GLAISYERS ETL GLOBAL

PART 1

Employment Guide to GDPR

What is 'personal data'?

Personal data is any information which by itself or in combination with other information allows you to identify an individual. In the case of employee personal data, this can include a wide range of information ranging from the obvious such as name, address, and date of birth, to less obvious examples such as information gathered from employee monitoring (website activity, telephone calls and e-mail activity), CCTV footage, appraisal records, medical fit notes and background check information (references, qualifications etc).

What is 'sensitive personal data'?

Sensitive personal data includes information relating to a data subject's racial or ethnic origin, political opinions (for example Union membership), religious and philosophical beliefs (holding records of individuals who take certain religious holidays) and information relating to employees' health, sex life or sexual orientation such as medical reports.

What is 'processing'?

GDPR states processing can cover collecting, recording, organising, storing, using, disclosing or disseminating data. If you hold employee data, even if you do not actively do anything with it, you are processing for the purposes of GDPR.

One of the practical obstacles employers need to overcome is that most employee data is unstructured which creates challenges when employers try to comply with the various data principles. As an example, the text of an e-mail may hold personal data about the sender, the recipient and a third party and in certain instances, some of it may contain sensitive personal data, for example, "Sorry I can't make the meeting, my daughter has chicken pox" or "I wish to raise a complaint regarding the way in which one of my colleagues has been treated by others on the grounds of his sexual orientation".

As a data controller, it is very hard for employers to have control over unstructured data like this in comparison to commercial data collected which is often in a far more predefined structured format. The starting point in managing compliance involves carrying out an audit of all processing of data to establish what is being held. Only then can you start to check whether the processing of that data is lawful and GDPR compliant.

Data Protection Principles

There are a number of principles which form the core of an employer's obligations as a data controller. Failure to comply with the principles will usually form the basis of any GDPR breach.

Transparency
Personal data must be processed lawfully, fairly and in a transparent manner. Amongst other things, this involves explaining to employees what kind of data you hold about them, why you need it, what you intend to do with it, and how long you intend to keep it.

Purpose Limitation
You should only collect personal data for specified explicit legitimate purposes and having obtained the information on this basis, you must not process it in any manner incompatible with those purposes.

Data Minimisation
The personal data you collect must only be what is necessary in relation to the purpose for which you are processing. This means you should not request data if you don't have a good reason to hold it and shouldn't, for example, collect data for some general or unspecified purpose.

Accuracy
All personal data must be accurate and kept up to date. It is your obligation to ensure that any inaccurate data is rectified or erased.

Storage Limitation
You mustn't retain personal data for any longer than necessary. As an example, there is no need to retain copies of employees' job applications, references and qualifications once these have been checked and the individual has commenced employment. There is no justification in holding this information on the off chance it might transpire at some point in the future that the employee has lied during the recruitment process.

Integrity and Confidentiality
Personal data must be processed in a way which ensures its security in order to protect it against accidental loss, destruction, damage or disclosure. This involves introducing systems to protect data ranging from password protection and encryption to restricting access to only those who require use of the data.

Accountability
As a data controller, you are responsible for and must demonstrate compliance with all of the above principles.

Manchester Office:
One St. James's Square
Manchester
M2 6DN
T: 0161 832 4666

London Office:
Pinners Hall
103-105 Old Broad Street
London, ECNZ 1ER
T: 0207 842 8000

www.glaisyers.com | 0161 832 4666 | hello@glaisyers.com