The General Data Protection Regulation
One Year On

by Gerry Egan

This article summarises the work that needs to be done to ensure compliance with the data management principles, the obligations of data controllers and the rights of data subjects.

It is now one year since the GDPR came into effect. Internationally, privacy is becoming an increasingly important topic. Internationally, privacy is becoming an increasingly important topic and major losses of personal data by 'blue chip' companies resulting in multi-million-euro fines have given organisations and citizens pause for thought.

Regulatory Activity Increasing

Regulatory activity is on the increase across Europe and we are starting to see the imposition of penalties for non-compliance with GDPR. While newspaper headlines have tended to focus on high profile investigations into organisations like Facebook and Google, 'ordinary' businesses have also been investigated and fined.

In Denmark, the Supervisory Authority (the Datatilsynet) imposed a penalty of €160,000 on a national taxi firm for failing to delete records of over nine million taxi rides after they were no longer needed.

A Portuguese hospital was fined €400,000 for a combination of offences including allowing too many people to have unnecessary access to patients' data (breach of the minimisation principle), inadequate security measures to prevent unlawful access to personal data and further breaches of basic data processing principles.

A Polish company that provides digital business, marketing, and credit information services has also been fined around €220,000 for failing to fulfil the company's transparency obligations towards six million data subjects. The company argued that its data processing activities have been inspected by authorities in two other countries and no irregularities had been found. This highlights the difficulties of applying the Regulation consistently across Europe.

To date, there have been no formal GDPR prosecutions in Ireland. The Data Protection Commission (DPC) has announced that 15 statutory inquiries (investigations) were opened in relation to multinational technology companies' compliance with the GDPR in 2018 and at least three further enquiries have commenced in 2019. In addition, the DPC's annual report for the period 25 May - 31 December 2018 says the DPC received over 4000 complaints and reports of almost 5000 data breaches in May 2018. Given that the DPC is statutory obliged to investigate every complaint, it seems inevitable that prosecutions will follow in at least some of these inquiries and investigations.

The State of Compliance

How seriously are organisations taking their responsibilities under GDPR and what progress is being made? In 2018, the Global Privacy Enforcement Network's (GPEN) 6th annual intelligence gathering operation ('Sweep'), examined organisations' self-reporting of how they have taken responsibility for complying with data protection laws.

GPEN members contacted 356 organisations in 18 countries and came to the following conclusions:

- Nearly three quarters of organisations across all sectors and jurisdictions had appointed an individual or team with responsibility for ensuring that their organisation complied with relevant data protection rules.
- Organisations were generally found to be quite good at giving data protection training to staff, but often failed to provide refresher training to existing staff.
- Around a quarter had no programmes in place to conduct self-assessments and/or internal audits to monitor internal performance in relation to data protection standards.
- The organisations that indicated that they have monitoring programmes in place generally gave examples of good practice, noting that they conduct annual audits or reviews and/or regular self-assessments.
- Over half of the organisations surveyed indicated that they have documented incident response procedures, and that they maintain up-to-date records of all data security incidents and breaches.

In Ireland, the Sweep involved 30 randomly-selected organisations across a range of sectors (including pharma, multinational, national and local Government, transport, charity, education and finance). The DPC noted the following trends among Irish organisations:

- 86% of organisations have a contact for their DPO listed on their website. All of these organisations have privacy policies that are easily accessible from the homepage.
- Most organisations reported that they have policies and procedures in place to respond to requests and complaints from individuals.
- 75% of organisations reported that they have adequate data breach policies in place.
- All organisations reported that they provide some form of data protection training for staff. However, only 38% of those organisations provided evidence of training programmes for all staff.
- In most cases, organisations reported that they undertake some data protection monitoring/ self-assessment, but not to a sufficiently high level. Three of the 29 respondents scored 'poor' in this section, while 13 reached 'satisfactory'.
- One third of organisations failed to provide evidence of documented processes to assess risks associated with new products and technology (data privacy impact assessment). However, most organisations appear to be aware of the need for this and many reported that they are documenting appropriate procedures.
- 30% of organisations failed to demonstrate that they had an adequate inventory of personal data while almost half failed to maintain a record of data flows.

So, quite a bit done but much more to do.

Re-cap - What is the GDPR?

The GDPR is an EU Regulation that came into effect on 25th May 2018 on the 'protection of natural persons with regard to the processing of personal data and on the free movement of such data'. It is designed to protect European residents by safeguarding personal data that we provide to public authorities, companies, etc. The scope extends beyond the EU as it is binding on all organisations that provide services to, or monitor, EU residents.

Personal Data

Personal Data is any information relating to an identified or identifiable living, natural person, who is called the data subject (DS). Examples of personal data include name and PPS number and also data like CCTV images or an IP address, which can identify an individual indirectly.

The GDPR defines some Special Categories of data. These are: racial or ethnic origin, political views, religious or philosophical beliefs, physical or mental health, sexual orientation, sex life, trade union association, genetic data and biometric data. More stringent rules apply to this data.

The Seven Principles of Data Management

Compliance with the seven principles of data management requires us to challenge current personal data management practices as follows:

Principle	Key Considerations
1	Do we have a privacy notice, and have we communicated to Data Subjects? What is our lawful purpose(s) and which lawful processing conditions do we rely on?
2	Are we using the data used only for the purpose for which it was provided?
3	How do we minimise the data processed?
4	How do we ensure the accuracy and quality of data?
5	How long to retain? Delete obsolete data? Appropriate disposal?
6	Appropriate security? Sources of risk? Respect for confidentiality?

What are your Obligations as Data Controller and Data Processor?

Principle 7 relates to the responsibilities of the Data Controller (DC) (and Data Processor (DP)). The DC must be able to demonstrate compliance with the GDPR. Most CPA Ireland members will control personal data e.g. of employees and clients and some will also be processors e.g. when providing payroll services (processing personal data on the instructions of a client).

The key obligations of DCs and the questions you need to consider are:

Privacy notice(s)
What are the best ways to communicate our privacy notice(s) to our DS's?

Maintain logs of data processing
Do I need a DC log, DP log or both?

Record and notify data breaches
How do I detect, record, notify data breaches and take corrective action?

Contract between controllers and data processors
Who are my processors, and do I have compliant contracts in place?

Understand Data Subject Rights and have process to handle requests
Are these understood? Do we have a process to handle requests?

Carry out Data Privacy Impact Assessment.
Do I understand when required? Know how to carry out?

In addition, some DCs may have the following additional obligations:

Designate Main Establishment?	Companies operating in more than one country are required to designate one country where they will be supervised by the Data Protection Supervisory Authority as their main establishment.
Appoint Nominated Representative?	Companies without a presence in EU but who provide services in EU must appoint a nominated representative.
Enter Joint Controller Agreement (JCA)?	If you control personal data jointly with another controller you require a JCA.
Appoint Data Protection Officer?	Must I or should I appoint a DPO? See below.
Understand rules governing overseas transfer of data	Do I transfer data overseas? Understand rules governing such transfers?

Rights of Data Subjects (DS)

DSs have stronger rights under GDPR. In summary these are:

The Right to Erasure (a.k.a. Right to be Forgotten): the right to have personal data erased where it is no longer required by the DC.

The Right to Restriction of Processing: the right to have the processing of data restricted e.g. in order for data to be corrected.

The Right to Rectification: the right to have incorrect data corrected.

The Right to Object: the right to object to processing of personal data on the basis that the DS no longer wishes you to process his data.

The Right to Data Portability: the right to receive a copy of personal data or to have it transferred e.g. to a new service provider.

The Right of Access to One's Personal Data: the right to know what personal data you hold in relation to a DS.

In addition, data subjects now have enhanced rights in relation to profiling and automated decision making.

This is a key focus area under GDPR, and it is essential that data controllers have robust processes in place to deal with requests from DS's within one month as prescribed by the Regulation.

Failure to uphold the rights of data subjects is a Category B i.e. most serious offence and a complaint from a DS will always be investigated by the DPC.

Do you need to appoint a Data Protection Officer?

Under Article 37 of the GDPR a DC must appoint a DPO where (a) the processing is carried out by a public authority or body; or (b) the core activities require regular and systematic monitoring of Data Subjects on a large scale; or (c) the core activities consist of processing on a large scale of special categories of data such as data relating to medical, social welfare administration or criminal offences.

Otherwise, appointment of a DPO is optional. A DPO does not have to be an employee nor does it have to be a full-time role. DPO services can be procured on a contract basis.

Conclusion and Final Tips

GDPR is a positive development and, when properly applied, greatly enhances our privacy. While the benefits for citizens are obvious, the consequences for organisations of non-compliance are serious with administrative fines of up €20million or 4% of worldwide turnover. Directors of offending companies can also be held personally liable.

CPA Ireland members have important roles to play in ensuring that their organisations and clients are aware of and compliant with their data protection obligations.

I would draw attention to the following areas in particular which the DPC has highlighted as issues most likely to have the DPC calling to your door.

Transparency: advising the data subject about what data is being processed is fundamental so ensure that you have appropriate privacy notices.

Security: keep personal data secure and, if you have a data breach, notify the people affected and the DPC as necessary.

Finally, deal with requests from data subjects promptly. Addressing each of these three areas greatly reduces the prospect of a complaint being made to the DPC.

75% of organisations reported that they have adequate data breach policies in place.

Gerry Egan,

M.Sc. (Mgmt.), C. Dir,

Gerry is a Consultant and Trainer specialising in corporate governance, GDPR compliance and strategy working with clients in the private, public, and non-profit sectors.