# Data Protection

## Key Points

* The General Data Protection Regulation comes into force on 25 May 2018.
* Workers have legal right to access information that an employer may hold on them.
* The Data Protection Act contains 8 principles that everyone responsible for using data has to follow.
* All staff have a responsibility under the act to ensure that their activities comply with the Data Protection.
* Data Protection applies when monitoring employee's telephone calls, emails and CCTV.
* Employees who feel the as a company we have misused information or hasn't kept it secure can contact the Information Commissioner's Office.

The European Union's GDPR (General Data Protection Regulation) comes into force in the UK on 25th May 2018. The GDPR will bring in stricter obligations that all employers must follow.

Until May 25 2018, The Data Protection Act 1998 still applies. The Data Protection Act is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with employees about the use of information about them and by following good data handling procedures. The act is mandatory and all organisations that hold or process personal data must comply.

## The Data Protection Act contains 8 principles:

1. Personal data should be processed fairly and lawfully
2. Data should be obtained only for one or more specified and lawful purposes
3. The data should be adequate, relevant and not excessive
4. It should be accurate and where necessary kept up to date
5. Any data should not be kept for longer than necessary
6. Personal data should be processed in accordance with the individuals rights under the act
7. Data should be kept secure
8. Personal data should not be transferred outside the European Economic Areas unless the country offers adequate data protection.

All staff have responsibilities under the Act to ensure that their activities comply with the Data Protection Principles. As a franchisee owner or delegated staff member will have responsibility for the type of *Personal Data* collected and how they use it. Staff should not disclose personal data outside the company’s procedures, or use personal data held on others for their own purposes.

Staff members have a legal right to access information that an employer may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes. Arrangements should be in place to deal with requests as a 40 day time limit is stipulated. Information can be withheld if releasing it would make it more difficult to detect crime or the information is about national security. If an employee feels the organisation has misused information or hasn't kept it secure they can contact the Information Commissioner's Office.

**Monitoring employees - CCTV, telephone calls, emails**

The Data Protection Act will apply if we are monitoring employees; for example to detect crime or excessive private use of e-mails, internet use etc. However, the act requires that staff members should be aware of the nature and reason for any monitoring.

**Health Information**

As an employer we can seek to collect information regarding an employee's health if the employee freely gives consent. This information once collected will be held securely.