GUIDE TO UK DATA PROTECTION REGULATIONS

ASECCA

Welcome to our guide on UK DATA PROTECTION

This document is a simple and concise guide to help our UK corporate customers revise their knowledge of the data protection regulations. It is the primary legislation for organisations who are disposing of data bearing equipment.

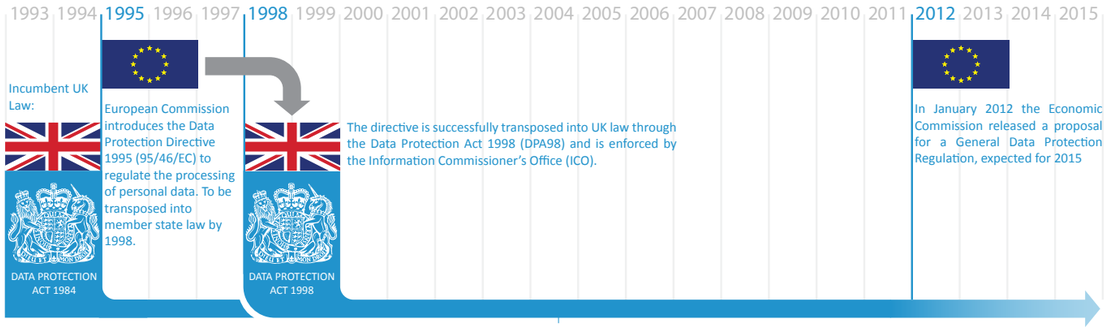
The Data Protection Act is close to 100 pages long and can be a daunting piece of legislation to get to grips with. This guide will help you become familiar with its primary points and show how ASECCA can help you stay safe.

CONTENTS

HOW ARE THE LAWS CREATED?

As members of the European Union (EU), the UK has some of its laws controlled by the European Commission (EC, the executive body that implements the work of the EU).

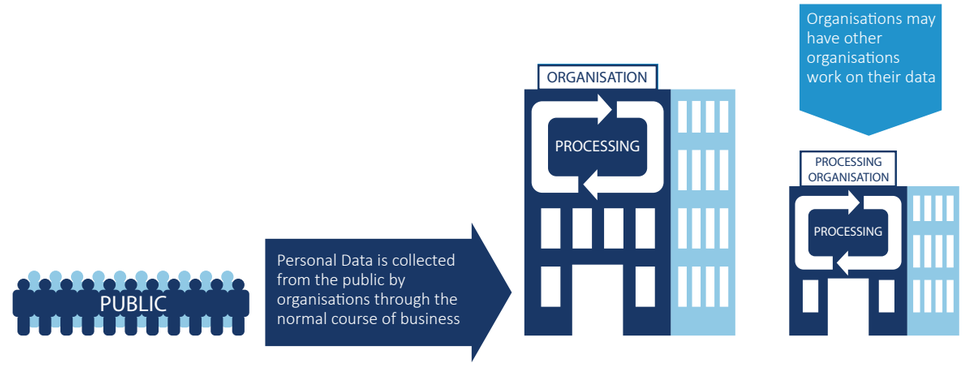
As illustrated below, in 1995, the EU introduced a new directive regarding data protection which had to be transposed into member state law by 1998. Consequently the UK updated the Data Protection Act to the 1998 version we are governed by today.



TERMINOLOGY AND DEFINITIONS

The Data Protection Act takes all transacting parties in the processing of data and categorizes them under certain definitions. Each party has specific conditions applied to it relating to various responsibilities and powers.

TRANSACTING PARTIES



LEGAL DEFINITIONS

DATA SUBJECTS
The customers, employees, prospective customers for who the data relates to

PERSONAL DATA
Data from which a living individual can be identified

SENSITIVE PERSONAL DATA
contains the following information:
1. Racial or ethnic origin
2. Political opinion
3. Religious beliefs
4. Trade union connections
5. Physical or mental health
6. Sexual life
7. Offences
8. Legal proceedings

DATA CONTROLLER
The organisation that collects the data for:

PROCESSING
The obtaining, recording, holding and carrying out operations on the data

DATA PROCESSOR
Anybody other than the data controller who processes data on behalf of the data controller

WHO POLICES DATA PROTECTION?

ico.

Information Commissioner's Office

The Data Protection Act 1998 is enforced in the UK by the Information Commissioner's Office. They keep registers of Data Controllers in the UK and ensure organisations and their staff are abiding by the Data Protection Act.

In order to police this law they have the following powers of enforcement:

- **Compulsory Audits**
- **Criminal Prosecution**
- **Penalties up to £500,000**

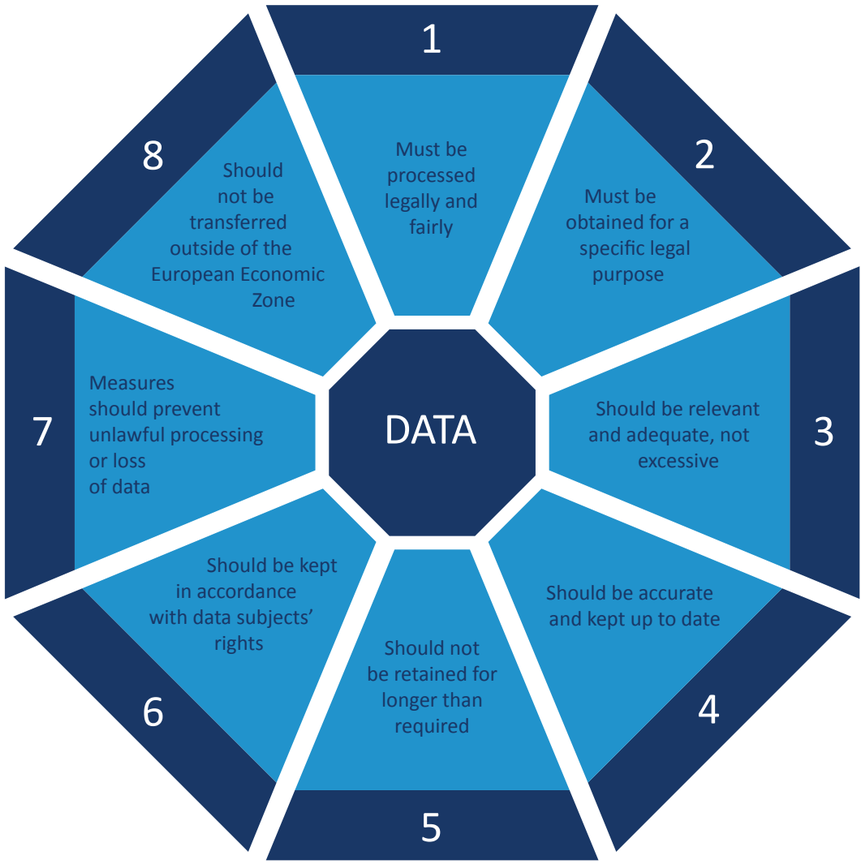
Between 2013 and 2014, the ICO issued fines of £2.17m. Here are some real life examples of ICO judgement:

Date	Organisation	Fine	Cause
19.03.2014	Kent Police	£100,000	Highly sensitive information left in basement at former site.
29.10.2013	NE Lincolnshire Council	£80,000	Loss of unencrypted memory device containing data relating to 286 children.
29.08.2013	Aberdeen City Council	£100,000	Inadequate home-working arrangements led to 39 page leak of personal data.
12.07.2013	NHS Surrey	£200,000	Sensitive data relating to thousands of patients held on hard drives were found being sold on auction sites.
07.06.2013	Glasgow City Council	£150,000	Loss of two unencrypted laptops, containing details of 20,143 people.
03.06.2013	Stockport PCT	£100,000	Discovery of large number of patient records at a site formerly owned by the Trust.

WHAT ARE THE RULES?

The Data Protection Act is complex and, in places, hard to understand. However it is underpinned by a set of eight straightforward, common sense principles:

THE 8 DATA PROTECTION PRINCIPLES



PRINCIPLE 7 - INFORMATION SECURITY

Principle 7 of the Data Protection Act covers information security.

The data that an organisation holds is for their use only and they have a responsibility to keep that data secure to protect the data subject's privacy.

To establish a method of best practise we can look to the ICO. In 2012 they issued a guidance notice for IT Asset Disposal for Organisations. The essence of this guidance is thus:

Equipment disposal is often the weakest link in the Data Protection chain of custody.

It is vital to create an airtight seal between your organisation (the data controller) and the asset disposal firm (the data processor) before commencing any disposals.

This means a legally defined allocation of scope and responsibility, a logistics strategy that is fully understood on both sides, an agreed level of data erasure of devices and disaster recovery procedures in the unlikely event of a breach.

HOW SHOULD YOU DISPOSE OF EQUIPMENT?

To achieve security, the ICO suggests multiple tasks to be executed. These tasks can essentially be partitioned into the following twelve requirements:

1 Data destruction method.	5 Have a procedure for the instance of a breach.	9 Select a disposal method.
2 Execute the process.	6 Select security to fit the nature of the personal data your organisation holds.	10 Make an inventory of the different types of devices you have.
3 Appoint an internal responsible party, a "data protection"	7 Select a Third Party IT asset disposal company.	11 Train staff.
4 Carry out a risk assessment.	8 Establish policies/procedures for asset disposal.	12 Sign contract with Third Party.

The ASECCA asset disposal service takes the 12 points made by the ICO and takes responsibility for the maximum of 9 that can be outsourced. The end product is a service that has been specifically suited to your requirements and that can easily be referenced back to the Data Protection Act 1998.

INTERNAL

Initially your organisation needs to appoint an internal data protection champion and select ASECCA as your third party asset disposal company.

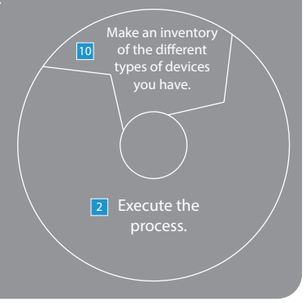
- Appoint an internal responsible party, a "data protection" champion. 3
- Select a Third Party IT asset disposal company. 7
- Sign contract with Third Party. 12

ASECCA

Once engaged the first thing to do is to carry out the preliminary tasks. This is analysing your estate (quantities, locations, types, data), and working with you to choose the best fit strategy for your organisation. We then take this strategy/policy and communicate it to your relevant members of staff.

- ONE-OFF PRELIMINARY EXERCISES
- 4 Carry out a risk assessment.
- 6 Select security to fit the nature of the personal data your organisation holds.
- 9 Select a disposal method.
- 1 Data destruction method.
- 8 Establish policies and procedures for asset disposal.
- 11 Train staff.
- 5 Have a procedure for the instance of a breach.

After the initial establishment, ASECCA enforces your policy and strategy on your behalf, and then executes it on an ongoing basis across your organisation.



UPCOMING CHANGES

There are changes in the pipeline for Data Protection laws in the UK and across Europe. To harmonize regulations across Europe, the EC is working on creating a new European regulation called the General Data Protection Regulation (GDRP). Adoption is expected in 2015/2016 and enforcement from 2017/2018 but here are the main differences that will affect you:

SCOPE	Currently, sanctions can be charged to EU data controllers processing data that relates to EU residents. Going forwards, this will be extended to any data controller in the world processing EU resident data.
RIGHT TO ERASURE	Data subjects will be able to request that Data controllers erase their information where there has been a occurance of non-compliance.
DATA PROTECTION OFFICER	The new regulation will force multi-national companies to appoint independent Data Protection Officers.
DATA BREACHES	The aforementioned Data Protection Officer is legally obligated to notify the Supervisory Authority without undue delay if there is a data breach.
SANCTIONS	Sanction limits will drastically increase, to the higher of €1m or 2% of global turnover.

ASECCA

info@asecca.co.uk 0161 315 0152 43 Northgate, White Lund Industrial Estate, Lancaster, LA3 3PA