GDPR & the UK Data Protection Bill

GDPR is the European General Data Protection Regulation and changes the way companies and public sector organisations can handle their customers' 'Personal Data'. (See UK Information Commissioner's Office https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr).

The UK Data Protection Bill largely includes all GDPR European privacy laws but will be the UK view of GDPR when it enters the UK statute books post Brexit. (See UK Information Commissioner's Office https://ico.org.uk/for-organisations/data-protection-bill).

Both address the massive increase of digital information we create, capture & store, and represents the biggest change in data protection rules since they were created in the 1990's. All UK organisations will need to comply with GDPR from 25th May 2018 and the UK Data Protection Bill will replace the UK Data Protection Act 1998 (DPA) post Brexit. This means that ignoring GDPR could lead to large fines.

Summary definitions

Data Subject means an individual who is the subject of personal data.

Personal Data: According to the European Commission "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

(Personal data can even when individuals are not identified by name, but bear unique reference numbers which can be matched to the individuals concerned. Plus, if it's possible that a person could be identified by a pseudonym, pseudonymised personal data can also fall under the law.)

> ***Example 1****) opinions about the individual, or what is intended for them:*
>
> A manager's assessment or opinion of an employee's performance during their initial probationary period will, if resulting information is to be entered into any computer based system, be personal data about that individual. Similarly, if a manager emails that an employee must do remedial training that will also be personal data.

Example 2) An organisation holds personal information in paper records:

Paper records which are held in an organised filing system structured either by reference to individuals or by criteria relating to individuals which allows ready access to specific information about a particular individual will be personal data.

Data controller means a person or entity who determines the purposes and manner in which any personal data is used, or will be used. (Term also applies when two or more persons or entities act together).

Any organisation (or individual) which has the authority to decide how personal data is to be processed is a data controller.

Example: Any organisation with employees such as a Utilities company.

Data processor, in relation to personal data, means the person or group that processes (obtaining, recording, adapting or holding) the data on behalf of the data controller.

Data processors include accountants, payroll companies and call centres, all of which could hold or process personal information on behalf of someone else. "Cloud" service providers are usually data processors.

Example 1) A utilities company engages a call centre company to provide its customer services functions. The call centre staff have access to the utility company's customer details but may only use the information they contain in accordance with strict contractual arrangements. The utilities company remains the data controller. The company that operates the call centre is a data processor.

Example 2) An organisation employs a business services company to take care of its employee payroll. The organisation also engages a marketing company to carry out a customer satisfaction survey. The business services company will need information about the organisation's employees, and the marketing company will need information about its customers. Both companies will be processing the information on behalf of the organisation, and so they are both data processors.

Remember, all organisations mentioned above will be processing personal data regarding their own employees, so they will also be data controllers.

Data controllers & Data processors must ensure compliance to the new UK Data Protection Bill & GDPR. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.