NMT HR SERVICES LTD

INTRODUCTION TO THE DATA PROCESSING AND THE GENERAL DATA PROTECTION REGULATIONS (GDPR)

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU **will not** affect the commencement of the GDPR.

All organisations have to get ready for the new data protection rules, but small businesses in the UK face particular challenges:

- Where to start
- Potentially less time and money to invest in getting it right.
- Potentially less likely to have compliance teams, data protection officers or legal experts to advise them what to do.

The Information Commissioner's Office (ICO) is a non-departmental public body which reports directly to Parliament and is sponsored by the Department for Digital, Culture, Media and Sport. Their role is to uphold information rights in the public interest and they hold a register of data controllers that includes details of organisations that process personal data. Among other things, they handle complaints relating to Data Protection and take actions to improve the behaviour of those who handle personal data.

Any individual or organisation handling, controlling and/or processing personal data is required to register with the ICO. Failure to do so could result in the individual / organisation facing a fine for non-declaration. Registering can be done on line via the ICO website: https://ico.org.uk/for-organisations/register/

To ascertain if you need to register, you can complete a simple self-assessment, via: https://ico.org.uk/for-organisations/register/self-assessment/

This first blog is an introduction to the key themes of the GDPR to help organisations understand the new legal framework. Subsequent blogs will look at preparing for the change to regulations next year.

Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors' (*). The definitions are broadly the same under the current Data Protection Act 1998 (DPA) – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR

  If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. **These obligations for processors are a new requirement under the GDPR.**

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

(*) *"Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.*

A data controller must be a "person" recognised in law, that is to say:

- *Individuals;*
- *Organisations; and*
- *Other corporate and unincorporated bodies of persons*

Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

Example: A network of town-centre CCTV cameras is operated by a local council jointly with the police. Both are involved in deciding how the CCTV system is run and that the images of it captures are used for. The council and the police are therefore joint data controllers in relation to personal data processed in the operating system.

"Data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. "Processing", in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisations, adaptation or alterations of the information or data,
- Retrieval, consultations or use of the information or data,
- Disclosure of the information or data by transmission, dissemination or otherwise making available, or
- Alignment, combination, blocking, erasure or destruction of the information or data.

Example: An organisation engages a company which provides business services to administer its employee payroll function. The organisation also engages a marketing company to carry out a satisfaction survey of its existing customers. 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. However, they may also be processing personal data about their own employees, and, in respect of that personal data,

they will be data controllers.

To establish whether you are a data controller or a data processor, go to the following link on the ICO website:

https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

What is personal data?

Personal data means data which relate to a living individual who can be identified:

- From those data, or
- From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and
- Includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".

Example:
An organisation holds data on a spreadsheet. The spreadsheet records do not identify individuals by name, but bear unique reference numbers which can be matched to a card index system to identify the individuals concerned. The information held on the spreadsheet records is personal data.

The definition also specifically includes opinions about the individual, or what is intended for them.

Example:
A manager's assessment or opinion of an employee's performance during their initial probationary period will, if held as data, ne personal data about that individual. Similarly, if a manager notes that an employee must do redial training, that note will, if held as data, be personal data.

Therefore, if you hold information about individuals either on computer or in certain types of filing system you may be holding 'personal data'.

Broadly speaking the DPA covers four types of information (referred to as 'data' in the Act):

- Information processed, or intended to be processed, wholly or partly by automatic means (That is information in electronic form usually on computer),
- Information processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is usually paper records in a filing system),
- Information that forms part of an 'accessible record' (that is, certain health records, educational records and certain local authority housing or social services records, regardless of whether the information is processed automatically or is held in a relevant filing system), and

- Information held by a public authority (referred to as 'category 'e' data' as it falls within paragraph (e) of section 1(1) of the DPA)

Further guidance on personal data can be found at: https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf

What is sensitive personal data?

Sensitive personal data means personal data consisting of information as to –

- The racial or ethnic origin of the data subject,
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature,
- Whether they are a member of a trade union (within the meaning or the Trade Union and Labour Relations (Consolidations) Act 1992),
- Their physical or mental health or condition,
- Their sexual life
- The commission or alleged commission by them of any offence, or
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. In particular, if you are processing sensitive personal data you must satisfy one or more of the conditions for processing which apply specifically to such data, as well as one of the general conditions which apply in every case. The nature of the data is also a factor in deciding what security is appropriate. Further information is available on the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/

There are many more elements to the DPA. These include who are "Data Subjects", their rights (including their rights to access any data held relating to them), along with how long records should be held for. All of these will be covered in separate blogs.

NMT HR SERVICES LTD

https://www.linkedin.com/in/nicolemaxinethompson/

https://www.facebook.com/nmthrservicesltd/

