The European General Data Protection Regulation (GDPR)
Overview

From 25 May 2018, the General Data Protection Regulation (GDPR) will replace the UK's current statutory framework on managing data protection. Let's consider what data actually means:

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Personal data

- **The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier**.
- This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
- The GDPR applies to **both automated personal data and to manual filing systems** where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
- Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

- The GDPR refers to sensitive personal data as "special categories of personal data".
- The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
- Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

All organisations with professional or commercial activity (whether or not payment is received for that activity) will have to comply with GDPR regardless of their size, provided that they process personal data.

All Domiciliary Care Agencies, Care Homes etc. must comply with the new Regulation.

Severe fines will be applied to certain types of data breaches which will have to be reported to the supervisory authority within strict deadlines.

A new Data Protection Act will be introduced by the UK Government to replace the Data Protection Act 1998. This Act is not currently finalised.

The new Act will not remove the existing data protection principles, however, the new rules will mean that organisations will need to consider data protection in every aspect of new projects e.g. "by design and default" and **some will need to appoint a specific Data Protection Officer to ensure compliance.**

Greater significance will be placed on accountability meaning that processes and procedures will need to be put in place to show that data protection is at the forefront of an organisation's processes.

All organisations with professional or commercial activity (whether or not payment is received for that activity) will have to comply with GDPR regardless of their size, provided that they process personal data.

All Domiciliary Care Agencies, Care Homes etc. must comply with the new Regulation.

The UK's exit from the European Union <u>will have no effect</u> on the application of the GDPR; it will still apply.

Definitions

- 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 e.g. 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.

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.

- 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 Officer

A new requirement under the GDPR is the appointment of a Data Protection Officer (DPO) by an organisation 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 (except for courts acting in their judicial capacity);
- where the organisation carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- where the organisation carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

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 ensure the organisation is aware of its obligations under the GDPR and that it puts in place appropriate processes to ensure compliance.

First impressions suggest that a Domiciliary Care Agency or Care Home (unless part of a large group) will not, by itself, need to appoint someone to this position, although this should be clarified with, for example, the ICO, and by reference with individual circumstances. As has already been mentioned, an organisation may choose to have a Data Protection Officer if it wishes.

Individual rights

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

- **The right to be informed**. Individuals should receive certain information about the processing of their data, such as the categories of data and the purpose of processing. The information must be concise, transparent and written in clear and plain language. A fee cannot be charged for providing this.

- **The right of access**. Individuals have the right to access their personal data and other supplementary information. A fee can only be charged in certain circumstances (see Access to data).

- **The right to rectification**. Individuals have the right to rectify their personal data if it is inaccurate or incomplete. A request for rectification must be responded to within 1 month, or 2 months if the request is complex.

- **The right to erase or "the right to be forgotten".** Individuals can request removal or deletion of personal data where there is no compelling reason to keep processing the data. This includes where consent is withdrawn.

- **The right to restrict processing**. Individuals have the right to restrict or block processing of personal data in specific circumstances, including where the accuracy of the data is questioned. The personal data can continue to be stored but no further processing can take place.

- **The right to data portability**. Individuals can obtain their personal data for personal use across different services. A fee cannot be charged and requests must be responded to without delay and within 1 month, or 2 months if the request is complex.

- **The right to object**. Individuals have the right to object to the processing of personal data in specific circumstances, including for processing on the basis of a legitimate interest or direct marketing.

- **Rights in relation to automated decision making and profiling**. Individuals have rights regarding decisions made without human intervention that have a significant effect on the individual. This right does not apply to all automated decisions, including where these are authorised by law

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:

1. **processed lawfully**, fairly and in a transparent manner in relation to individuals;

2. 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;

There are six data protection principles under GDPR rather than the eight existing ones.

3. **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

4. **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;

5. **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

6. **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."

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 before processing begins. The appropriate lawful basis needs to be identified in certain pieces of documentation as a result of a data subject's right to be informed, e.g. in privacy notices and responses to subject access requests. There are six lawful bases:

- Consent
- Legitimate interests
- Performance of a contract
- Legal obligation
- Vital interests
- Public task

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.

- **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 ICO 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.

- The Article 29 Working Party will produce further guidelines on obtaining consent under the GDPR once it finalises its response to a closed consultation exercise.

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 as part of a data protection compliance system. A notice under GDPR needs to be more detailed than under current provisions; the ICO recommends that organisations:

- include concise, transparent, intelligible and easily accessible information on how data is processed;
- write in clear and plain language;
- provide it free of charge.

When the data is obtained directly from the data subject, the GDPR requires the following to be included in a privacy notice:

- identity and contact details of controller and the controller's Data Protection Officer;
- the purpose of the processing;
- the legitimate interests of the controller of third party where applicable;
- the categories of personal data;
- recipient or categories of recipient of the personal data;
- details of transfers to third country and safeguards;
- retention period or criteria used to determine the retention period;
- the existence of each of the data subject's rights;
- the right to withdraw consent at any time;
- the right to lodge a complaints with a supervisory authority;
- the source of the personal data and whether it came from a publically accessible source;
- the existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

Data protection impact assessments

Organisations 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.

An impact assessment must be carried out when an organisation:

- uses 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.

Access to data

Employees have the right to access their data under existing data protection laws and this is known as a subject access request.

Employees have the right to access their data under existing data protection laws and this is known as a subject access request. This right will remain under the GDPR but the administrative system will be changed. Employees have a right to know whether or not their employer is processing personal data about them. If the employer is processing data, the employee has a right to know:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom data has been or will be disclosed;
- the period during which personal data will be retained;
- information on the source of the data;
- information regarding complaints and disputes: the right to complain to a supervisory authority, the right to request rectification or erasure of personal data, to object to processing of data or to restrict that processing; and
- information on any safeguards where personal data is transferred outside the EEA.

It is a common misconception that employees have a right to see a copy of documents; this is not the case.

They have a right see their personal data. However, a request is likely to be most easily dealt with by providing copies of documents. These may need to go through a process of redaction before being sent due to the identification of another person.

Organisations have a duty to be fair, transparent, and facilitate the request. Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It is an offence to alter or erase information with the intention of preventing disclosure, unless the data would have been altered or erased even if no subject access request would have been made.

The request must be complied with without delay, and within one month of receipt at the latest (this can be extended by a further two months where requests are complex or numerous but this must be explained to the requester).

Organisations will no longer be able to charge a standard £10 fee for complying with a request. A ‘reasonable fee’ can be charged only where a request is “manifestly unfounded or excessive, particularly if it is repetitive”, or where further copies of the same information is requested. Refusal to comply with a request is permitted when the request is “manifestly unfounded or excessive”. In these circumstances, the requester must be informed without undue delay of the refusal to comply, and within one month at the latest. An organisation’s reasons for refusal must be given, together with information on the employee’s right to complain to the Information Commissioner or to take legal proceedings. A subject access request may be refused if the information requested falls into one of the exemptions permitted by the legislation:

- confidential references;
- information that the organisation is required to publish by law;
- personal data processed for the purpose of prevention or detection of crime, the capture or prosecution of offenders and the assessment or collection of tax;
- management planning or management forecasting;
- a record of intentions in negotiations with the employee;
- in relation to core regulatory activities;
- legal privilege;
- health and education records;
- social work records.

Other, less common, exemptions also apply.

An employee may complain to the Information Commissioner if they believe their right of access under the GDPR has been infringed. If the Information Commissioner is clear that an infringement has taken place, it may serve an assessment notice on the employer and has the power to enter the employer's premises, view documents, see the employer's data processing procedures and speak to the workforce. A penalty notice may be served on the employer if an assessment notice is not complied with. The complaint may be escalated to the Information Tribunal if the Information Commissioner fails to deal with the complaint adequately.

Courts have the power to make an order for the purposes of securing compliance if an infringement has occurred.

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 e.g. sending information to the wrong email address.
- Reportable breaches must be reported to the relevant supervisory authority 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 €10 million or 2 per cent of the organisation's global turnover.

Fines

A breach of GDPR carries a maximum fine of €20 million or 4 per cent of the organisation's global turnover. The Data Protection Working Party's guidelines on the application and setting of administrative fines, adopted on 3 October 2017, sets out the principles for consistent application of fines for data protection breaches. Specific breaches will not carry a "price tag". Instead an assessment will be made on the individual circumstances of the breach against certain criteria. The following will be assessed:

- 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 e.g. 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 e.g. "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 higher 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.

ICO's "12 Steps To Take Now"

The ICO has published a document setting out steps that organisations can take in preparation for the introduction of GDPR. These are:

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.