PENINSULA

Main principles of GDPR

Guidance Notes

Definitions of data under GDPR

The GDPR will place obligations on 'data controllers' and 'data processors'. The 'controller' determines the purposes and means of processing the data; the 'processor' is responsible for processing personal data on behalf of the controller.

'Personal data' is any information relating to an identifiable person ('data subject') who can be directly or indirectly identified by reference to that information and, under GDPR, will include location data or an online identifier eg IP address. In HR terms, data subjects will be an organisation's employees.

Data known as 'sensitive data' under existing definitions is known under GDPR as 'special categories of personal data', including genetic and biometric data but not data relating to criminal convictions.

GDPR covers data which is kept by automated means and manual filing systems where personal data are accessible according to specific criteria, potentially including information ordered according to its chronology.

Data protection principles

There are six data protection principles under GDPR rather than the eight existing ones. Essentially a re-write of the originals, the principles under the GDPR are that data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects 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 and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Individual rights

Data subjects have the following rights regarding their personal data under the GDPR:

- the right to be informed
- the right of access
- the right to rectification
- the right to erase or "the right to be forgotten"

- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling

Lawful basis for processing

Personal data can only be processed where there is a **lawful basis** to do so and organisations must determine the lawful basis is for each processing activity before processing begins. The lawful basis which applies to each processing activity needs to be identified in certain pieces of documentation, eg in privacy notices and responses to subject access requests.

There are six lawful bases for personal data are:

- consent
- legitimate interests
- performance of a contract
- legal obligation
- vital interests
- public task

The lawful basis for processing sensitive data are:

- valid explicit employee consent
- necessary for carrying out employment rights and obligations, it is authorised by domestic or EU law and the employer has an appropriate policy document in place
- necessary to protect the vital interests of the employee or another person where the employee is incapable of giving consent
- processing by a foundation, association or not-for-profit with a political, philosophical, religious or trade union aim
- if the employee has made the personal data public
- necessary for the employer to establish or defend legal claims
- necessary for reasons of substantial public interest (including the processing of personal data revealing race, religious beliefs, health or sexual orientation for the purposes of promoting equality of treatment, and including processing necessary to determine eligibility for or benefits payable under an occupational pension scheme which can reasonably be carried out without the employee's consent), and the employer has an appropriate policy document in place
- necessary for the assessment of the employee's working capacity either on the basis of domestic or EU law or pursuant to a contract with a health professional, and subject to confidentiality safeguards.

You can read more on each lawful basis in our guidance note on "Determining a lawful basis for data processing".

Consent

Unless another lawful basis applies, organisations generally use that of 'consent' to process the data of their employees. However, the rules on obtaining consent are much more stringent under GDPR than under current rules.

Consent must be freely given, informed and unambiguous. It requires positive opt in meaning that organisations cannot use default methods including pre-checked boxes. Employees must be given detailed information on what their consent is being obtained for; the types of processing activity and the name of the controller. Blanket consent to cover many different aspects of processing will not be sufficient.

Documents used to obtain consent should be separate from other terms and conditions in order to ensure data subjects are acutely aware of the consequences of their actions. Data subjects must be informed of their right to withdraw their consent at any time and there must be no repercussions from withdrawal.

The Information Commissioner recognises that the free giving of consent may be compromised by the employer-employee relationship in that employers are in a position of power over individuals and so employees may feel they have no choice but to provide consent in order to gain or continue employment. Because of this, the ICO recommends organisations avoid relying on

consent as a lawful basis unless there is evidence that it has been freely given.

Privacy notices

As part of the enhanced accountability provisions, organisations will have a general obligation to implement measures to show that data protection is a primary concern in processing activities. A privacy notice can be used to do this.

The privacy notice is one of the most important documents in GDPR compliance. It tells your employees exactly what types of data about them that you hold e.g. their name and other personal details, their previous employment history and other information included on a CV, their training records and disciplinary records etc. It also sets out the lawful basis for each type of data you hold.

It is important that employees have easy access to your privacy notice. It is also important for job applicants to see a privacy notice that relates to the data you hold on them too.

Data protection impact assessments

You must, in certain circumstances, carry out a data protection impact assessment to help them identify the most effective way to comply with their data protection obligations. This is part of the concept of "privacy by design" involved in GDPR.

An impact assessment must be carried out when you:

- use new technologies and
- the processing is likely to result in a high risk to the rights and freedoms of individuals. This can include systematic and extensive processing activities; large scale processing of special categories of data (currently known as 'sensitive' data) or large scale systematic monitoring of public areas.

An impact assessment should include:

- a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate compliance

Data Protection Officer

A new requirement under the GDPR is that you must appoint a Data Protection Officer (DPO) where certain criteria are met. Whilst all organisations may choose to have a DPO, it will be a legal requirement in the following circumstances:

- where the organisation is a public authority or body (except for courts acting in their judicial capacity)
- where the core activities of the organisation consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- where the organisation carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

The key terms are defined below:

"Public authority or body" - a public authority or body is considered as one that is governed by national law. This concept is however not limited to national, regional and local authorities as under the respective national laws this may also include a range of other bodies that are governed by public law.

"Core activities" - these are described as the key operations necessary to achieve the controllers or processors goals.

"Regular and systematic monitoring" - Regular is defined as: (i) ongoing or occurring at particular

intervals for a particular period, or (ii) recurring or repeated at fixed times, or (iii) constantly or periodically taking place.

"Systematic" is defined as: (i) occurring according to a system, or (ii) pre-arranged, organised or methodical, or (iii) taking place as part of a general plan for data collection, or (iv) carried out as part of a strategy. Examples of activities that may constitute regular and systematic monitoring include email retargeting, data-driven marketing, profiling and scoring for purposes of risk assessment for detection of money-laundering.
"Special categories of data" - these consist of personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The DPO can be an existing employee (no specific qualifications are required but the individual should have professional experience and knowledge of data protection law) and one DPO can act for a group of companies. The role must report directly to the highest level of management and must be given adequate resources to carry out the role. He/she should not be dismissed or penalised for undertaking the tasks required by the role. The role may also be contracted out.

It will be the role of the DPO to:

- inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)

Reporting breaches

A personal data breach has a wider definition than simply losing personal data. It is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It may include a hacking attack or human error eg sending information to the wrong email address.

Reportable breaches must be reported to the relevant supervisory authority (this will be the Information Commissioner unless the data is transferred to another country) without undue delay and within 72 hours of discovery. Organisations will be permitted to provide information on the breach in phases where a full investigation is not possible within that timeframe.

A reportable breach is one which is likely to result in a risk to people's rights and freedoms. If this is not a likely consequence, the breach does not need to be reported.

If there is a high risk to people's rights and freedoms, the affected individual(s) will also need to be notified. This may be, for example, where an individual may be discriminated against, suffer financial loss or detriment to reputation or other social or economic disadvantage. Where the breach is such that the public need to be informed, this should be done without delay.

Guidelines will be made available on assessing the threshold of a breach. Failure to report can lead to a fine of up to €10million or 2% of your organisation's global turnover.

Fines

A breach of GDPR carries a maximum fine of €20million or 4% of your organisation's global turnover.

When assessing the level of a fine, the following will be considered:

- the nature, gravity and duration of the infringement including the purpose of the processing, the number of people

affected by the breach and the level of damage to their rights
- the intentional or negligent character of the breach, meaning whether the controller knew of the breach and acted wilfully, or whether there was no intention to cause a breach
- any action taken to mitigate the damage suffered by data subjects. Organisations should do whatever they can to reduce the consequences of the breach for those concerned
- the degree of responsibility of the controller or processor taking into account measures implemented by them eg has the organisation implemented measures to follow the principles of design and default?
- relevant previous infringements or whether the data controller is already on the supervisory authority's "radar"
- degree of cooperation with the supervisory authority to remedy the breach
- the type of personal data affected by the breach
- whether the data controller notified the breach
- the controller's adherence to codes of practice and approved certification mechanisms
- any other aggravating feature of the breach
- the extent to which the data controller notified the supervisory authority of the breach and its cooperation with that authority subsequent to the breach

In some cases, organisations may receive a reprimand instead of a fine. This may be, for example, where the breach does not pose a risk to the rights of data subjects eg "a minor infringement" or where the data controller is a natural person and the imposition of a fine would be a disproportionate burden.

Record keeping

Organisations with 250 or more employees will have an obligation to keep internal records on their processing activities. The following information must be recorded:

- 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 and
- a description of technical and organisational security measures.

Organisations with fewer than 250 employees must keep records of high risk activities where the processing could result in a risk to the rights and freedoms of individuals, or where special categories of data or criminal convictions are involved.

A HR Data Record has been provided in your GDPR suite.

Registration with the ICO

Unless exempt, all organisations that process personal data are required to register with the ICO. Fees are attached to the registration process: the fee structure will change upon GDPR implementation on 25 May 2018. The new charging structure does not necessarily mean that registration must be renewed on this date. Current registrations will continue to run until they are expired.