PENINSULA

GENERAL DATA PROTECTION REGULATION

Guidance Notes

What is the GDPR?

Currently, the law on data protection requiring the handling of data which identifies people to be done in a fair way, is contained in the Data Protection Act 1998 (DPA).

The EU will introduce new legislation, called General Data Protection Regulation (GDPR) that will replace the current EU structure on the handling of data. Because of this, the UK Government will introduce a new Data Protection Act to replace the current one.

The new Act, which will implement the requirements of the GDPR in the UK, will come into effect no later than 25th May 2018 which is the date that GDPR will apply to all EU member states.

Despite the fact that the UK will leave the EU in 2019, the Government has confirmed that GDPR will still take effect in the UK.

The Information Commissioner's Office (ICO) is the authority responsible for ensuring compliance with the law on data protection. It publishes good practice guidance for data controllers and data processers (see Key Definitions later) to assist compliance. Current ICO guidance on GDPR makes up this guidance note.

Why is the law changing?

It had become increasingly clear that the current statutory framework was not "fit for purpose". Personal data is now being used in ways that were not envisaged in the mid 90s, mainly down to the growth of the internet and the changes in online activities. Social media, advertising and email marketing are a few examples of areas in which personal, and sometimes sensitive, data is hosted and processed using principles that are not appropriate or safe.

Key principles

The current Data Protection Act sets out eight principles for the processing of data. These will remain once GDPR is introduced. They are:

- Data must be processed fairly and lawfully;
- Data must only be obtained for specified and lawful purposes;
- Data must be adequate, relevant and not excessive;
- Data must be accurate and up to date;
- Data must not be kept for longer than necessary;
- Data must be processed in accordance with the "data subject's" (the individual's) rights;
- Data must be securely kept;
- Data must not be transferred to any other country without adequate protection in place.

In addition the GDPR contains the following changes:

- Enhanced documentation to be kept by data controllers;
- Enhanced privacy notices;
- More detailed rules regarding 'consent';
- Mandatory data breach notification requirements;
- Enhanced data subject rights;
- New obligations on data processors;
- Expanded territorial scope;
- Appointment of Data Protection Officers;
- Significant increases in the size of fines and penalties for non-compliance.

Many of the implications of the new GDPR will affect companies on a commercial level. However, it also has an impact on the following areas from a HR/employment perspective:

- Documentation to be kept by data controllers;
- Data subject rights;
- New obligations on data processors and appointment of data protection officers;
- Data breach notification requirements;
- Fine and penalties for non-compliance.

Key definitions

Personal data – Under GDPR, this means "any information relating to an identified, or identifiable

PENINSULA

natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Special Categories of Personal Data (what we currently call "Sensitive" Personal Data) – Under GDPR, this will mean data relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Physical or mental health conditions;
- Sex life or sexual orientation;
- Genetic data;
- Biometric data.

Data subject – in both DPA and GDPR, this means the subject of personal data. It doesn't include deceased individuals or an individual who can't be identified/distinguished from others. You would need to show pure anonymity in order that a subject would not be caught.

Data controller – the data controller is the decision maker. Under the GDPR the data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.

Data processor – under GDPR this is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. This person acts only under instruction of the data controller, keeping personal data secure from unauthorised access, loss or destruction.

Processing – in both pieces of legislation this means the obtaining, recording or holding of information or data or the carrying out of any operation or set of operations on the information or data, including: access, storage, retrieval, disclosure and erasure/deletion.

Documentation to be kept by data controllers

Personal data should only be kept where there is a legitimate interest, such as a contractual or statutory requirement. Once obtained it should be used for a specific and lawful purpose without being processed any further. Any personal data should be limited to only that which is relevant.
In practical terms, employers should not ask for personal or sensitive data relating to an employee unless they can demonstrate a lawful, fair or obvious reason for it. Any personal data that is held in relation to an employee should be accurate, kept up to date and only held for as long as is necessary.

GDPR states: [data should be kept for] "no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals."

Employee rights

Data subjects (your employees, in this context) have the following rights under the GDPR:

- The right to be informed;
- **The right of access;**
- **The right to rectification;**
- **The right to erasure;**
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

Those highlighted bold are those most pertinent to the HR function.

The right of access. This is what we currently know as a subject access request. This gives individuals a right to request production of data held on them. Right now, a request must be complied with within 40 days (unless an exemption applies) and employers can charge the employee a £10 fee. Under GDPR, the rules will be different.

Information will have to be provided as soon as possible and within one month at the latest, which can be extended by a further 2 months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Employers will not normally be able to charge a fee, however, ICO guidance states that "you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive". They also advise that "You may charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information". For example, this may be when the employee asks for a copy of the information to be sent to them, and another copy to be sent to their legal adviser.

The following information needs to be produced:

- A description of the personal data, the purpose for which it is processed, recipients, retention period and rights of rectification, erasure, restriction and objections.
- A copy of the information comprising the data.
- Details of the source of the data.

The right of rectification. Individuals are entitled to have inaccurate data rectified without undue delay. The ICO guidance states that this should occur within 1 month, or 2 months for complex requests. If no action is to be taken, employers must explain why to the individual, informing them of their right to complain and to a judicial remedy.

Employers would also need to consider, from a separate perspective, how the error occurred in the first place.

The right to erasure ('the right to be forgotten'). This enables individuals the right to request that personal data be deleted or removed where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten' and can occur where, for example:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- The individual withdraws consent.

Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

Consent

Except where a lawful basis already applies, data controllers must obtain the consent of the data subject in order to process their data.

Where consent is required, it will have to be a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Consent will have to be obtained via free-standing notices rather than being held within an employee handbook, for example.

When obtaining consent, certain pieces of information will need to be included i.e.:

- The identity of the data controller;
- What the data is processed for (some processes will require their own specific consent);
- How the data is processed;
- The right to withdraw consent at any time.

The Information Commissioner is currently creating guidance to assist data controllers with how to obtain consent, however, this has not yet been finalised.

New obligations on data processors and appointment of Data Protection Officers

The introduction of "accountability" makes the data processor responsible for demonstrating that they comply with the GDPR principles. Businesses will need to:

- Implement measures to ensure and demonstrate compliance;
- Maintain documentation/records on processing activities;
- Where appropriate appoint a Data Protection Officer (DPO);
- Use data protection impact assessments (DPIA).

As well as the obligation to provide comprehensive, clear and transparent privacy policies, if an organisation has more than 250 employees, employers must maintain additional internal records of their

processing activities. Organisations with less than 250 employees are only required to maintain records of activities related to higher risk processing, such as:

- Processing personal data that could result in a risk to the rights and freedoms of individual; or
- Processing of special categories of data or criminal convictions and offences.

What do organisations need to record?

- Name and details of your organisation (and where applicable, of other controllers, your representative and Data Protection Officer);
- Purposes of the processing;
- Description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
- Retention schedules;
- Description of technical and organisational security measures.

The GDPR requires organisations to appoint a Data Protection Officer (DPO) if you:

- Are a public authority or body (other than a court);
- Carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

The DPO can be an existing employee whose responsibilities lend themselves to taking responsibility for GDPR compliance. Alternatively, employers may wish to recruit or contract the role out externally.

GDPR does not require DPOs to have any specific qualifications to undertake the role, but it does stipulate that they have professional experience and knowledge of data protection law appropriate to the type of processing an organisation carries out.

One DPO may be responsible for a group of companies.

Employers who do not meet the definition of a company who requires a DPO may still choose to appoint one due to the increased focus on accountability in GDPR.

A DPO must report into the highest level of management within the organisation (ie board level) and have adequate resources provided to enable them to meet their GDPR obligations. A DPO should not be dismissed or penalised for performing their tasks.

Data breach notification requirements

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. It may include:

- Inappropriate access controls (not using passcodes) which allow unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as fire/flood;
- Hacking attack.

A breach must be reported within 72 hours of its discovery. Employers will be permitted to provide information in phases where a full investigation is not possible within that timeframe.

It is likely that employers will need to have a policy on reporting breaches under GDPR. All those within an organisation who are responsible for complying with GDPR will have to be aware of the circumstances under which a breach must be notified, and how it must be done.

In some cases, the individual whose data is involved in the breach must also be notified i.e. where the breach is likely to result in a high risk to the rights and freedoms of individuals.

Fine and penalties for non-compliance

A maximum fine of up to €10 million or 2% of global turnover (whichever is greater) can be applied where the following occurs:

- Failure to maintain records of processing activities;
- Failure to appoint a DPO;
- Processing data without consent of the data subject;
- Failure to notify a breach to the supervisory authority or the data subject;

- Failure to carry out a data protection impact assessment in relation to high risk processing of personal data.

A maximum fine of up to €20 million or 4% of global turnover (whichever is greater) can be applied where the following occurs:

- Failure to provide data subjects with transparent information in a concise, intelligible and easily accessible form for the existence of their rights under GDPR;
- Failure to demonstrate that the data subject has consented to the processing of his/her data;
- Failure to comply with the rights of access, rectification and erasure;

The above lists are not exhaustive.

How to prepare

The ICO's "12 steps to take now" guidance sets out the following areas that employers should consider:

1. Awareness – let the relevant people in your organisation know that the law is changing
2. Information audit – check what data you hold and who you share it with
3. Privacy information – check your current privacy notices and make a plan for change
4. Individuals' rights – check how you currently comply with individuals' rights e.g. complying with a subject access request or deleting personal data
5. Subject access requests – plan how you will make changes to the process when the new law is here
6. Lawful basis – check you have a lawful basis for processing data. Employers who process data for employment purposes are likely to be able to rely on the lawful basis of "performance of a contract" for most data processing, but potentially not all processing
7. Consent – review how you obtain consent for processing data
8. Children – reviewing procedures for verifying ages and obtaining parental/guardian consent (not likely to have a great impact on the area of employment)
9. Data breaches – review how you would notify a breach
10. Impact assessments – consider how to implement data protection impact assessments
11. Data Protection Officer – do you need a DPO? Who will ensure your compliance with GDPR?
12. International – If you operate in more than one member state, determine a lead data protection supervisory authority.

Our HRface2face service consists of a team of advocates equipped to conduct, or support and assist you to conduct, any face to face meeting you are undertaking with your staff. For further information please speak to your HR Expert and visit: www.peninsulagrouplimited.com/services/hr/hr-face2face

Occupational Health intervention and Employee Assistance Programmes are essential tools to effectively manage absence in the workplace, to support staff and to add value to your business. We can provide you with the details of Health Assured, a company who can provide such services. For further information please speak to your HR Expert and visit: www.healthassured.co.uk

Need Further Advice?

T: 0844 892 2772 E: advice@peninsula-uk.com W: peninsula-uk.com