14. Data Protection Best Practice

1 Overview

It is advisable to have a data protection policy in place which applies to the processing of personal data in manual and electronic HR records kept by your company.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors.

2 Relevant Legislation

The General Data Protection Regulations (GDPR) form part of data protection law in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of the GDPR apply from May 2018.

3 Personal data

Personal data is information that relates to an identifiable person who can be directly or indirectly identified from that information. Where third parties process data on your behalf, you should ensure that the third party takes such measures in order to maintain your commitment to protecting data.

In line with GDPR, you will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

You may hold the following types of personal data on personnel files or electronic records:

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

4 Data protection principles

All personal data obtained and held by you will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose

- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

5 PROCEDURES

You should take the following steps to protect the personal data of relevant individuals:

- appoint an employee with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of its data protection systems and procedures
    c. overviewing the effectiveness and integrity of all the data that must be protected.
- provide information to employees on their data protection rights, how you use their personal data, and how you protect it.
- provide employees with information and training to make them aware of the importance of protecting personal data.
- account for all personal data you hold, where it comes from and who it might be shared with.
- carry out risk assessments to identify any vulnerabilities in personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security.
- recognise the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. Understand that consent must be freely given, specific, informed and unambiguous. Individuals have the right to withdraw that consent at any time.
- have the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. Be aware of the duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner.

6 ACCESS TO DATA

Individuals have a right to be informed whether the Company processes personal data relating to them and to access the data that the Company holds about them.

7 NEXT STEPS

- Carry out an audit of the personal data you hold to assess where it is kept.
- Develop a Data Protection policy with guidelines around the processing, management and regulation, and storage and retention of all personal data in line with the GDPR.
- Ensure that employees read and understand your data protection policy.

8 FACTSHEETS TO HELP

- Holding HR Records

9 FOR MORE ADVICE AND INFORMATION

ACAS - (Advisory, Conciliation and Arbitration Service) free and impartial information and advice to employers and employees on all aspects of workplace relations and employment law. www.acas.org.uk

Achieve in Bath & North East Somerset – free recruitment support, advice and help. Matching job seekers, employers and course providers to help employers recruit, train and retain employees. www.achieveinbathnes.co.uk

Future Bright – free help & support for businesses and employees to realise their full potential. Provide access to training and development, workshops and networking. HR support to promote career progression and best practice to attract and retain staff. www.futurebright.org.uk

Information Commissioner's Officer – online resource for employers including further explanatory information about Data Protection and GDPR. www.ico.org.uk

Bibliography *- this fact sheet was produced by Rathbone HR Solutions in association with Cool Ventures Ltd in December 2018 with content sourced from; HR Inform (www.hr-inform.co.uk), ACAS (www.acas.org.uk), CIPD (www.cipd.co.uk), the pensions regulator (www.thepensionsregulator.gov.uk/en/employers), HMRC(www.gov.uk/government/organisations/hm-revenue-customs), the Information Commissioner's Officer website (www.ico.org.uk)*

Created for Future Bright by Cool Ventures - Business Support in Bath, Bristol, Wiltshire, Gloucestershire, South Gloucestershire and throughout South West England www.coolventures.co.uk