Data Protection Act 1998

This is a summary guide regarding the Data Protection Act 1998 **for organisations** (including all companies).

Be aware: IMPORTANT CHANGE from 25th May 2018
From 25 May 2018, the **General Data Protection Regulation (GDPR)** to help organisations understand the new legal framework in the EU will apply. It explains the similarities with the existing UK Data Protection Act 1998 (DPA), and describes some of the new and different requirements. This is a living document and the ICO is working to expand it in key areas.

Introduction

The Data Protection Act 1998 (the DPA) is based around eight principles of good information handling. These give people specific rights to their personal information and place certain obligations on those organisations that are responsible for processing it. In data protection terms, these organisations must act as either **DATA CONTROLLERS** or **DATA PROCESSORS** to determine which organisation has a **data protection responsibility**.

"Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed." **This means that the data controller exercises overall control over the "why" and the "how" of the data processing activity.**
Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

"Data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

It is clear that the DPA makes the data controller legally responsible for the processing of personal data it undertakes itself and that is undertaken on its behalf by a data processor. No action can be taken under the DPA against a data processor itself. This is intended to ensure that data controllers put the necessary measures in place to protect their data processing operation from any vulnerability that may arise from their use of a data processor, such as a weakening of security.

I. The eight data protection principles

- **Principle 1- Fair and lawful**: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless(a) at least one of the conditions in Schedule 2 is met, and(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- **Principle 2 – Purposes**: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- **Principle 3- Adequacy:** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **Principle 4 – Accuracy**: Personal data shall be accurate and, where necessary, kept up to date.
- **Principle 5- Retention**: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- **Principle 6- Rights**: Personal data shall be processed in accordance with the rights of data subjects under this Act.
- **Principle 7- Security**: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- **Principle 8- International**: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

There is stronger legal protection for more sensitive information, such as: ethnic background, political opinions, religious beliefs, health, sexual health and criminal records.

II. Governance considerations between data controllers and date processors

Under the DPA all the legal responsibility for compliance falls directly on the data controller and not on the data processor. **The DPA requires that when a controller discloses personal data to a processor they should have a written contract in place**.

When a **controller discloses personal data to another controlle**r each has full data protection responsibility because both parties will exercise control over the purposes for which and the manner in which the data is processed. Where the sharing is systemic, large-scale or particularly risky, then both parties should **sign up to a data sharing agreement.**

III. Employment: quick guide

Please find in the annexe the "*quick guide to the employment practices code"* which is ideal for small businesses and provides all the information you'll need to keep on the right side of the law. It covers:

- What the Data Protection Act means to an employer
- Recruitment and selection
- Employment records
- Monitoring at work
- Information about workers' health
- What rights do workers have?

IV. Take action

a. Register (notify) your organisation under the Data Protection Act

The Data Protection Act 1998 requires **every data controller (eg organisation, sole trader) who is processing personal information to register with the ICO**, unless they are exempt.
For most organisations it's £35 each year.

b. Improve your practices

Your organisation might benefit from working with the ICO to improve your information rights practices using some ICO services such as:

- **Audits:** ICO aim is to complete an audit, from first meeting to issue of the final report, within 30 working days, normally including three days' at your organisation.
- **Advisory visits:** The aim of an advisory visit is to give practical advice to organisations on how to improve data protection practice. It normally involves a one day visit from the ICO and a short follow up report.
- **Posters, stickers and e-learning**: Download these posters, stickers and postcards to help you promote good data protection practice in your own organisation. Think. Check. Share.
- **Privacy Seals:** A privacy seal is a 'stamp of approval' which demonstrates good privacy practice and high data protection compliance standards.
- **Self-assessments, Training videos or Personal information promise.**

c. Security

It is difficult to provide a simple answer as each organisation processes personal data differently and is at risk from different threats. However, there are a number of organisations which provide advice specifically for small business. The ICO provide a range of resources which you can order from the website, www. ico.org.uk.

Get Safe Online (www.getsafeonline.org)
A joint initiative between the government, law enforcement, leading businesses and the public sector to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely and securely.

Business Link (www.businesslink.gov.uk)
Business Link is the government's online resource for businesses. The site contains information relating to at businesses.

Sources: gov.co.uk and ico.org.uk