An Introduction to
Data Protection Compliance

www.datacompliant.co.uk
For more free information, visit
www.datacompliantblog.com
**The Requirement to be Data Compliant**

Regardless of the size of your business, if you are a data controller and processing personal data, you have a legal requirement to be data compliant. Companies are no longer able to "get away with" non-compliance as UK individuals are increasingly aware of the steps to take if they believe a business is handling their personal data inappropriately. And the consequences of non-compliance can be costly.

---

**THE CONSEQUENCES OF NON-COMPLIANCE**

- **Prosecution.** Many breaches are criminal offences and will be prosecuted.
- **Prison.** Directors may be personally liable for companies in breach and can be imprisoned.
- **Fines.** The ICO has the power to levy fines of up to £500,000 for serious breaches.
- **Litigation.** Staff can be held individually responsible for data breaches, and may sue their employer if relevant data protection training has not been provided.
- **Loss of customer data.** In the event of non-compliant or unfair personal data collection, the company is likely to be required to **eliminate** all customer and prospect records from their databases.
- **Reputational damage.** The ICO publicises successful prosecutions or upheld complaints. Mainstream media increasingly publish data compliance and security breaches.

---

**Legislation**

Any organisation collecting and using personal data needs to comply with two key pieces of legislation:

**The Data Protection Act 1998**

The Data Protection Act (DPA) establishes a framework designed to ensure that data about living individuals is not processed without that individual’s knowledge and consent; and to keep personal data safe. The DPA addresses the complex balance between organisations’ need to collect and use personal data for business, versus the rights of individuals to the privacy and security of their personal details.
Privacy and Electronic Communication Regulation (PECR) 2003

The evolving complexities of the digital age needed further data protection consideration. PECR was introduced to cover electronic communications, including email, telephone and SMS.

The Eight Key Principles of Data Protection

Best practice data governance addresses the eight key principles of data protection. The Data Protection Act 1998 and the Privacy and Electronic (EC Directive) Regulations 2003 are the backbone of compliant use of personal data.

THE EIGHT PRINCIPLES OF DATA PROTECTION

1. Personal data must be collected and processed fairly and lawfully, and shall not be processed unless at least one of the conditions in Schedule 2* is met.
2. Personal data must be obtained for specified, defined purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Data must be accurate and kept up to date.
5. Data must not be kept for longer than necessary to fulfil the defined purpose or purposes.
6. Data must be processed in accordance with data subjects’ rights under the DPA.
7. Security - appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data.
8. Data may not be transferred outside the EEA 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.
It is increasingly important both to be compliant and to be seen to be compliant in terms of collection and use of personal data, whatever the size of your business.

### KEY PRINCIPLES OF DATA COMPLIANCE AND SECURITY

Fairness and transparency are two of a number of data compliance considerations, including:

- **Key Principles.** Always follow the eight data protection principles outlined above.
- **Data Governance Policies.** Data governance is essential. A management framework and appropriate policies and procedures for handling personal data need to be clear, practical, monitored and enforced.
- **Security.** A vital area covering computers, systems and staff. Data must be kept secure whether in storage, in use, or legitimately being shared. Access should be restricted to those who have need of it. Destroyed or discarded records or equipment must not hold personal information which can subsequently be accessed.
- **Notification.** The ICO must be notified by the data controller and accurately advised of the purposes of the personal data being processed.
- **Subject Access Requests.** Data subjects may request a copy of the personal information an organisation holds about them. The information must be provided within a limited time frame.
- **Data Processors.** You are responsible for ensuring data processors you employ are compliant and secure.
- **Training.** Employee negligence is a significant factor in data and IT security breaches.
- **Transfer Abroad.** Ensure data is transferred only to and via countries with an adequate level of data protection. Individuals must be informed before transferring their data outside the EEA.

### About Data Compliant

Data Compliant provides businesses with a robust data governance methodology, including compliant and secure processes, policies, practices and systems. Data Compliant undertakes Data Compliance Reviews, Governance Training and Workshops, Data Security ISO Certification [27001/27002] and provides a Data Protection Officer Service to keep your business’s personal data and reputation safe and provide protection against inadvertent breaches.