

GENERAL DATA PROTECTION PRIVACY NOTICE

Introduction

The EU General Data Protection Regulation ("**GDPR**") replaces the 1995 EU Data Protection Directive. The GDPR strengthens the rights that individuals have regarding personal data relating to them and seeks to harmonize data protection laws across Europe, regardless of where that data is processed.

Our business is made up of different legal entities, as follows: Minster Care Group Ltd and its subsidiaries and associates (collectively referred to as "**Minster Group**" in this privacy policy). This privacy policy is issued on behalf of the Minster Group so when we mention "we", "us", or "our" in this privacy policy we are referring to the relevant company within the Minster Group responsible for processing your data.

Minster Group is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with our legal obligations.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This notice sets out how we collect and process personal data and seek to protect personal data.

Data Controller and contact information

Minster Group are data controllers. Enquiries can be directed to Mr John Alflatt (Finance Director and Company Secretary) , john@minstercaregroup.co.uk or Mr Amit Shah (Data Protection Officer): amit@minstercaregroup.co.uk

Third-party links

Our website may include links to third-party website, plug ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data. We do not control these third party websites and are not responsible for their privacy statements.

Reasons/purposes for processing information

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, process, store and transfer personal information to enable us to provide residential healthcare services; to maintain our own accounts and records; to support and manage our employees. We may also collect, process, store and transfer personal information by way of our CCTV systems to monitor and collect visual images for security and the prevention and detection of crime or by using audio recording equipment to record telephone calls for record or training purposes.

We may collect and process information relevant to the above reasons/purposes. This information may include:

- personal details including names, addresses, telephone numbers, email addresses, dates of birth, NHS numbers, National Insurance numbers
- lifestyle and social circumstances such as []

- financial details (including bank account details, payment card details and details about payments made to and from us to other people)
- education and employment details
- visual images of individuals, details regarding individual's personal appearance and behaviour
- technical information including internet protocol (IP) addresses, browser type and version, time zone setting and location, operating system and platform and other technology on devices used to access this website

We may also process special categories of personal data including:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- offences including alleged offences
- criminal proceedings, outcomes and sentences

We also collect, use and share aggregated data such as statistical aggregated data which could be derived from your personal data but is not considered personal data in law as this data will **not** directly or indirectly reveal your identity. For example, we may aggregate certain types of personal data to calculate the percentage of individuals who have a certain preference. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we will treat the combined data as personal data which will be used in accordance with this privacy policy.

Who the information is processed about

We process personal information about:

- residents/service users/patients
- personal representatives of the above
- complainants
- enquirers
- individuals captured by CCTV images
- offenders and suspected offenders
- employees and their next of kin

Who information is obtained from

The information we hold is obtained from:

- The subjects themselves
- Their next of kin or personal representatives
- Professional bodies engaged to represent the subject
- Other data controllers for whom we are processing data (eg. Local Authorities)
- Government agencies providing data relevant to our business (together the "**Sources**").

How the information is obtained

We may use different methods to collect data regarding data subjects, including:

- **Direct interactions.** This is when personal data regarding a subject is obtained directly by any of the Sources by filling in hard copy forms or forms on our website or by corresponding with us by post, phone, email or otherwise.

- **Automated technologies or interactions.** As individuals interact with our website, we will automatically collect technical data about their equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies.

How we use your personal information

We will only use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

Change of purpose

We only use 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 we need to use personal data for an unrelated purpose, we will notify the data subject and explain the legal basis which allows us to do so.

Please note that we may process personal data without knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Who the information may be shared with

We sometimes need to share the personal information we process with the data subject and also with other organisations for the purposes of performing the contract we are about to enter into or have entered into, where it is necessary for our legitimate interests (or those of a third party) and the data subject's interests and fundamental rights do not override those interests or where we need to comply with a legal obligation. The types of organisations we may need to share some of the personal information we process with for the purposes set out above may include:

- healthcare professionals, social and welfare organisations with whom or for whom we carry out legitimate business
- The Care Quality Commission or other legitimate regulators of our business
- family, associates and representatives of the person whose personal data we are processing
- central and local government
- suppliers and service providers
- employment and recruitment organisations
- credit reference agencies
- debt collection and tracing agencies
- business associates and other professional advisers
- financial organisations
- current, past or prospective employers
- educators and examining bodies
- people making an enquiry or complaint
- police forces and security organisations
- data processors with whom we contract (eg. Payroll service providers)

International Transfers



We do not transfer any personal data outside of the European Economic Area.

Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Data retention

- We will only retain personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting



requirements. We may retain personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation.

- To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the personal data, the purposes for which we process the personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.
-

Data Security

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

We have put in place procedures to deal with any suspected personal data breach and will notify any applicable regulator of a breach where we are legally required to do so.

Subject Access Requests

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information.

We must provide an individual with a copy of the information they request, free of charge. This must occur without delay, ideally within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

Right to lodge a complaint

You have the right to complain to the Information Commissioners Office on telephone helpline 0303 123 1113 or to Minster Care Group, 1 Grove Hill Road, Harrow, HA1 3AA or by email to one of the contact email addresses above or via our website at www.minstercaregroup.co.uk.

.