customers, current or past employees, unsuccessful job candidates or other third parties. The Data Protection Commissioner (DPC) has suggested examining all such personal data under the following headings:

a. **Why are you holding it?**

b. **How did you obtain it?**

c. **Why was it originally gathered?**

d. **How long will you retain it?**

e. **How secure is it, both in terms of encryption and accessibility?**

f. **Do you ever share it with third parties and on what basis might you do so?**

The GDPR explicitly requires organisations to be in a position to demonstrate compliance with its requirements. Documenting the above review and any subsequent action will enable employers to:

1. Identify any gaps in its compliance with data protection rules
2. Put in place processes to ensure all gaps or errors are rectified
3. Produce evidence of its compliance on the coming into force of the GDPR

When carrying out this "data protection audit", employers should pay particular attention to outdated data which it may no longer justify retaining. The GDPR does not specify any particular retention periods for personal data. However, it states that personal data may only be kept in a form which permits identification of the individual for no longer than is necessary for the purpose for which it was processed.

When considering retention periods, employers should be guided by statutory retention periods, limitation periods, individual business needs and, of course, data protection principles.

For employee data, employment legislation dictates retention periods for certain data. Some of these statutory retention periods are set out below.

Statutory Retention Periods for HR Data

Wage information	**3 years**
Working hours and related information	**3 years**
Collective redundancy information	**3 years**
Parental leave records	**8 years**
Carer's leave	**3 years**
Employment permit records	**5 years or period equal to duration of employment (whichever is longer)**
Employment records of young persons	**3 years**
Accident records	**10 years**

Other data may need to be retained to defend any actions against the employer. In this regard, account should be taken of the six year limitation period to take a breach of contract claim and the two year limitation period to take a personal injuries claim.

Crucially, all retention periods should be evidence based and the period chosen cannot seek to cover all possible eventualities where personal data may be useful to the business.

Outsourcing activities should also form a key part of your data protection audit.

If, in the course of business, you transfer, or intend to transfer, an individual's personal data to another organisation for data processing ensure that the data processing contract addresses GDPR requirements and clearly sets out the responsibilities and liabilities of all parties.

If, in the course of business, you transfer, or intend to transfer an individual's personal data outside the EU, ensure that approved transfer mechanisms are in place to do so. Guidance on international transfer mechanisms is expected to be published over the course of 2017. However guidance on current rules regarding international data transfers can be found on the websites of the Data Protection Commissioner and the UK's Information Commissioner.

Recommendation 3

Consider the basis on which you have collected personal data

Businesses must be able to identify and document the legal basis for processing personal data.

Some of the legal bases of most relevance to employers include the following:

- Consent of the data subject
- Processing is necessary for the performance of a contract to which the data subject is a party
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary for the legitimate interests of the data controller unless such interests are overridden by the interests or rights of the data subject.

Businesses should, in particular, note the GDPR's provisions on consent when carrying out their review of personal data held or processed.

The GDPR provides that consent must be "freely given, specific, informed and unambiguous" and crucially, consent may be withdrawn at any time. Silence, pre-ticked boxes or inactivity will not constitute consent.

For employers, there are question marks over whether employee consent can be freely given because of the imbalance of power which can exist between employer and employee. While employers are, for the moment, still advised to seek employee consent for any processing of data, they may also need to be able to rely on one of the other bases outlined above.

Where employee consent is relied upon, it should be obtained by way of a separate data protection document rather than a data protection clause in the employment contract. Employees should also be told that they may withdraw their consent at any time.

Recommendation 4

Review your data protection notices

Employers should review their data protection and/or privacy notices and analyse whether they require any updating to ensure compliance with the new rules. For employers that do not currently have data protection or privacy notices, they should start to put these in place as the GDPR re-emphasises their importance.

When first collecting personal data, the GDPR requires businesses to provide information such as the following to individuals:

- The business's identity
- Contact details for the business and for the data protection officer (DPO), if applicable
- The reasons for collecting the data
- The use(s) to which the data will be put
- To whom the data will be disclosed

- Whether the data will be transferred outside of the EU
- The legal basis for the processing of the data
- The period for which the data will be stored, or the criteria to be used to determine retention periods
- Where the processing is based on the legitimate interests of the business, the legitimate interests concerned
- Where the processing is necessitated by a statutory or contractual requirement, the consequences for the individual of not providing the data
- Whether the data subject will be subject to automated decision making
- The rights of the individual under the GDPR

When preparing notices, businesses must set this information out in a clear, concise and easily accessible manner.

Further guidance on the contents of data protection notices can be found on the UK Information Commissioner's website.

Recommendation 5

Review your data protection policies

The GDPR contains enhanced rights for individuals. These include the right to:

- Receive certain information on the collection of personal data
- Access his/her personal data
- Rectify inaccurate personal data
- Be forgotten
- Restrict the processing of his/her data
- Transfer data from one organisation to another
- Object to direct marketing
- Object to automated decision making or profiling. Automated decision making occurs when decisions are taken solely by automated means involving no human intervention. Further guidance can be found on the UK Information Commissioner's website.

Employers should review their current data protection policies and consider whether they can currently facilitate these rights.

For employers that do not currently have any data protection policies in place, they should introduce these over the course of 2017.

Recommendation 6

Review your data access request procedures

The GDPR provides that a data access request must be responded to within 1 month of receipt of the request. This is a reduction on the 40 day period provided for by current data protection legislation. This 1 month period may be extended for up to 2 further months where necessary, taking into account the complexity and number of requests.

In another slight change, documents will have to be provided free of charge, unless the request is "manifestly unfounded or excessive", in which case a reasonable fee may be charged. Guidance on the circumstances in which a fee may be so charged, and the level of the fee which may be charged, is awaited.

Employers will also be obliged to provide further information to individuals making data access requests. This includes:

- The purposes of the processing
- The categories of personal data concerned
- To whom the personal data has been or will be disclosed
- Whether the data will be or has been transferred outside of the EU
- The period for which the data will be stored, or the criteria to be used to determine retention periods
- The right to make a complaint to the DPC
- The right to request rectification or deletion of the personal data
- Whether the data has been subject to automated decision making

Even under current data protection rules, responding to data access requests can be a costly and time consuming process. Employers should, therefore, review their procedures for responding to requests now to ensure that this process is as smooth as possible for the arrival of the GDPR.

Recommendation 7

Review your data security procedures

The GDPR contains new rules regarding mandatory security breach reporting for which employers should prepare.

The GDPR requires organisations to notify the DPC of a data security breach within 72 hours of becoming aware of the breach, unless the risk to rights and freedoms of data subjects is unlikely. The notification must contain the following information:

- The nature of the data breach including where possible, the categories and approximate number of individuals and personal data records concerned
- The name and contact details of the DPO or other contact within the organisation
- The likely consequences of the breach
- The measures taken or proposed to address the breach, including measures to mitigate possible adverse effects.

Organisations that are late in reporting breaches must provide a reasoned justification for the delay.

If there is a high risk to the data protection rights of individuals affected, they must also be informed promptly. Any such communication to individuals must be in clear and plain language.

Given the every increasing risk of data security breaches, employers that have not already done so, should put in place clear and adequate procedures for their detection, reporting and investigation. For employers that have data security procedures in place, these should be reviewed to ensure that the timelines and information requirements set out above are encompassed.

Recommendation 8

Consider whether you will need to carry out data protection impact assessments

Once the GDPR comes into effect, employers may have to carry out data protection impact assessments in respect of projects which pose a high risk to individuals' data protection rights. Examples of projects which are likely to require an impact assessment include the adoption of new technology, introduction of CCTV monitoring or profiling.

Employers should consider whether any current or planned projects will require a data protection impact assessment. Where projects do require such assessment, businesses should begin to carry them out to determine whether the activity can continue in light of data protection requirements. Further information and template impact assessments can be found on the UK Information Commissioner's website.

Recommendation 9

Consider whether you will need to appoint a DPO

Although many larger businesses already have a DPO in place, it is not currently required by data protection law. The GDPR provides that all public authorities must appoint a DPO. Private sector organisations must appoint a DPO if they:

- Carry out regular and systematic monitoring of data subjects on a large scale; or
- Carry out large scale processing of special categories of data.

The European Article 29 Working Party has published draft guidance to assist organisations to determine whether they are required to appoint a DPO. This guidance can be found on their website.

For employers that will require a DPO, or choose to appoint a DPO, they must allocate an adequate budget, whether they decide to recruit internally or externally. As the GDPR makes clear that DPO's must have sufficient expertise, independence and security of tenure, businesses must be careful to appoint suitable candidates to the role.

Once appointed, the DPO will report to top management and will serve as the contact point for data subjects and the DPC. They will also have to be allocated adequate resources to carry out the role effectively.

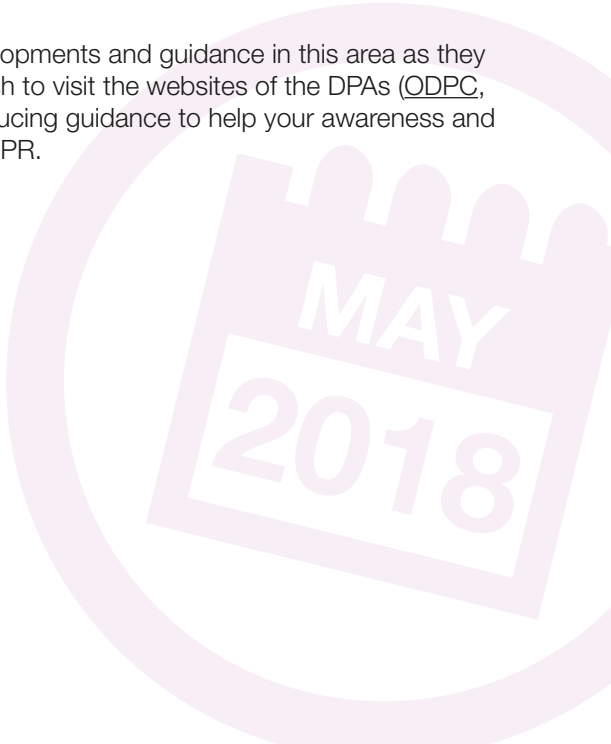
Recommendation 10

Keep abreast of developments between now and May 2018

Although the GDPR will be directly applicable from May 2018, a bill setting out some further detail on its implementation is expected to be published over the course of this year.

The DPC has also promised to publish further guidance on how best to ensure compliance with the GDPR between now and its coming into effect.

Businesses should, therefore, continue to monitor developments and guidance in this area as they prepare for May 2018. In particular, businesses may wish to visit the websites of the DPAs (ODPC, the ICO and the Article 29 Working Party) who 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 Services Division
www.ibec.ie/employerservices

Notes

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.