DATA PROTECTION UPDATE (GDPR)

The General Data Protection Regulation (Regulation (EU) 2016/679), enforceable 25 May 2018

This commentary is published by Chartered Accountants Ireland as a service to Chartered Accountants and their clients.

Presented by

KERRY LEHANE & CO.

CERTIFIED PUBLIC ACCOUNTANTS & REGISTERED AUDITORS

CHARTERED ACCOUNTANTS IRELAND

INTRODUCTION

The General Data Protection Regulation (GDPR) is a new EU Regulation that replaces previous data protection legislation. Written before mass Internet and mobile connectivity, before it was socially acceptable to share personal information online, data protection law was considerably out of date and replacement legislation long overdue. The GDPR is also being introduced to legislate for certain individual rights that were not covered by the previous legislation (e.g. 'right to be forgotten').

The GDPR comes into force on 25 May 2018. In Ireland, the Data Protection Commissioner (DPC), whose functions include the enforcement of the GDPR, expects organisations to be 'GDPR-ready'. This means that organisations must review and update their personal data processes and be able to demonstrate compliance with the new legislation.

WHY IS THE GDPR IMPORTANT?

The right to privacy is a fundamental human right. Organisations must always balance this right with their need to use 'personal data', i.e. "any information relating to an identified or identifiable natural person" (the 'data subject'). Organisations that gather, store and/or otherwise 'process' personal data are legally obliged to safeguard the privacy of the individuals with whose data they are entrusted. In introducing stricter measures, including consequences for non-compliance, the GDPR is intended to further ensure that this right to privacy is protected.

An organisation's need for personal data must be carefully considered and have a legal basis, and the gathering and processing of that data must be proportionate to that need. An example of this is a retailer installing CCTV cameras on its premises. What is the purpose or need? Is it to detect crime? Will ordinary, innocent people also be captured by the CCTV cameras? Is the need for CCTV proportionate to capturing the personal data of those individuals? Is the business's right to protect its property **balanced** with the individuals' right to privacy?

KEY CHANGES UNDER THE GDPR

The GDPR is more robust than previous legislation, enhancing the powers of the DPC and the rights of data subjects. Key changes under the GDPR are as follows:

1. Fines

The DPC now has the power to impose fines on **any** organisation holding personal data and in breach of the GDPR. These fines can be up to €20 million or 4% of turnover, whichever is greater. The DPC can take into account measures taken to comply with the GDPR when deciding on what fines, if any, to impose.

2. Compensation in the Courts

Data subjects will have a right to sue data controllers or data processors that have infringed their rights under the GDPR. Where a breach occurs that infringes the rights of a numbers of data subjects, each of them may seek judicial remedy from the offending data controller and/or data

processor. For example, if a record of 100 individuals is breached, then potentially 100 people will have suffered a loss for which they can seek compensation through the courts.

3. New Obligations for Data Processors
Previous data protection legislation required that, generally, only data controllers (those that initially obtain the personal data) had to comply. GDPR extends the legal obligations to include organisations that are data processors (those that process personal data on behalf of data controllers).

4. Accountability
The GDPR introduces the legal obligation of accountability for the handling of personal data and for being able to demonstrate compliance with the data protection principles (see below). The GDPR requires that the processing of personal data is recorded at each stage: as it enters, is held and used by an organisation.

5. Consent
While the legal bases for processing personal data will not change under the GDPR, if you are relying on the consent of the data subject, there are stricter rules about how such consent is captured, recorded and managed (covered in more detail below in relation to direct marketing – see Step 10).

6. Enhanced Rights of Data Subjects
While individuals always had rights under data protection legislation, these have been enhanced under the GDPR, including:

- changes to the conditions around the right of access to personal data:
  - the fee organisations could charge has been abolished; and
  - the time limit for complying with a data request is reduced from 40 to 30 days;
- a qualified right to erasure of personal data (the 'right to be forgotten');
- a right of rectification (to have any inaccuracies corrected);
- a right to 'data portability' (personal data must be stored so that it is readily identifiable and transferable to another organisation if so requested by the data subject); and
- a right to object to personal data being processed or to restrict it being processed.

7. Reporting of Data Breaches
A 'data breach' occurs when the security of personal data is compromised, e.g. when emails containing personal data are sent to the wrong person. Before the GDPR, it was not mandatory to report data breaches; now, in certain circumstances, it is mandatory to report breaches to the DPC, including where the personal data of a large number of data subjects is involved, or where special category data has been breached (e.g. medical records). Reported or not, all organisations are obliged to maintain a record of all data breaches.

8. Data Protection Officers
Some organisations, including public authorities or bodies, are now obliged to appoint a data protection officer (DPO), who must have the knowledge, support and authority to take responsibility for data protection compliance.

9. 'Privacy by Design' and Data Protection Impact Assessments

Organisations are now required to build data protection into all new products and services, and all new processes that involve the use of personal data. Data protection impact assessments (DPIAs) will identify, assess and minimise risks with the processing of personal data. DPIAs are particularly relevant when a new data process or system is being introduced. DPIAs are mandatory where data processing is likely to pose a high risk to the protection of data subjects' personal data. Documenting DPIAs will help to demonstrate compliance (accountability).

10. Global Applicability

The GDPR applies to organisations throughout the world that obtain or otherwise process the personal data of individuals resident in the EU.

WHAT YOU NEED TO DO ABOUT THE GDPR

You are obliged to comply with the principles of the GDPR as set out below:

The Main Principles of the GDPR

1. Lawfulness, Fairness and Transparency	Have a 'legal basis' for obtaining personal data, obtain the data fairly and be fully transparent as to your purpose for gathering it.
2. Purpose Limitation	Only use personal data for the purpose(s) for which you have obtained it under Principle 1 above.
3. Data Minimisation	Only collect personal data that is necessary and relevant to the purposes for which you are collecting it.
4. Accuracy	Make every reasonable effort to keep personal data accurate and up to date.
5. Storage Limitation	Do not retain personal data for any longer than the purposes for which it was collected.
6. Integrity and Confidentiality	Keep personal data secure, protected from any form of data breach.
7. Accountability	Be prepared to demonstrate compliance with your obligations under the GDPR.
8. Upholding Data Subject Rights	Uphold the rights of data subjects, including rights to: • access their data; • have their data erased or corrected;* • have their data transferable and moved on request;* • object to their data being processed or to restrict it being processed. * A qualified right.

HOW TO DO IT:
12 STEPS TO GDPR COMPLIANCE

1 Start by assessing and understanding what personal data you hold. Consider the following:

- all workflows or processes through which you collect personal data;
- your purposes (legal bases) for collecting it;
- categories of personal data gathered, such as names, addresses, bank details, etc.;
- how you are using the data;
- how you store it;
- the security of your storage methods;
- if you share the data with any third parties;
- whether you transfer personal data outside of Ireland and if those transfers are legal;
- how long you retain the data;
- how you delete or dispose of it.

(***Note***: Carrying out the above will help to demonstrate GDPR compliance.)

2 Review workflows against the GDPR principles to identify areas falling short of compliance.

3 Create a project plan for compliance, based on your findings from Step 2.

4 Review/create appropriate data protection and data retention policies for your organisation.

5 Review and update employment contracts and employee handbooks to include these new policies.

6 Ensure procedures are in place to manage and respond to data subjects' requests and for carrying out DPIAs (see above).

7 Ensure that personal data stored in both hardcopy and electronically is secure and protected against data breach. Measures to ensure this can include:

- strong password and access-permissions policies, ensuring that all computers, smartphones and portable memory devices are encrypted;
- regular back-up of data to servers located off-site or 'in the cloud';
- if personal data is leaving the European Economic Area, ensuring that the host country has an adequate data protection regime;
- checking the physical security of your offices and that all personal data in hardcopy is stored in locked filing cabinets;
- having a clean-desk policy so that personal data is never left lying around;
- training staff to be aware of GDPR requirements regarding data security (see Step 11);
- if personal data in either electronic or hardcopy form is ever taken off site, ensuring that protocols and measures are in place to protect its security.

8 If you share any data with third parties, e.g. outsourced payroll, marketing, IT, have GDPR-compliant data-processor agreements in place with all such service providers.

9 If you process personal data on behalf of other organisations, or have access to personal data that has been obtained and is controlled by your customers, then you are a data processor and must

have the same level of protection as set out above for such third-party data. Remember: the GDPR now requires data processors to provide the same level of protection as data controllers.

10 If you carry out any **direct marketing**, e.g. by email or post, you will have to consider carefully the legal bases (including consent, legitimate interest, contract) for obtaining, using and retaining the personal data with which you market to individuals. You must inform the data subject that you intend to market to them when you collect their details. If you are relying on consent you must have the data subject's valid consent to receive marketing material, this consent must be by way of "a statement or by a clear affirmative action", and you must be able to demonstrate that the data subject has provided this consent. Pre-ticked boxes and 'implied consent' are no longer acceptable. You must also make it easy for data subjects to exercise their right to withdraw their consent at any time. (***Note***: with direct marketing, data protection can be complex and it is worth seeking professional advice about compliance issues for your business.)

11 Most data breaches are caused by employee negligence. Creating both an understanding and a culture of data-protection compliance will reduce this risk. Provide data-protection training for all staff, not just those who handle personal data. Organise updated training annually. Again, keep records to help demonstrate compliance with the GDPR.

12 Consider whether you are required to appoint a data protection officer (DPO). Depending on the organisation and its activities, a DPO can be full-time or part-time, an employee or a contractor. They may carry out other tasks and functions as long as they are not in conflict with the autonomy required to fulfil the DPO role.

CONCLUSION

The GDPR is likely to impact on each and every organisation and cannot be ignored. The enforcement date of 25 May 2018 is only the beginning. As organisations become more aware of their obligations, individuals will become more aware of their rights and will demand a higher standard of care, with an expectation that their personal data will be handled in line with the law. Compliance will not only reduce the risk of legal action, but could also put you at a competitive advantage.