119 - DATA PROTECTION POLICY

The General Data Protection Regulations (GDPR) come in to effect on 28th May 2018, replacing the Data Protection Act 1998 (DPA). Regulations become a legal requirement when they come in to effect and do not require a new Act. The main requirements of the previous Act are embedded in the new Regulations but have been extended in certain areas.

The Care Home or service needs to collect and use certain types of information about residents, service users, employees and others. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the GDPR.

The Care Home regards the lawful and correct treatment of personal information as very important and therefore ensures that personal information is treated lawfully and correctly. To this end the Care Home fully endorses and adheres to the principles of data protection, as detailed in the General Data Protection Regulations as detailed below.

Principles

The data protection principles, as set out in the DPA, remain but they have been condensed into six as opposed to eight principles. Article 5 of the GDPR states that personal data must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Processed in a way 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.

Consent

Like the DPA, the GDPR will require data controllers to have a legitimate reason for processing personal data. If they rely on the consent of the data subject, they must be able to demonstrate that it was freely given, specific, informed and unambiguous for each purpose for which the data is being processed. Consent can be given by a written, including electronic, or oral statement. This could include the data subject ticking a box when visiting a website, choosing technical settings for social network accounts or by any other statement or conduct which clearly indicates their acceptance of the proposed processing of personal data. Silence, pre-ticked boxes or inactivity will no longer constitute consent.

Children

The preamble to the GDPR states: 'Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child.'

Article 8 requires that where the personal data of a child under 16 is being processed to provide 'information society services' (for example, online businesses, social networking sites and so on) consent must be obtained from the holder of parental responsibility for the child. Member states are allowed to lower this threshold where appropriate but not below the age of 13.

Data subjects' rights

The list of rights that a data subject can exercise has been widened by section 2 of the GDPR. The subject access right, rectification and being able to object to direct marketing remain. The right to have personal data processed for restricted purposes and the right to transfer data/have it transferred to another data controller (data portability) are new rights.

In addition, article 17 introduces a 'right to be forgotten', which means data subjects will be able to request that their personal data is erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed, where data subjects have withdrawn their

consent, where they object to the processing of their data or where the processing does not comply with the GDPR. However, the further retention of such data will be lawful in some cases where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims.

To strengthen the 'right to be forgotten' online, the GDPR requires that a data controller who has made the personal data public should inform other data controllers which are processing the data to erase any links to, or copies or replications of, that data.

Data protection by design

Data controllers will be expected to include data protection controls at the design stage of new projects involving the processing of personal data. Where they wish to process personal data that poses potentially high risks they will have to, prior to the processing, carry out a data protection impact assessment. Supervisory authorities (the member state's data protection regulators, for example the Information Commissioner's Office (ICO)) will be able to produce lists as to what sort of processing would warrant such an assessment.

Notification

The current system of notification under the DPA will be replaced by a requirement for data controllers to keep an internal record in relation to all personal data they process (article 28). The record must include, among other things, details of the purpose of processing personal data, recipients, transfers to third countries, time limits for erasure as well as a general description of the technical and organisational measures in place protecting the data.

Security breaches

Under the DPA, even in the most serious data breaches, there was no requirement to inform the ICO. Article 31 of the GDPR requires that, as soon as the data controller becomes aware a personal data breach has occurred, it should, without undue delay and, where feasible, not later than 72 hours after becoming aware of it, notify the personal data breach to the ICO, unless the controller is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification to the ICO and information may be provided in phases without undue further delay.

Furthermore, data subjects should be notified without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms to allow them

to take the necessary precautions. This notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. This should be done as soon as reasonably feasible, and in close cooperation with the ICO and respecting guidance provided by it or other relevant authorities (for example, law enforcement authorities).

Fines

Previously, the ICO could issue a monetary penalty notice of up to £500,000 for serious breaches of the DPA.

The GDPR introduces much higher fines.

For some breaches of the GDPR, data controllers can receive a fine of up to 4% of global annual turnover for the preceding year (for undertakings) or €20m. For other breaches (for example, failing to keep records or complying with security obligations) the fine can be up to €10m or 2% of global annual turnover (for undertakings).

Data protection officer

Section 4 of the regulation introduces a statutory role of data protection officer (DPO). Most organisations handling personal data, both data controllers and data processors, will require a DPO who will have a key role in ensuring compliance with the GDPR. A group of undertakings may appoint a single DPO provided that s/he is easily accessible. Public bodies may also have a single DPO for several such authorities or bodies, taking account of their organisational structure and size.

The DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, knowledge of data protection law and practices, and the ability to fulfill the tasks referred to in article 37. These are:

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to the GDPR;
- to monitor compliance with the GDPR, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to article 33;
- to cooperate with the supervisory authority (the ICO); and
- to act as the contact point for the supervisory authority on issues related to the processing of personal data.

Procedure

The Care Home will, through appropriate management, comply with strict application of criteria and controls,

1. Observe fully conditions regarding the fair collection and use of information.
2. Appoint an appropriate person to the role of Data Protection Officer
3. Meet its legal obligations to specify the purposes for which information is used.
4. Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
5. Ensure the quality of information used.
6. Apply strict checks to determine the length of time information is held.
7. Ensure that the rights of people about whom information is held, can be fully exercised under the GPDR. (These include; obtaining informed and valid consent, the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information).
8. Take appropriate technical and organisational security measures to safeguard personal information.
9. Ensure that personal information is not transferred abroad without suitable safeguards.
10. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
11. Set out clear procedures for responding to requests for information.

In addition, the Home will ensure that:

1. Everyone managing and handling personal information understands that they are contractually responsible for following good data practice.
2. Everyone managing and handling personal information is appropriately trained to do so.
3. Everyone managing and handling personal information is appropriately supervised.
4. Anybody wanting to make enquiries about handling personal information knows what to do.
5. Queries about handling personal information are promptly and courteously dealt with.
6. Methods of handling personal information are clearly described.
7. A regular review and audit is made of the way personal information is held, managed and used.
8. Methods of handling personal information are regularly assessed and evaluated.
9. Performances with handling personal information is regularly assessed and evaluated.

10. A breach of the rules and procedures identified in this policy by a member of staff may lead to disciplinary action being taken.
11. A breach of the rules and procedures identified in this policy by a member of staff is a potential breach of the Code of Conduct.

This Policy will be updated as necessary to reflect best practice in data management, security and contract and to ensure compliance with any changes or amendments made to the GDPR.