GDPR - Establishing the lawful basis for processing personal data

From 25th May 2018, you will no longer be able to rely upon data protection consent clauses in your contracts of employment as the lawful basis to process employee data.

You will now have to identify the lawful reasons for holding and processing personal data.

A template data protection policy will be available from the NTF in April 2018 which will contain helpful clauses for you to use in notifying your employees of why you process their data and the reasons for doing that but as a business you need identify why you process the data you hold and if there is a lawful reason for that processing.

Steps to take:

When you have completed your data audit, you then need to identify why you hold that data -so for example an employee's National Insurance and bank account details are held so that you can pay them and process their tax and National Insurance. You hold records of their working hours so that you can pay them the correct amount and show HMRC or the HSE that you comply with National Minimum Wage and Working Time Regulations.

You may find you have data which you cannot ascertain why you hold it – you should make a note of that and ensure that it is dealt with to decide if you can lawfully hold it or if you should delete it.

It may well be that you decide to cleanse certain data from your system if you cannot justify retaining it to avoid being in breach.

Lawfully processing data under the GDPR

Under the GDPR to process personal data you must satisfy at least one of the following conditions:

1. **Is it necessary for the performance of the employment contract or take steps to enter into a contract at an individual's request (e.g. processing job applications)?**

   This ground is likely to be of use for holding personal data to process salary or other benefits. What will be considered as "necessary" is not at this stage clear – and it may be that ground 4 below is more appropriate for general employment records such as data held on performance or disciplinary issues.

2. **Protecting the employee's vital interests**

   This is likely to be fairly limited but could be used for holding and processing information about emergency contact details or about an employee's allergies.

3. **Legal obligation: the processing is necessary for you to comply with your legal obligations**.

   This ground would be used for processing data to HMRC.

4. **Legitimate interest: the processing is necessary for the legitimate business interests of your business or a third party except where those interests are overridden by interest or fundamental rights and freedoms of individuals.**

   This is likely to be the most useful ground for processing employee data. However if you rely on this ground you have to tell the employee which specific interests are being pursued – so for example to comply with a contract or to run the business profitably. The employee has to be notified that they have a right to object to how you handle information for a specific purpose. The template data protection policy to be issued by the NTF in April will be of assistance to members in providing employees with this information.

5. **Consent: the employee has given clear consent for you to process their personal data for a specific purpose.**

   *You are advised **not** to use consent as a ground for processing personal data within the employment relationship as the Information Commissioner's Office has stated that it will be difficult for the employer to rely upon such consent given the imbalance in the relationship between the employer and employee (the balance of power being with the employer as to contract terms thereby making it difficult for an employee to freely consent).*

   From 25th May 2018 you cannot rely upon a blanket consent in an employment contract.

Special category data

Information about an employee's health is now 'special category data' (it used to be called sensitive data) and needs additional protection.

To be lawful, processing must meet one of the legal basis above and one from the special category list below, so

i. be for the purposes of performing or exercising obligations or rights of the employer or employee under employment law, such as not to discriminate against an

employee or dismiss them unfairly (it relates to legal rights or obligations, not contractual rights).

ii. be necessary for the purposes of establishing, exercising or defending legal claims

iii. be necessary for occupational medicine or assessing the working capacity of the employee (although consent will still be needed under the Access to Medical Records regulations as at present). The employer will need to have confidentiality safeguards in place.

v. be information which has been manifestly made public by the individual

v. Individual has given explicit consent for the specified purpose (although the Information Commissioner's Office has said not to use this ground for employment)

As mentioned above, during April the NTF will be producing a data protection policy template for members to use which will explain the procedures for complying with these principles and which members can put in place tailored to suit their own business requirements.