GDPR – An introduction Direct Payment for Employers

The EU wide General Data Protection Regulation (GDPR) becomes law in the UK on 25 May 2018. This has an impact on any employer in the UK who processes personal data. 'Personal data' is any information that enables an individual to be identified. 'Processing' includes everyday use of that data to manage employees such as keeping their contact details and using their information to pay their wages.

This guide is to provide awareness of the changes in the law and how this impacts upon how you use, store and retain data. The key issues to focus on are:

Privacy Notices

You must formally advise all employees (and applicants during the recruitment process) about how the personal data you hold about them is used, shared and retained. The notice needs to state what information you have, why you have it and what you use it for.

Where you share employee's personal data with any other party, you must ensure it is made clear to the employee in the Privacy Notice.

You must have a legal reason for processing personal data and state what that is in the Privacy Notice.

The Privacy notice must be issued to all employees either individually or it can be included in your Employee Handbook.

New Rights for employees

- Subject Access Request – Employees have always had the right to request details of the personal data you have about them. In future you must provide the information they want within 30 days.
- Right to rectification – Employees can ask for errors in the personal data you have to be corrected.
- Right to be forgotten – In some cases employees can ask for a personal data record to be removed. The employer needs to be able to evidence that the employee's data has been removed.

Breach Reporting

If there is a data breach – meaning someone who shouldn't have has seen or is in possession of the data -it is mandatory that you report it to the Information Commissioners Office (ICO), within 72 hours of the breach. They can be reached on 0303 123 1113.

Penalties for breaches

A breach could result in a fine for the employer. Details of the fines which can be imposed can be found at https://www.itgovernance.co.uk/dpa-and-gdpr-penalties

Registration with the Information Commissioners Office (ICO)

You do not need to officially register with the ICO as a data processor if you are only using personal data for Staff Administration. However, you must still comply with the all data protection obligations.

Record of Data Processing

You should consider whether to conduct a data processing audit and record in a formal Record of Data Processing document how you manage personal data.

Ask your Direct Payment Case Worker for a template 'Record of Data Processing' document

Brexit

The Government has confirmed that these rules will apply post Brexit.

Where can you get help?

Your insurance company will be able to advise you on how to ensure you are compliant with GDPR. Your Direct Payment Case Worker will also be able to advise you.