

## Your Rights as a Data Subject

Under the Data Protection Law (GDPR & E-Privacy) you have a number of rights.

These are:

### Right to Confirmation and Access

You have the right to confirm what personal data is being held and to what purpose it is being used.

You have the right to obtain copies of the personal data that is being held about you.

You have the right to obtain confirmation of the safeguards being implemented with regards any sharing of your personal data with third parties.

### Right to Be Forgotten (Right to Erasure)

You have the right to have information about you to be irretrievably erased. Where legal for us to do so, where it does not interfere with our ability to provide any ongoing services to you and so long as your request does not involve the interference of the personal data of another person, we will when requested:

1. Ensure the prompt erasure of that data within a reasonable amount of time – which you will be informed of
2. Issue the instruction to any third-parties, where they are acting as a processor on our behalf, to do the same

We will keep a minimum record of this request detailing:

1. Who you are (name, email address and what supporting documentation was used to verify your identity)
2. When you asked for the action to be undertaken
3. What action you asked to be undertaken
4. When the action was undertaken

This information is necessary to protect both you and the company and so we are recording this minimum information on the basis of legitimate interest.

### Subject Access Request

You have the right to request the nature and actual information that we hold about you and we are required to:

1. Inform you of the data we hold on you
2. Inform you of the data you have agreed for us to share with third-parties and who those third parties are
3. Have information requested on your behalf e.g. through a solicitor or a person with power of attorney or similar authority

Under usual circumstances we will ensure that we comply with the current law and provide this information to you within 30-days.

However, where there are large volumes of information or the request is complex we may be required to contact you for clarification. In the event of a complex request we will inform you of the likely timescale. In the event you are not satisfied with this you also have the right to complain by contacting us at the address set out in the contact details on page one of this document.

To complete a subject access request (SAR), please contact us at the address set out on page one of this document. You will be required to verify your identity appropriately before we release any personal data this may require us to undertake further identify checks against you/the information you have provided.

All subject access requests shall be recorded on our internal log.

#### The Right to Object to Automated Decision Making or Profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling. You will however, be informed in the relevant privacy policy of any automated decision making or profiling.

#### Right to Object to Processing

You have the right to object, on grounds relating to your situation, at any time, to the processing of personal data concerning you. However, you will be made aware of the consequences of any objection at the time it is raised.

#### The Right to Rectification

Where at all possible we will provide you direct access to update, correct and generally maintain your own information. We do this because you are more likely to be aware of changes to your information than we are. That said, we are also under an obligation to ensure that the personal information we have about you is correct in the event you are not able to update this yourself.

In the event that information changes please inform us of these changes by contacting us at the address set out on page one of this document and we will endeavour to update your personal information within 48-hours (mon-fri). Certain updates where they coincide with third party systems e.g. banking, may be withheld to ensure that there is reduced chance of corruption. You will be informed of this in the relevant privacy statement.

### Withdrawal of Consent and/or Limit Processing

In the event that we are using your personal data with your consent, you can withdraw that consent at any time.

You can do this by contacting us or in the case of newsletters, by clicking on the unsubscribe link (at the bottom of each newsletter) or managing your personal preferences.

In some case's you may not want to entirely withdraw consent but limit the breadth of processing we undertake using your data. The extent to which we process your data will be provided in the relevant privacy policy for the service(s) we are providing you. Some processing is necessary in order that we can deliver that service, any impact on this will be explained to you in the event you wish to limit processing. That said you can always contact us at the address set out on page one of this document, to discuss this.

The legal basis for processing will be explained to you in the specific privacy policy for that service.

### Right to Data Transfer

Some of our services use systems that allow us to export data in common formats such as comma separated values (csv) files, spreadsheets etc.

In the event that we are providing services that allow this type of export, you have the right to request that this information is exported and provided to you or another supplier of such services.

You will be required to provide the same identify verification information in the same manner as the subject access request.

### Right to Complain

If at any time you feel that we have failed to safeguard your information appropriately you have the right to complain.

In the first instance we would ask you to contact us and allow us to investigate and identify any issues you may have, by contacting us:

On-Line : <https://www.springhillcare.com>

Email : [info@springhillcare.com](mailto:info@springhillcare.com)

Phone : 01254 304500

Post: Riversway Care Limited, 11 Cannon Street, Accrington, Lancashire, BB5 1NJ, United Kingdom

You do however have the right to complain directly to the appropriate regulatory authority in your country, place of work or where you believe any issue has occurred.

In the case the UK, the regulatory authority is the Information Commissioners Office (ICO) and they can be contacted here:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF,

United Kingdom. Phone: +44 (0) 303 123 1113, Email: [casework@ico.org.uk](mailto:casework@ico.org.uk).

Website: <https://ico.org.uk>.

## **Security**

We operate a Privacy by Design and By Default policy. This means that before we use your data we have already considered the potential impact on you were your data to be lost, stolen, shared or compromised.

We undertake routine reviews of our processes and security policies in order to ensure that we can take all reasonable precautions in protecting your data.

Where at all possible we encrypt all information that is either stored or transmitted to third-parties. Where data is stored or transmitted to a Third Country (any country outside of the European Economic Area (EEA)) we will ensure appropriate adequacy protection is in place in accordance with Data Protection Legislation.

Consequently, we may also need to sometimes undertake further security and screening questions when undertaking our routine dealings with you these are there to protect your personal data and security.

Whilst we undertake all reasonable precautions, encryption, software updates and patches, we cannot guarantee the safety of data transmitted over the internet.

## **Data Breach**

In the event of a data breach of your personal data, which means:

“The unintended loss, destruction amendment or disclosure of personal data”

We will first do all that is necessary in order to minimise the impact on you, identify any potential malicious third-party, identify any third-parties that may also be impacted and take all reasonable efforts to ensure that you are notified.

In the event that we are notified by a third-party of a breach, in their systems, we will undertake the same level of efforts.

We will undertake this communication either directly with you as an individual or by sending out a public notification.

At the same time, we will comply with the current law in respect of informing the appropriate supervisory authority which is currently the Information Commissioners Office (ICO). We are under a legal requirement to report data breaches to the ICO.