

Privacy Policy

VERSION: 5
DATE: 07 FEB 19

| | |
|---|---|
| Who will use my data? | TWINGLOBE – including Twinglobe Ltd, Twinglobe Care Ltd |
| What for? | We will store and process your data in order to allow us to provide our care and personal support services to you. |
| What will happen you contact us? | If you contact us, we will use your information send you the information you have requested about our care services, care homes, and other relevant services. If you contact us regarding employment, supplier, or other opportunities we will store and process your details as described in this document. |
| What data will be stored? | We will store your personal details including your sensitive personal information where necessary in order to provide our services to you and to reply to your request. We will also store related financial information as required. We will store information you provide to us plus other information we collect from other sources where required to provide our services to you and to ensure we are always able to act in your best interests. |
| What data will be shared? | As a resident or service user we will not share your data with any third parties other than as described here and as necessary to provide our care services to you and to ensure we are able to act in your best interests. We will share your information with other medical professionals, and care organisations as necessary and any authorised regulator or legal body that requests it. As an employee or other third party we will not share your data with any third party other than as required to run our business and meet our obligations to you. |
| How long? | Your data will be stored as described in our Data Retention and Erasure policy after which time your data will be deleted. |
| Who can access my data? | We will never sell, share or otherwise distribute your data to any other third party. Access to your data will be strictly controlled and only accessed by authorised people and organisations. |
| How is my data kept secure? | We will usually store your data on secure UK based servers which will be processed in the UK. We use industry standard security protocols/technology to secure data. Where data is stored outside the EU we will ensure we establish appropriate technical and contractual measures to keep your data safe. |

We take your privacy seriously and will only use your personal information to provide the services you have requested from us and to send you information about our care services you may be interested in. We will never sell, share or use your personal information other than as described here.

About This Privacy Policy

This policy sets out how we will use and share the information that you give us. This policy describes your relationship with Twinglobe Ltd. The General Data Protection Regulation (GDPR) describes how organisations must collect, handle, process and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. GDPR is underpinned by eight important principals. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than is necessary
- Processed in accordance with the rights of the data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area, unless that country or territory also ensures an adequate level of protection

We take these responsibilities seriously. This document describes our approach to data protection. This policy helps to protect us from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.
- Any loss or damage caused as a result of a data breach or related issue.

Mihir Thakerar is the Data Controller and is committed to protecting the rights of individuals in line with the General Data Protection Regulation (GDPR).

Who We Are And How To Contact Us

Twinglobe Ltd and Twinglobe Care Ltd are registered with Companies House in UK and is with the Information Commissioner's Office. The data controller is: Julie Burton. You can contact us in any of the following ways:

Email: centraloffice@twinglobe.com

Phone: [020 8370 1773](tel:02083701773)

Website: <http://www.twinglobe.co.uk/>

Post: 58 Abbey Road, Bush Hill Park, Enfield, EN1 2QN

Scope of Agreement

Submitting your personal data including sensitive personal information is required for us to provide our care and related services to you, you are affirming your agreement for such information to be used in accordance with this privacy policy. You will be able to change your preferences at any time by the methods as prescribed in this document.

When you contact us we will use your information to respond to any requests we receive from you and ensure we are able to provide our services to you. As one of our residents and service users we will always act in your best interests and may collect and share your information with other health care professionals. Where we share your information with our people this will always be as you would reasonably expect us to do so. We may from time to time use your information for business management purposes. The main purpose of this is to maintain any existing relationship we may have with you and ensure we are able to provide our services to you.

What information do we collect about you?

When you contact us as a potential client, employee, volunteer, or any other third party we will collect information about you including contact details and other information.

As a service user we will collect additional information including your health information, care needs, financial information, and other sensitive personal information. We need to collect this sensitive data about you in order to deliver the appropriate care that you need and to ensure that your ongoing healthcare requirements are met. We require explicit consent for processing sensitive data from you or your representative.

Who this privacy policy applies to

Twinglobe is a provider of Care Home services. This policy relates to any individual related to Twinglobe in any capacity. Processing of your data is required in order to offer you our services as a care provider. This policy applies to individuals who have shared their data with Twinglobe in any capacity. This might include sharing data either a client, service user, employee, supplier or in any other capacity.

This policy applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of Individuals
- Postal addresses
- Email Addresses
- Telephone numbers
- Medical information including previous medical history, medication, allergies, and other sensitive information
- Personal and family history as required to help provide the best possible care for you and your family
- Other personal information including the most sensitive information such as religious preferences, EOL preferences, DNAR requests, and other personal information

What this policy applies to

This section describes the lawful basis for processing your data and applies to the information about yourself that you choose to provide us with or that you allow us to collect. This includes:

- The Information you provide when you contact us
- When you contact us in order to discuss using our services
- Information relating to Care services we offer to you. Also, others including financial and any personal information required to complete these transactions
- Information that is given and stored as part of our ongoing relationship
- Information we collect from other sources that we use to provide the best possible care for you
- Information we collect as part of our ongoing relationship with you - this information includes sensitive personal information

As a care service provider, we will collect sensitive information. We require explicit consent for processing sensitive data, however we will always act in your best interests and may collect, store, and process sensitive information without your explicit consent. Where this occurs, this will always be in your best interests and as you would reasonably expect. Where necessary we may process information provided by your representative, for example where you have granted power of attorney to a third party. We will accept consent from your representative as being given by you.

What personal information we collect about service users, employees and third parties

Service users:

As a registered care provider, we must collect some personal information on our service users, including financial information, which is essential to our being able to provide effective care and support. The information is contained in individual files (manual and electronic) and other record systems, all of which are subject to strict security and authorised access policies. Personal information that becomes inactive, for example from enquiries or prospective users who do not enter the service is also kept securely for as long as it is needed, before being safely disposed.

Employees and volunteers:

The service operates a safe recruitment policy to comply with the regulations in which all personal information obtained, including CVs and references, is, like service users' information, securely kept, retained and disposed of in line with data protection requirements. All employees are aware of their right to access any information about them.

Third parties:

All personal information obtained about others associated with the delivery of the care service, including suppliers, contractors, visitors, other thirds parties etc. will be protected in the same ways as information on service users and employees.

What is Personal Data?

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly. Personal data includes any personally identifiable information that we may collect, store, process, or otherwise use to facilitate our relationship and allow us to provide the Elderly care services you need. For example, data we collect about you may include:

| | |
|--------------------------------|---|
| Contact Information | Personal address, business address, service address, email address and telephone number. |
| Identity Information | First name, maiden name, last name, username or similar identifier, marital status title date of birth and gender. |
| Technical Information | Internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website. |
| Transaction Information | Details about payments to and from you and other details of Elderly care services you have purchased from us. |
| Medical Information | Details about any medical conditions, medication, treatment, Care Plans, DNAR, End of Life Plans, and other sensitive personal information. |
| Other Information | One or more factors specific to the physical, physiological, genetic, medical, mental, economic, cultural identifiers, personal and family histories, personal preferences, and other personal information required so we can provide our services to you and act in your best interests. |

Where/how we collect your data?

The bulk of service users', employees' and thirds parties' personal information is collected directly from them or through form filling, mainly manually, but also electronically for some purposes, for example when contacting the service via its website.

With service users, we might continue to build on the information provided in enquiry and referral forms, and, for example, from needs assessments, which feed into their care and support plans.

With employees, personal information is obtained directly and with consent through such means as references, testimonials and criminal records (DBS) checks. When recruiting staff, we seek applicants' explicit consent to obtain all the information needed for us to decide to employ them.

All personal information obtained to meet our regulatory requirements will be with your explicit consent where possible. Our website and databases are regularly checked by experts to ensure they meet all privacy standards and comply with our general data protection security and protection policies.

We collect your information when you contact us via our website, by phone, or when you or your representative completes forms or other documentation as required by us. We will also collect information about you as a consequence of provide care services to you. This may include data from other medical professionals and authorised third parties. As a service user this may include sensitive personal information and also include personal information collected indirectly from an Advocate, other Healthcare Professionals, or authorised agencies that have been involved in that individuals' care or treatment.

How your information will be used

We will only use your personal data for the purposes for which we collected it and as you would reasonably expect, unless we consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to find out more about how the processing for the new purpose is compatible with the original purpose, please email us. If we need to use your personal data for a purpose unrelated to the purpose for which we collected the data, we will notify you and we will explain the legal ground of processing.

- Administering finance (e.g. fees, contracts and payments)
- Providing support services Care and medical services
- Provided to other health care professionals to allow them to care for you
- Providing information to authorised third parties to provide care, personal, support services to you
- Providing, IT and information services
- Managing accounts
- Monitoring equal opportunities
- Carrying out research and statistical analysis
- Providing operational information
- Safeguarding
- Security
- Preventing and detecting crime
- And other functions necessary for your best interests

The lawful basis we apply are as described below:

| Purpose/Activity | Type of data | Lawful basis for processing |
|--|---|---|
| To register you as a new service user, client, or in an equivalent relationship | (a) Identity, (b) Contact information, (c) personal information | Performance of a contract with you, with your consent, and in our legitimate interests |
| To provide care and medical services: Manage medication, care, and provide support in your best interests | (a) Identity, (b) Contact, (c) Medical, (d) Care, (e) Needs assessment data (initially and ongoing) | (a) Performance of a contract with you, (b) Necessary for our legitimate interests, (c) Protect your vital interests, (d) with your consent or consent from your representative |
| To process and deliver your services including: (a) Managing payments, fees and charges, (b) Collecting and recovering money owed to us, (c) managing your care and well-being | (a) Identity, (b) Contact, (c) Financial, (d) Transaction, (e) Marketing and Communications | (a) Performance of a contract with you, (b) Necessary for our legitimate interests to recover debts owed to us, (c) in your vital interest |
| To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy, (b) Asking you to leave a review or take a survey | (a) Identity, (b) Contact, (c) Profile, (d) Marketing and Communications | (a) Performance of a contract with you, (b) Necessary to comply with a legal obligation, (c) Necessary for our legitimate interests to keep our records updated and to study how clients use our services. |
| To administer and protect our business and our site (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data) | (a) Identity, (b) Contact, (c) Technical | (a) Necessary for our legitimate interests for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise, (b) Necessary to comply with a legal obligation |

Twinglobe processes sensitive data and as such the lawful basis for processing is particularly important. For example, we process information relevant to the above reasons/purposes subject to the statutory duty under section 251B of the Health & Social Care Act 2012. The lawful basis for processing your information under the GDPR is: S6(1)(e) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"

Special Category data is processed to operate the business (sensitive data including racial or ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs, or trade union membership, information about mental health or physical health and wellbeing).

Wherever possible, explicit consent will be obtained prior to your data being processed, however, where appropriate, service users' next of kin may give explicit consent for those who lack mental capacity, otherwise "best interest" decisions will be made in line with the Mental Capacity Act 2005.

This is particularly important where we process data for people with reduced or variable capacity. Under the GDPR we must obtain consent from a person holding Lasting Power of Attorney or Next of Kin. We will also make reasonable efforts to verify that the person providing that consent is indeed responsible for that individual. As a Care Home we rely on Article 9 in order to process special categories of data.

The legal basis we use for processing employees data is given in s9 (2) (b) of the GDPR, as "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law."

We will process data relating to criminal convictions and offences under the lawful basis set out in Article 10 and processing of personal data relating to criminal convictions and offences shall be carried out with appropriate safeguards for the rights and freedoms of data subjects. Any information regarding criminal convictions shall be processed only for the purposes of safeguarding requirements within our recruitment process.

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to find out more about how the processing for the new purpose is compatible with the original purpose, please email us. If we need to use your personal data for a purpose unrelated to the purpose for which we collected the data, we will notify you and we will explain the legal ground of processing.

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes. We may process your personal data without your knowledge or consent where this is required or permitted by law or where we consider this to be in your vital interest.

Who receives your information?

We may have to share your personal data with the parties set out below for the purposes set out in the table above:

We only share the personal information of service users, employees and others with their consent on a "need to know" basis, observing strict protocols in doing so. Most information sharing of service users' information is with other professionals and agencies involved with their care and treatment. Likewise, we would not disclose information about our employees without their clear agreement, e.g: when providing a reference.

The only exceptions to this general rule would be where we are required by law to provide information, e.g: to help with a criminal investigation. Even when seeking to notify the local authority of a safeguarding matter or the Care Quality Commission of an incident that requires us to notify it, we would only do so with consent or ensure that the information provided is treated in confidence.

Where we provide information for statistical purposes, the information is aggregated and provided anonymously so that there is no privacy risk involved in its use.

Any transfers to third countries and the safeguards in place

We may use third parties located outside the EU, where this is the case we will ensure that these companies have taken appropriate steps to secure your data. We will may use third parties outside the EU to store transactions and payment data, this data will be stored as defined in the Data Retention and Erasure policy or for as long as required by UK financial and company regulations.

How personal information held by the care provider can be accessed

There are procedures in place to enable any staff member, employee or third party whose personal information we possess and might process in some way to have access to that information on request. The right to access includes both the information and any uses which we might have made of the information.

What are your rights?

We respect all your rights under GDPR, we will always act lawfully and transparently, you will have the right to access your personal information, to object to the processing of your personal information, to rectify, to erase, to restrict and to port your personal information and to withdraw or change your consent. Any requests or objections should be made in writing to us at: Azalea Court, 58 Abbey Road, Bush Hill Park, Enfield, EN1 2QN.

You will not normally have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

How to change your preferences

We operate in line with EU GDPR (May 2018) data protection guidelines. We respect your rights and will respond to any request for access to personal information and requests to delete, rectify, transfer, data and to stop processing. We will also advise you on how to complain to the relevant authorities, namely the Information Commissioner's Office. Any requests or objections should be made in writing to the Data Controller or you can visit our website, call, or email us to contact us to change your preferences at anytime.

How we store and process your data

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Your personal information will be collected, stored and processed in the EU and where necessary in strictly controlled third countries.

In order to provide our services to you we use recognised third parties to take payment, conduct credit reports and other checks, manage our company accounts and provide banking services. We will store transactions, payments as per our Data Retention and Erasure policy or for as long as required by UK financial and company regulations. These third parties may operate outside the EU. If this is the case we will ensure precautions are in place to protect your data.

We may be legally obliged to disclose your personal information without your knowledge to the extent that we are required to do so by law; in connection with any ongoing or prospective legal proceedings; in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk); to any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal information where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal information.

Our obligations

We are a data controller. In relation to the information that you provide to us, we are legally responsible for how that information is handled. We will comply with the GDPR (2018) in the way we use and share your personal data. Among other things, this means that we will only use your personal data:

- Fairly and lawfully
- As set out in the legislation and this policy
- To the extent necessary for these purposes
- We will take steps to ensure your data is accurate and rectify data as necessary

Under certain circumstances, you have rights under data protection laws in relation to your personal data. These include the right to:

- Request access to your personal data.
- Request correction of your personal data.
- Request erasure of your personal data.
- Object to processing of your personal data.
- Request restriction of processing your personal data.
- Request transfer of your personal data.
- Right to withdraw consent.

You can see more about these rights at: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know such data. They will only process your personal data on our instructions and are subject to a duty of confidentiality.

We will report any breaches or potential breaches to the appropriate authorities within 24 hours and to anyone affected by a breach within 72 hours. If you have any queries or concerns about your data usage, please contact us.

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

Cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added, and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences. We use traffic log cookies to identify which pages are being used. This helps us analyse data about webpage traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

As well as your ability to accept or reject cookies, we also require your permission to store cookies on your machine, which is why when you visit our site, you are presented with the ability to accept our terms of use, including the storage of cookies on your machine. Should you not accept then you are free to leave our website, at any time. For more details see our full policy at: <http://www.twinglobe.co.uk>

Legitimate Interests

Under the GDPR, we are also permitted to share some information with third parties who use such data for non-marketing purposes (including credit and risk assessment and management, identification and fraud prevention, debt collection and returning assets to you). In addition, we may use your information to send you offers, updates, and other marketing information, if you prefer not to receive information from us please contact us.

Your Vital Interests

Under the GDPR, we are also permitted to share your information if we believe that this is necessary to protect your health and preserve life. Where this is necessary we will only share your data with authorised and appropriate third parties and will always act in your best interests. This may include medical professionals, Healthcare professionals, and other people and companies involved in your care.

Contacting us, exercising your information rights and Complaints

If you any questions or comments about this Privacy Policy, wish to exercise your information rights in connection with the personal data you have shared with us or wish to complain, please contact: Julie Burton at Twinglobe Ltd. We will process SARs within 30 days, SAR responses are usually free but we reserve the right to charge for excessive or unfounded requests. We fully comply with Data Protection legislation and will assist in any investigation or request made by the appropriate authorities.

If you remain dissatisfied, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

www.ico.org.uk

Many thanks