Data Protection and HR.

Introduction

25th May 2018 see's the introduction of the General Data Protection Regulation (GDPR) in the UK. The GDRP is a new EU legal framework that replaces the current UK Data Protection Act (DPA).

Whilst retaining many of the requirements of the Data Protection Act, the GDPR extends the data rights of individuals, and requires organisations to develop clear policies and procedures to protect personal data, and adopt appropriate technical and organisational measures.

Responsibilities of the HR Department

Under existing legislation, companies are responsible for ensuring employee data is kept secure, is accurate and up to date. Additionally, employee data mustn't be kept any longer than is necessary for a particular purpose. For example, there the following are some of the statutory retention periods for the recording of employee data:

- Salary records (including overtime, bonuses and expenses) - 6 years
- Working Time Records - 2 years
- Accident Books (accident records/reports) - 3 years
- Medical Records (relating to COSHH) - 40 years

There are also a number of recommended (non-statutory) retention periods, such as:

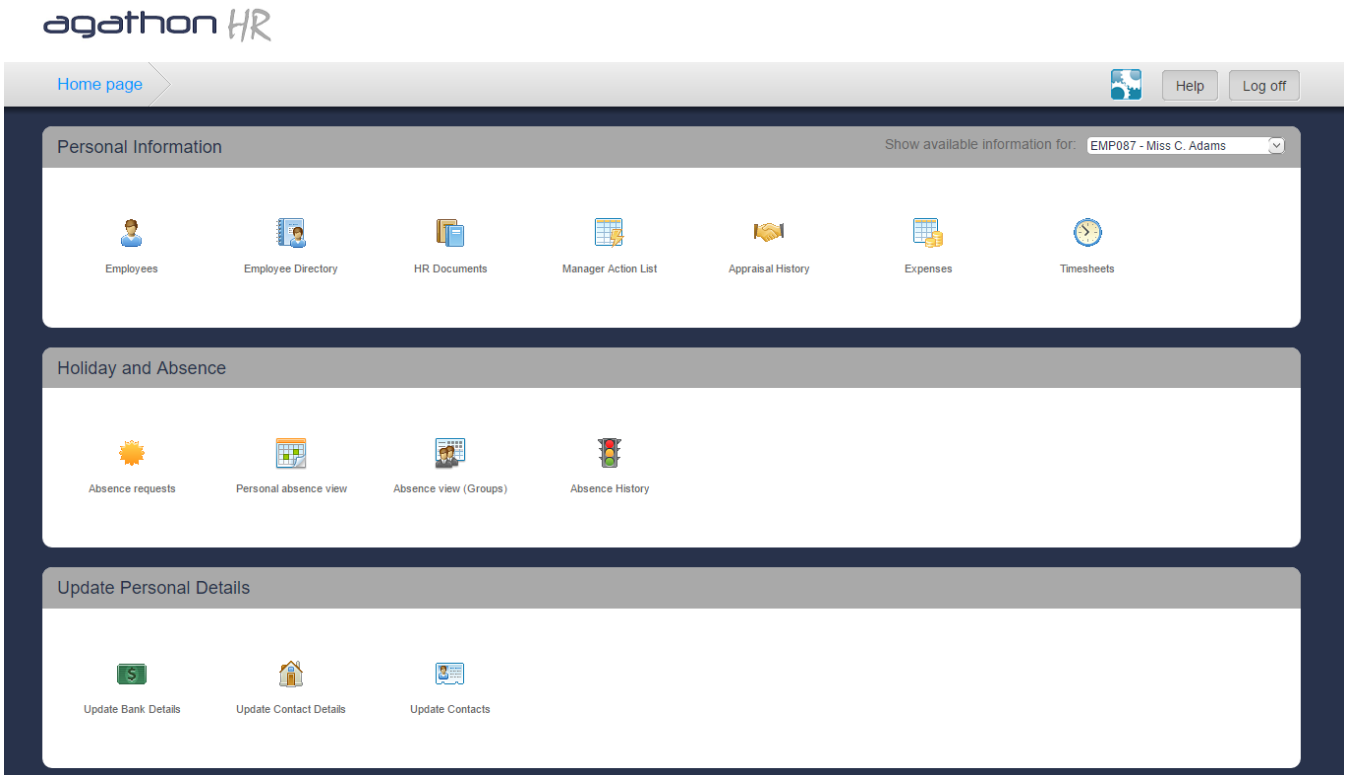
- Personnel Files and training records (including disciplinary records) = 6 years
- Application forms and interview notes (for unsuccessful candidates) – 6 months to 1 year
- Parental Leave - 5 years

In order to meet legislation, the CIPD suggests organisations do the following:

- Appoint a data protection officer to be in charge of all aspects of information including the DPA and Freedom of Information Act (for public authorities).
- Audit information systems to find out who holds what data, and why.
- Consider why information is collected and how it is used. Issue guidelines for managers about how to gather, store and retrieve data.
- Ensure that all information collected now complies with the Data Protection Act 1998.
- Check the security of information stored.
- Check the transfer of data outside the EEA.
- Check the organisation's use of automated decision making.
- Review policy and practice in respect of references.
- Review or introduce a policy for the private use of telephones, email and post.

Employees Rights

Employees are entitled to request (in writing) a copy of the data held about them and employers must supply this information within 40 days of the request, although this could be managed in some part by implementing Employee Self Service to provide some level of 'transparency' to employees.



Employee Self Service provides a level of transparency and trust between an organisation and its workforce

It is important therefore that organisations keep their employee information in a 'well-organised and appropriate system so that it complies with relevant legislation and can be easily retrieved'.

Penalties for breaching DPA/GDPR

Whilst at present organisations face fines of up to £500,00 for breaching the Data Protection Act, the new General Data Protection Regulation means organisations may find themselves facing a fine of up to 4% of global turnover if they breach the new rules.

Further information

Further information can be found on our website http://agathonhr.co.uk. If you require any support with People Inc. HR or Employee Self Service, please call 01242 663974 or email support@agathonhr.co.uk.