Chartered Institute of Internal Auditors

**27 September 2016**

# Data protection

## Chartered Institute of Internal Auditors

Data is used by all businesses – from insurance firms and banks to social media sites and search engines. There are no borders online and cloud computing means data may be sent from Berlin to be processed in Boston and stored in Bangalore.

The Data Protection Regulation (Regulation (EU) 2016/679) will come into force across the EU on 25 May 2018 and internal auditors need to understand how this will affect their organisation.

Read our summary of the key changes

---

## Brexit and data protection regulation in the UK

How will this EU directive impact your organisation following the result of the UK's referendum to leave the EU?

There is a two year minimum period in which we remain a member of the EU while negotiating an exit. During this period the new regulation will become applicable in the UK without the need for domestic legislation whilst we remain part of the EU.

In addition, Article 3 of the Regulation provides for extra-territorial effect meaning that the Regulation will apply to businesses based outside of the EU where:

- Goods or services, irrespective of whether a payment is required, are offered to individuals located within the EU; or
- Monitoring of EU individual's behaviour takes place as far as their behaviour occurs within the EU.

Given the above, many businesses with supply chains or customers in the EU will therefore need to ensure they are meeting the regulation, regardless of UK decisions on data protection law.

Personal data from the EU may only be transferred to jurisdictions which protect that data as per EU standards.

---

## What should internal audit do?

Whilst it is too soon to know any of the detail, we suggest that internal auditors in the UK should be advising their organisations to:

### 1. Consider the implications

Consider which parts of the operations and which data sets may be affected by proposed changes where the organisation has key customers in the EU. It is likely that many organisations have started work on this given the significance of some of the changes. Based on the ICO's statement,

it is possible that some or all of the changes set out in the GDPR are adopted under UK law after Brexit.

Monitor the Information Commissioner's Office for statements on Brexit, General Data Protection Regulation (GDPR) and guidance on remaining compliant.

### 2. Continue to review current practices

Continue reviewing internal data processing and to aim to be compliant with the GDPR by May 2018.

Internal audit should also be looking out for news and updates and amend the audit plan accordingly as the position regarding GDPR and application in the UK becomes clearer.

We will publish further comment once Article 50 is invoked and we know more about timescales and the Brexit plan. Internal auditors in the Republic of Ireland should continue with their plans, and may find the Data Protection Commissioner useful.

---

## Key changes in the new regulation

### 1. The right to be informed

This encompasses an organisations obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how organisations use personal data.

### 2. The right to restrict processing

When processing is restricted, organisations are permitted to store the personal data, but not further process it. Organisations can retain just enough information about the individual to ensure that the restriction is respected in future.

### 3. The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling)
- processing for purposes of scientific/historical research and statistics

Organisations must offer a way for individuals to object online.

### 4. Organisations must appoint a Data Protection Officer

They must do this if they:

- are a public authority (except for courts acting in their judicial capacity)
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking)
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

A single data protection officer may be appointed to act for a group of companies or for a group of public authorities, taking into account their structure and size.

### 5. Increased penalties under the GDPR

Under the new regulations penalties will reach an upper limit of €20 million or 4% or annual global turnover – whichever is higher, per incident. Previously the maximum was £500,000 and in practice, the ICO has never issued a penalty higher than £350,000.

### 6. A right to be forgotten

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. People will be able to delete their data if there are no legitimate grounds for retaining it.

### 7. The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

### 8. General

If personal data is handled abroad, EU rules must apply by companies that are active in the EU market and offer their services to EU citizens.

Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home.

A new Directive will apply general data protection principles and rules for police and judicial cooperation in criminal matters. The rules will apply to both domestic and cross-border transfers of data.

---

## Further reading

Information Commissioner's Office:

Overview of the GDPR
Response to the referendum result

European Commission:

Take control of your personal data (pdf)