MATT GINGELL
020 3797 1264 | mattgingell@mattgingell.com

GDPR: HR guide

Description

Introduction

The EU General Data Protection Regulations (**GDPR**) came into force on 25 May 2018.

This guide sets out the main obligations for employers.

In the employment context, for the purposes of the **GDPR**, the employer will usually be the data controller and employees will be the data subjects.

Personal data

The **GDPR** applies to personal data. Personal data means any information relating to an identifiable person – who can be directly or indirectly identified.

Data protection principles

The data protection principles set out in the **GDPR** are as follows:

- Personal data must be processed lawfully, fairly and in a transparent manner.
- Personal data must be collected for specified, explicit and legitimate purposes and must not be processed in a manner which is incompatible with those purposes.
- Personal data must be adequate, relevant and limited to what is necessary for the purposes for which it is processed (which is a stricter requirement than under the previous law).
- Personal data must be accurate and kept up to date (where appropriate). This would now include correcting or removing inaccurate data.
- Personal data must be kept for no longer than is necessary for the purposes for which the data is processed (though there are a few exceptions).
- Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or

damage.
- The data controller must be able to show compliance with these principles (which is a new obligation of accountability).

Under the first data principle of the **GDPR**, data will only be processed lawfully if at least one of the conditions below is satisfied:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- The processing is necessary for the performance of a contract with the data subject or in order to take steps at the request of a data subject prior to entering into a contract.
- The processing is necessary to comply with a legal obligation of the data controller.
- The processing is necessary to protect the vital interests of the data subject or another person.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority which the data controller has.
- The processing is necessary for the purposes of the legitimate interests of the data controller or the legitimate interests of a third party, except where such interests are overridden by the interests and fundamental rights and freedoms of the data subject.

Consent needs to be freely given, specific and informed. The Information Commissioner's Office (ICO) has provided guidance stating that given the unequal bargaining power between the employer and the employee, employers will find it difficult to rely on consent, and employers are advised to identify another legitimate basis for processing data.

It is important to be aware that under the first principle of the **GDPR** transparency means that individuals have the right to be informed about the collection and use of their personal data. Employers should provide their employees with information including: the contact details of the the data controller, the purposes for processing their personal data, the categories of personal data (if received from a third party), the retention periods for that personal data, who the data will be shared with and the legal rights of the data subject. The privacy information (known as a privacy notice) should be provided at at the time of collecting the personal data. Privacy notices, for instance, should be used when applicants apply for jobs, for references, when new starters join the organisation and when information is collated as part of disciplinary and grievance procedures.

The GDPR and special categories of personal data

For special categories of data it is necessary to satisfy one of the conditions above as well as one of the separate conditions (see below). The special categories of data under the **GDPR** are those revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic and biometric data
- Health
- Sex life or sexual orientation

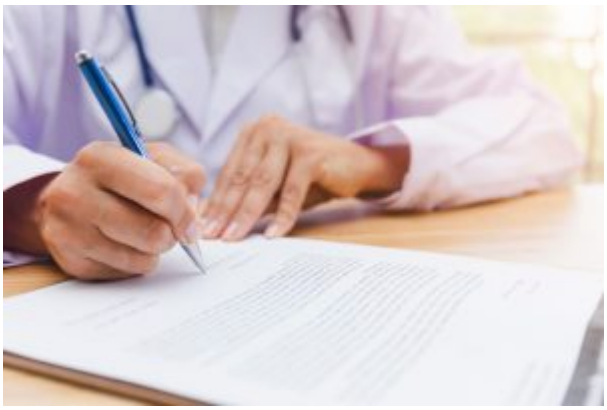
The separate conditions include:

- Where the data subject has given explicit consent.
- Where it is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment law.
- Where it relates to personal data which has been clearly made public by the data subject.

Here is the full list.

The ICO has indicated that explicit consent is unlikely to be very different from the standard consent.

Again, employers are unlikely to be able to rely on specific consent for the purposes of the **GDPR**. So, for example, where an employer is requiring an employee to attend a medical examination and a medical report be prepared, although consent will clearly be needed, consent cannot be relied on for processing the data. An employer will therefore have to rely on another exception such as the one concerning carrying out obligations under employment law.



Accountability

Employers need to demonstrate that they are complying with the **GDPR**. This may include employers:

- Having detailed data protection policies.
- Carrying out internal audits.
- Keeping records on processing (which is usually only mandatory for employers who have at least 250 employees).
- Undertaking a data protection impact assessment (which is compulsory where the type of processing involves a high risk to the rights and freedoms of individuals).
- Training staff on data protection issues.
- Ensuring internal processes are kept up to date.
- Appointing a data protection officer (which in some circumstances is mandatory) or at least appointing someone with responsibility for overseeing data protection compliance.

Employers also have an obligation to report a personal data breach (which means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of,or access to, personal data). This must be done within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the employer must also inform those individuals without undue delay.

Enforcement and consequences of any breach of the GDPR

The ICO may serve on employers information notices, assessment notices, enforcement notices and penalty

notices. Data subjects may complain to the ICO for breaches, and data subjects also have the right to receive compensation from the data controller for damages.

This guide is intended for guidance only and should not be relied upon for specific advice.

If you need any advice on the **GDPR** or have queries relating to other employment law issues please do not hesitate to contact me on 020 3797 1264.

Do check mattgingell.com regularly for updated information.