hasslefree

Human Resources & Health and Safety

hasslefree

Do you employ staff?

Data Protection;

What Should be Kept and How Long For?

What is Data Protection?

The Data Protection Act 1998 was brought into place to ensure that an individual's data is processed, kept, and disposed of appropriately and securely. This is to prevent an individual's personal and sensitive data becoming accessible to people who do not have the right to see or use it. It also prevents an individual's data from being used in a way that could be harmful to that individual.

The Data Protection Act 1998 has the following 8 principles in relation to how data should be managed:

- It should be fairly and lawfully processed
- It should be processed for limited purposes
- The amount of data sought should be adequate, relevant and not excessive
- It should always be accurate
- It should not be kept for longer than is necessary
- It should be processed in line with the individual's rights
- It should always be kept secure, and
- It should not be transferred to countries outside of the European Economic Area without adequate protection.

If an organisation / data controller does not follow these 8 principles, they are breaking the law.

What is Data?

Computerised and manual records, photographs, CCTV or other footage, mainframes, laptops, organisers, palm pilots, audio and visual systems, telephone logging or surveillance systems, microfiche and microfilm are all currently classed as data. The definition of data is complex and is designed to be rather "open" so that it encompasses all that it needs to, but it does include information:

- Which is personal data relating to any living individual, and
- Includes any expression of opinion about the individual and / or
- Includes an indication of the intentions of the data controller or any other person in respect of the individual
- Information about an individual's medical history
- Salary details
- Information on tax liabilities
- Information on bank details
- Information on spending preferences
- Making lists containing a name and address / telephone number / email address / etc.

Secure Retention

The Data Protection Act 1998 clearly states that both computerised and manual retention systems should be as secure as possible. In practice, this means that physical copies should be filed in a way that ensures the contents is kept private. Locked filing cabinets are the most commonly used form of secure retention for physical data. For electronic data, a computer should be password protected and should also have all the normal, up to date security protocols. However, it can be surprisingly easy to break through one "layer" of electronic security, so we would recommend not only having a password protected computer, but password protected files too.

Retention Periods

Under the Data Protection Act 1998 there are both statutory retention periods, and advised retention periods. The statutory retention periods are as follows:

- **Records relating to Working Time:** 2 years from the date the records were made.
- **Accounting records:** 3 years for private companies, 6 years for public limited companies.
- **Accident books/records/reports:** 3 years from the date of the last entry (unless a child is involved, in which case this would be up until the child reached 21 years of age).
- **Income tax, Nation Insurance Returns, Income tax records and correspondence with the HMRC:** no less than 3 years after the tax year the data relates to.
- **Maternity records/information:** 3 years after the tax period in which the maternity period ends.
- **National Minimum Wage records:** 3 years after the end of the pay reference period following the pay reference period the records cover.
- **Wage / Salary Records:** 6 years from the last payment.
- **Records relating to Children and Young Adults:** up until the individual reaches the age of 21.

- **Medical Records under the control of Asbestos at Work Regulations:** 4 years for medical examination certificates, 40 years for medical records.
- **Medical Records as specified by the Control of Substances Hazardous to Health Regulations:** 40 years from the date of the last entry.
- **Medical Records and details of biological tests under the Control of Lead at Work Regulations:** 40 years from the date of the last entry.
- **Medical Records under the Ionising Radiation Regulations:** at least 50 years, or up until the individual turns 75 years of age.

For many HR records, there is no definitive retention period. In these instances, an employer must consider what would be a necessary retention period, depending upon the nature of the data. When in doubt, the CIPD recommend records are kept for 6 years to cover the time limit for bringing any civil legal action. The recommended retention periods are as follows:

- **Application forms and interview notes (for unsuccessful candidates):** 6 – 12 months.
- **Time cards:** 2 years after the audit they would have first been reviewed in.
- **Information relating to Parental Leave:** 5 years for a birth / adoption situation, 18 years when the family is in receipt of disability allowance for the child.
- **Money purchase details:** 6 years after the transfer of the value taken.
- **Personnel files & Training records:** 6 years after employment ceases.
- **Information relating to Statutory Sick Pay:** at least 3 months, although keeping these documents for 6 years after the individual's employment ceases is more advisable.
- **Trade Union agreements:** 10 years after the agreement ceases to be effective.
- **Pension scheme investment policies:** 12 years from the ending of any benefit payable under the policy.
- **Trust Deeds & Rules:** permanently.
- **Trustees' minute books:** permanently.
- **Works Council minutes:** permanently.
- **Actuarial Valuation reports:** permanently.
- **Assessments under the Health and Safety Regulations and records of Health and Safety related consultations:** permanently.
- **Inland Revenue / HMRC approvals:** permanently.
- **Senior executive records:** permanently, for historical purposes.

Data Destruction

The Data Protection Act 1998 also covers how data should be disposed of. Just because data is no longer needed by an organisation does not mean that the organisation loses the responsibility to protect that data, so data must be disposed of in a responsible manner. This means that every electrical copy will need to be deleted, and then the "trash can" on the computer will also have to be emptied. After this has been done, a search will need to be completed to ensure that none of the remnants of the deleted files remain – which can and does regularly happen. When it comes to physical data, it needs to be disposed of in a way that ensures it cannot be accessed again. In most cases, this involves shredding documents, bagging up the remnants of the shredded

documents, and disposing of these in the appropriate recycling bin. Recycling bins with lids are recommended, as it removes the chance of someone being able to easily view what is on a shredded piece of paper.

How We Can Help

If you have any queries relating to any of the above, please don't hesitate to contact us at hradvice@hasslefreehr.co.uk

References

The CIPD: https://www.cipd.co.uk/knowledge/fundamentals/emp-law/data-protection/factsheet

The CIPD: https://www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet

The Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/