May 2018

Data Protection - GDPR Policy

Date Written	*25.05.2018*
Author(s)	Living Carers Ltd
Version	*1.0*
Date Signed Off	25/05/18
Reviewed by	

Unit 1,
Chandos House,
Taunton,
Somerset
TA1 2LR

Review Data

Initial Production

Name	Role/Department	RACI	Date
Pete Cullen	Managing Director	RA	25.05.2018

R = Responsible for document production; **A** = Accountable; **C** = Consulted; **I** = Informed

Change History

Version	Date	Details of Change	Author
1.0	25.05.2018	Initial Creation Date	Living Carers Ltd

Emergency Contact Details

Name	Email	Telephone
Pete Cullen	pete@livein.care	0800 772 3567

CQC Fundamental Standards

Regulation Number	Regulation Details
Regulation 10: Dignity and respect	Clients must be treated with dignity and respect, including ensuring the privacy of the Client.
Regulation 17: Good governance	Both paper and electronic records can be held securely providing they meet the requirements of the Data Protection Act 1998.

Key Lines of Enquiry

KLOE	How this applies to Data Protection
Caring	To provide a caring service we must respect the confidentiality, privacy and dignity of Clients.
Well led	As a well led organisation, we ensure compliance with data protection legislation.

Related Documents

This policy should be read in conjunction with our:

- **Confidentiality Policy**
- **Dignity and Respect Policy**

Policy Statement

Policy Aims

- To ensure that Living Carers Ltd apply appropriate measures to comply with the General Data Protection Regulation (GDPR)
- To inform staff on how data is protected within Living Carers Ltd, and what their responsibilities are when it comes to Data Protection.

Living Carers Ltd needs to collect and use certain types of information about employees, Clients, and those individuals who encounter Living Carers Ltd in the supply of care services. This personal information will be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 1998 and the GDPR.

Social care organisations hold a significant amount of personal information relating to individuals, whether they be employees, people who need care and support or other customers or suppliers. A proportion of that data is likely to constitute sensitive personal data or “special categories of data” (including for example, medical records, religious beliefs or ethnic origin).

All organisations that process personal data are required to comply with the Data Protection Act 1998 (DPA) and, from 25 May 2018, the General Data Protection Regulation (GDPR).

In order to comply fully with the new regulations, Living Carers Ltd has incorporated the ICO 12-point checklist into practice, and into this policy.

The checklist includes:

1. **Awareness**
2. **Information held**
3. **Communicating privacy Information**
4. **Individuals’ rights**
5. **Subject access requests**
6. **Lawful basis for processing personal data**
7. **Consent**
8. **Children**
9. **Data breaches**
10. **Data protection by design and Data Protection Impact Assessments**
11. **Data Protection Officers**
12. **International**

Awareness

Living Carers Ltd aims to make sure that decision makers and key people in the organisation are aware that the law is changing to the GDPR.

We appreciate the impact this is likely to have and therefore will work to identify areas that could cause compliance problems under the GDPR. We will begin this process by evaluating the company's risk register.

Living Carers Ltd will work to ensure that staff throughout the organisation understand the requirements of the new Data Protection legislation and will offer support and training where needed to ensure that the necessary changes are implemented throughout the entire company.

Personal Information

Personal Information is any data relating to a living individual, and under the Data Protection Act 1998 all Personal Information:

Must be processed fairly and lawfully;

Must be obtained for one or more specific and lawful purposes and only processed in a manner compatible with them;

Must be adequate, relevant and not excessive for the purposes defined;

Must be accurate and where necessary kept up to date;

Shall not be kept for longer than is necessary;

Must be processed in accordance with the data subject's rights;

Must be kept secure;

Must not be transferred outside the European economic area unless there is adequate protection for the rights of data subjects.

The GDPR widens the definition of what constitutes personal information.

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 – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Question: How is the company documenting what personal data it holds, where the data came from and who it is shared with?

Moving forward, every document that contains personal data will include details of where the data came from. For example, we may have core data in a care plan from the Council on referral of a Client, a copy of which will be held on file and a reference to which will be noted on our own care plan – which is developed following our own risk assessment visit.

Question: How does GDPR affect the company?

The GDPR extends current requirements set out in the Data Protection Act 1998 and places new obligations on organisations that process personal data and special categories of data. These include, amongst others:

1. more stringent requirements around consent, particularly if special categories of data are involved;
2. the right to be forgotten;
3. taking an approach to projects that promotes privacy and data protection compliance from the start and using privacy impact assessments to identify and reduce risk;
4. a modified subject access request procedure that favours the individual;
5. if there is a breach of GDPR there are new, stricter requirements to notify the Information Commissioner's Office and the affected data subjects; and
6. expanded territorial reach – a non-EU company could be subject to the same sanctions as EU companies.

Data Protection Officer

The Data Protection Officer for Living Carers Ltd is Pete Cullen.

Living Carers Ltd has appointed a formal data protection officer on the basis that we are conducting large scale processing of personal data. A formal DPO benefits from enhanced employment rights, but is also beneficial as a point of contact for the organisation in respect of GDPR including, for example, responding to subject access requests.

The Data Protection Officer takes proper responsibility for data protection compliance and has the knowledge, support and authority to carry out their role effectively.

Data Controller

Living Carers Ltd is mainly a Data Controller under the Act, which means that it determines what purposes held personal information will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

The GDPR applies to both controllers and processors. The changes introduced by GDPR in this respect may result in data processors (including, for example, commissioning support units, IT and software providers) seeking more detailed data processing agreements to ensure their obligations are clearly defined.

In line with GDPR, Living Carers Ltd ensures the data processing agreements are clear and detailed so that responsibility and liability is appropriately shared between the parties.

There may be times that we are processors or we hold joint data controller roles, such as with the Councils with whom we work.

This sort of joint controller working has been standard practice to date, and compliance with the data protection principles 52 includes that, when a controller discloses personal data to another controller each has full data protection responsibility because both parties will exercise control over the purposes for which and the manner in which the data is processed.

Where the sharing is systemic, large-scale or particularly risky, then both parties should sign up to a data sharing agreement, covering for example how the data can be used and whether it can be further disclosed. A data sharing agreement could provide for the controller that holds most of the personal data to be responsible for the practical elements of compliance.

For example, if a number of organisations – each data controllers in their own right – are working together in a child protection initiative it would be acceptable for one of the organisations to take responsibility for giving individuals subject access to the personal data held by all the organisations involved.

Disclosure

Living Carers Ltd may share data with other agencies such as the local authority. When sharing personal data with other organisations Living Carers Ltd seriously considers whether the data subjects need to be actively informed.

In order to treat people fairly prior to sharing information, you must carefully consider what any recipient organisation is going to do with it and what the effect on people is likely to be. Living Carers Ltd obtains an assurance about this, in the form of a contract or a written data sharing agreement.

The Individual/Client will be made aware in most circumstances how and with whom their information will be shared. Living Carers Ltd will do this through the use of a privacy notice which will be clear and accessible. There are circumstances where the law allows Living Carers Ltd to disclose data (including sensitive data) without the data subject's consent.

These are:

a) **Carrying out a legal duty or as authorised by the Secretary of State**

b) **Protecting vital interests of an Individual/Client or other person**

c) **The Individual/Client has already made the information public**

d) **Conducting any legal proceedings, obtaining legal advice or defending any legal rights**

e) **Monitoring for equal opportunities purposes – i.e. race, disability or religion**

f) **Providing a confidential service where the Individual/Client's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Clients to provide consent signatures.**

Privacy Notices

Living Carers Ltd regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Living Carers Ltd intends to ensure that personal information is treated lawfully and correctly.

Privacy notices, routinely telling people how their information will be used or held, reasons for collecting the data and an individual's right to complain to the ICO has only ever been via the existence of policies and procedures. However the reality of this is that few people are interested in reading these.

Living Carers Ltd will clearly communicate:

1. **What information we hold on Clients, why and who it will be shared with,**
2. **What choice and control Clients have over Data Sharing, for example whilst they may be in control of us not telling their family something. It is our understanding there will be few exceptions where we are not at liberty to share with the Commissioners all details pertaining to the Clients health and wellbeing but will document the parameters of this,**
3. **Staff will have a clear understanding of who within the organisation has access for example to their Disclosure and Barring information and the parameters of who we can / will share this with, how and why and the length of time we will store this. We will also disclose destruction methods, such as shredding,**
4. **Stakeholders will have a clearer understanding on the way we will work and where we may request for example that there is clarity in a situation where we believe they are the lead data controller and we are merely data processing in that given situation.**

Fair Data Processing

The GDPR requires a significant increase in the information to be provided by data controllers to data subjects.

Article 12 states data controllers shall have transparent and easily accessible information notices. Information must be provided in a concise form, using clear and plain language, particularly where information is addressed to a child.

In addition to the requirements contained in the DPA, data controllers must also provide:

- the contact details of the data controller;
- the contact details of the Data Protection Officer
- the Schedule 2/Article 6 and Schedule 3/Article 9 condition relied, the purpose of the processing and:
- whether the provision of personal data are required by law or for a contract, as well as whether the data subject is obliged to provide the data and the possible consequences of the failure to provide such data; or
- if the processing is based on the controller's legitimate interests, an explanation of
- those interests; or
- if the processing is based on consent, the right to withdraw consent at any time
- the data retention period;

- a reference to the rights to erasure, to object to processing, data portability and to complain to the ICO
- information on international transfers and the safeguards applied to such transfers and
- the existence of automated decision making (including profiling) and the envisaged consequences of such pro-cessing for the data subject
- Where the personal data is not obtained directly from the data subject, the notice should also identify the categories of personal data concerned and the source of the data.
- There are also detailed requirements for when such information should be provided which depends on whether the data are collected from the data subject themselves or from a third party.

Lawful Basis for Processing

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever Living Carers Ltd processes personal data:

(a) Consent: the individual has given clear consent for Living Carers Ltd to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract Living Carers Ltd has with the individual, or because they have asked Living Carers Ltd to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for Living Carers Ltd to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for Living Carers Ltd to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for Living Carers Ltd.'s legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Our Commitment

Living Carers Ltd will:

- **Observe fully conditions regarding the fair collection and use of information**
- **Meet its legal obligations to specify the purposes for which information is used**
- **Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements**
- **Ensure the quality of information used**
- **Ensure that the rights of people about whom information is held, can be fully exercised under Data Protection legislation. These include:**
  - **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)**
- **Take appropriate technical and organisational security measures to safeguard personal information**
- **Ensure that personal information is not transferred abroad without suitable safeguards**
- **Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information**
- **Set out clear procedures for responding to requests for information**

Children

The GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking.

The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

Data Collection

Informed consent is when

- An Individual/Client clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent.

Living Carers Ltd will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Living Carers Ltd will ensure that the Individual/Client:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Individual/Client decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

e) Has received sufficient information on why their data is needed and how it will be used

A consent to sharing information form, will be produced for each Client and on which there will be clear instructions detailed around who they give consent for us to share what information with. This will include which family members are to be contacted, under what circumstances and this will remain with the care plan at all times.

The Mental Capacity Act (MCA) is a key piece of guidance that we work with in managing consent to share information issues, and our MCA policy sets out the process in managing decision making and sharing information.

The consent to sharing information form will therefore include clear guidance that where a person has capacity to make decisions and even if they are considered poor decisions, we will as required by the MCA, we will respect the Clients choice. This consent form will specify for example, where a Client does not want their family notified if they are diagnosed with an illness.

It will be each Clients choice as to whether they wish to tell their family ahead of any issues or choose that the sharing information form in itself remains confidential until such a time as it is to be actioned, and this decision will also be detailed on the form.

Key Question: How will data be stored securely?

Information and records relating to Clients will be stored securely and will only be accessible to authorised staff.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is Living Carers Ltd responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Data Access and Accuracy

All Individuals/Clients have the right to access the information Living Carers Ltd holds about them. Living Carers Ltd will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

The GDPR includes the following rights for individuals:

- 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; and
- the right not to be subject to automated decision-making including profiling.

Living Carers Ltd ensures that:

1. It has a Data Protection Officer with responsibility for ensuring compliance with Data Protection
2. Everyone processing personal information understands that they are responsible for following good data protection practice
3. Everyone processing personal information is appropriately trained
4. Everyone processing personal information is appropriately supervised
5. Anybody wanting to make enquiries about handling personal information knows what to do
6. It deals promptly and courteously with any enquiries about handling personal information
7. It describes clearly how it handles personal information
8. It will regularly review and audit the ways it holds, manage and use personal information
9. It regularly assesses and evaluates its methods and performance in relation to handling personal information
10. All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them
11. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.
12. Personal Data is provided in a structured commonly used and machine readable form and provide the information free of charge.

Subject Access Requests

Requests from current and former employees, as well as people who need care and support, for sight of all data held about them are relatively common in the social care sector. GDPR removes the £10 fee payable to make a request and decreases the timescales for complying with a request from 42 days to 1 month. Removal of the £10 fee may result in an increase in the number of SARs placed, simply because an administrative obstacle has been removed.

Clients should have access to their own records in accordance with the Data Protection Act 1998 and the GDPR.

Any access to records must always be considered in terms of Living Carers Ltd.'s confidentiality policy. This means that such information must not be made available to other people and anyone else mentioned in the records should have their identity protected. **The Act does not give the user the right of access to information about other people.**

The implication of the legislation is that records are shared with the individuals concerned as they are made. This allows for openness, and an agreement between care worker and Client and the potential for greater accuracy. Only in rare circumstances should access be refused. The person seeking access to information should have the Living Carers Ltd policy carefully explained to them.

If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month

Question: What should I do if I get a request from a Client for their personal file?

Any request from Clients for access to their personal file must be discussed with the Data Protection Officer, who takes the decision as to what may or may not be shared. The request should be noted in the Client's file.

All staff receive training in the access to records policy at induction and whenever changes need to be made to it.

Notification/ Representation

All organisations that process Personal Data must notify the ICO (ico.org.uk).

Please provide the following information

1) Registration Number
2) Date of Renewal
3) Copy of notification certificate with the ICO

Living Carers Ltd's nominated a representative for the purposes of dealing with data protection enquiries or concerns from individuals is Pete Cullen.

Under the current legislation, the ICO may levy fines of up to £500,000.

Under GDPR, those fines will increase to a maximum of 20 million Euros or 4% or group worldwide turnover (whichever is greater).

Breaches that are deemed by the ICO to be less serious could incur fines of up to 10 million Euros or 2% of group worldwide turnover. Reputational impact could also be significant.

Erasure

Article 17 of The GDPR provides data subjects with a new enhanced right to request erasure of their personal data. Data subjects do not need to prove substantial unwarranted damage or distress or inaccuracy. Data controllers must delete personal data on request where specified grounds apply. Such grounds include:

- where the personal data are no longer necessary for the original purpose for which the data were collected/ processed; and
- if the data subject withdraws their consent and no other legal ground for processing applies.

However, there are a number of grounds on which data controllers can rely to keep personal data. These include if the data is needed for:

- the delivery of public services;
- the protection of public health; or
- the establishment, exercise or defence of legal claims.

Where a request for erasure has been received in respect of personal data which has been disclosed by the data controller to a third party, the data controller must take all reasonable steps to inform any onward data controllers of the request.

Data Protection Impact Assessments

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and we cannot sufficiently address those risks, Living Carers Ltd will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

All procedures relating to this point are to be reviewed as part of the Audit Framework

Data Breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals.

We will ensure that the designated Data Protection Officer is fully conversant with the parameters of breaches and if when and how to report these. The importance of such reporting will also formulate a part of the Officers contract of employment in order that we have clear understanding around accountability in this regard.

International

The GDPR states that If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

This is not applicable to Living Carers Ltd, however we are aware of the requirements surrounding International Data Protection and will implement robust procedures if the need arises.

Glossary of Terms

Data Controller – The person who decides what personal information Living Carers Ltd will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that Living Carers Ltd follows its data protection policy and complies with the Data Protection Act 1998.

Individual/Client – The person whose personal information is being held or processed by Living Carers Ltd for example: a Client, an employee, or young person.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Client in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

GDPR - The EU's General Data Protection Regulation (GDPR) is the result of four years of work by the EU to bring data protection legislation into line with new, previously unforeseen ways that data is now used.

Notification – Notifying the Information Commissioner about the data processing activities of Living Carers Ltd, as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual Clients or employees within Living Carers Ltd.

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

Monitoring and Review

The Managing Director will check this policy is working properly and they will review it at least once a year. We will make improvements to the policy wherever we can.

Employees are invited to suggest any ways the policy can be improved.

Key Points to Take Away

- All organisations that process personal data are required to comply with the Data Protection Act 1998 (DPA) and, from 25 May 2018, the General Data Protection Regulation (GDPR)
- Data controllers must delete personal data on request where specified grounds apply
- **Clients should have access to their own records** in accordance with the Data Protection Act 1998 and the GDPR.
- Information and records relating to Clients will be stored securely and will only be accessible to authorised staff

Policy Review

This policy will be reviewed by the Managing Director at least annually to make any updates and amendments necessary to ensure the policy conforms to current legislation, reflects current practice and expectations.

Authorisation and Signature

This Policy is the official and authorised version agreed by the Directors of Living Carers Ltd. All employees are expected to work in accordance with this policy and failure to comply with this policy could result in disciplinary action.

Pete Cullen
Managing Director
25.05.2018