The Radiant Hand

Data Protection Policy

The Radiant Hand Data Protection Policy

1. Context and Overview

Key Details

Policy prepared by: Amaryllis Holland and Helen Smith
Approved by Director: 20 May 2018
Policy operational date: 25 May 2018
Next review date: 24 May 2019

Introduction

The Radiant Hand Limited needs to gather and use a certain amount of information about individuals. These include customers, suppliers, business contacts, employees and other people the company has a relationship with or may need to contact.

This policy describes how this personal data is collected, handled and stored to the meet the data protection standards of The Radiant Hand and to comply with the law (The Data Protection Act (DPA) 1998) and the General Data Protection Regulation (GDPR 2016).

The lawful basis for us processing personal data under GDPR is 'Consent'.

Why this policy exists

This Data Protection Policy ensures The Radiant Hand:

- Complies with data protection law and follows good practice
- Protects the rights of customers, employees and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risk of data breach and responds appropriately to data breaches.

Data Protection Law

The DPA (1998) and the GDPR (2016) describe how organisations including The Radiant Hand Limited must collect, handle 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.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

8. Not be transferred outside of the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

2. People, risks and responsibilities

Policy Scope

This policy applies to:

- The head office of The Radiant Hand Limited
- All studios and therapy centres of The Radiant Hand Limited
- All employees and volunteers working for The Radiant Hand Limited
- All contractors, suppliers, and other people working on behalf of The Radiant Hand.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This includes:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Medical information
- Other information relating to and shared by individuals

Data Protection Risks

This policy helps to protect the Radiant Hand from data security risks and breaches 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.

Responsibilities

Everyone who works for or with The Radiant Hand has some responsibility for ensuring data is collected, stored and handled appropriately.

Each employee or contractor ("Team Member") that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- **Directors** are ultimately responsible for ensuring that The Radiant Hand meets its legal obligations.

- **The Data Protection Officer,** is responsible for:
    - Keeping the Directors updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Dealing with requests from individuals ('subject access requests') to see or delete any data The Radiant Hand holds about them.
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- **The IT Manager** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services The Radiant Hand is considering using to store or process data. For instance, cloud computing services. This evaluation will include a Privacy Impact Assessment.

- **The Marketing Manager** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from clients, customers, journalists or the media.
    - Where necessary working with other team members to ensure marketing initiatives abide by data protection principles.

3. General Guidelines

- The only people able to access data are those that need it for their work.
- The Radiant Hand Team members are responsible for keeping all data they have access to secure by taking sensible precautions including:
    - Locking mobile devices and laptops
    - Password protecting applications and documents where possible.
    - Strong passwords must be used and never shared.
    - Not saving or storing documentation on laptops or desktops that can be stored on the secure server provided.
    - Not sharing data informally.
    - Destroying paper notes with personal information on in line with this policy.
    - Not removing paper documents including personal data from any premises that is part of The Radiant Hand.
    - Ensuring all documentation is locked in required cabinets and not left unsecured in workspaces.
    - When access to confidential information is required, team members can ask The Data Protection Officer.

    - Not disclosing personal data to unauthorized people either inside or outside of The Radiant Hand.

- Team members must ask for help if they are uncertain about any area relating to data protection.
- The Radiant Hand provides guidance to all team members to help them understand their personal responsibilities when handling data.

4. Data Storage

These rules describe how data is stored at The Radiant Hand to ensure its security.

- **Data stored on paper**

    - When data is stored on paper it will be kept in an appropriate locked cabinet in locked premises that are part of The Radiant Hand (Head Office, Studio, Therapy Centre). This also applies to electronically stored data that has been printed out.
    - When not required, paper or files will be kept in a locked drawer or filing cabinet
    - Team members will ensure paper and printouts are not left where unauthorized people could see them, like on a printer.
    - Data printouts will be shredded and disposed of securely when no longer required.
    - Paper 'liability release forms' will be stored securely within a locked cabinet.
    - Notes from yoga courses attended will be kept in full for 2 years from the end date of the course. After 2 years an electronic record, detailing name and grade obtained will be kept and all paper documentation destroyed confidentially. Exceptions to this will be made where a dispute arose or may arise when the paper records may be kept for a maximum of 7 years and will then be destroyed confidentially.
    - Paper notes from therapies (including physiotherapy and massage) will be kept for 3 years after the end of the treatment and then destroyed confidentially.

- **Data stored electronically**

The Radiant Hand will only pass clients' details electronically to our administration provider companies; Glofox, Mailchimp and Stripe to administer each client's account with The Radiant Hand. These companies will not use your details for any other purpose including marketing their own products and services. Clients' details will never be shared with any other company.

Glofox supplies the cloud business management platform for The Radiant Hand and The Radiant Hand App, which is used for booking classes, courses and retreats. The Radiant Hand also sends push notifications via Glofox to clients who have actively consented to this. Clients can delete their own details at any time from Glofox, or can email info@theradianthand.co.uk to request this. Glofox can retrieve deleted

accounts. If permanent deletion is required, clients will need to email: info@theradianthand.co.uk and await email confirmation that this has been done within 14 days of the request being made.

Stripe provides online payment processing for The Radiant Hand. Clients can request deletion of their details from Stripe by emailing info@theradianthand.co.uk

The Radiant Hand uses Mailchimp as a platform for sending emails to clients who have actively consented to receiving marketing and communications. Clients can remove themselves from our mailing list by clicking 'unsubscribe' at the bottom of any email received. Alternatively, clients can email: info@theradianthand.co.uk and request that they are removed from our communications mailing lists.

- When data is stored electronically, it will be protected from unauthorized access, accidental deletion and malicious hacking attempts:

    - Data will be protected by strong passwords that are changed regularly.
    - Students and clients are required to protect their own data held on The Radiant Hand booking system by using strong passwords that are changed regularly via the website or app.
    - The Radiant Hand will delete all inactive accounts and information after 2 years of inactivity. Old accounts can be retrieved on request, unless permanent deletion has been requested, as outlined above.
    - No data will be stored on removable media such as USB keys, CDs or DVDs.
    - All data will be stored on designated servers and drives and will only be uploaded to approved cloud-based services including Glofox, Mailchimp and Stripe, as outlined above.
    - Servers are kept in secure locations separate from The Radiant Hand office storage.
    - Personal data is never saved directly on to laptops or other mobile devices like tablets or smart phones.
    - All servers and computers storing personal data are protected by security software and a firewall.

5. Data Use

Personal data is of no value to The Radiant Hand unless the business can make use of it to provide the services and products requested by students and clients. The point at which data is accessed by staff poses the greatest risk of data loss, corruption or theft:

- When working with personal data, team members will ensure the screens of computers and mobile devices are locked when unattended.
- Personal data is not shared informally, in particular it is not sent by email or text message as this form of communication is not secure.
- Data is encrypted before being transferred electronically.
- Personal data is never transferred outside of the European Economic Area, except for to Mailchimp with whom we have a data processing agreement in line with their EU-US Privacy Shield Framework.

- Team members do not save copies of personal data to their own computers. Only one version of personal data is stored centrally on the servers or cloud computing services for access and use.

6. Data Accuracy

The law requires The Radiant Hand to take reasonable steps to ensure data is kept up to date and accurate.

It is the responsibility of all team members who work with data or personal information to take reasonable steps to ensure it is kept accurate and up to date.

- Personal information and data will only be held on the Glofox system and paper records that require the individual to be identified. No other copies of information will be created.
- Team members will take opportunities to ensure information held is up to date including checking with students and clients from time to time that the information we hold is accurate.
- The Radiant Hand has made it easy for students and clients to update the information we hold on them using our website or app booking system.
- If we become aware that the information we hold is out of date it will be deleted, for example if we can no longer reach a student on a telephone number we hold, the number is deleted.

7. Data Breaches

Data breaches refer to any accidental or deliberate breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

Any breaches are reported to the Data Protection Officer who logs the breach and assesses the associated risks and takes action to minimise any negative impact to clients, staff or The Radiant Hand itself. If the Data Protection Officer deems the breach sufficiently serious the individual client and / or Information Commissioners Office (ICO) will be informed as appropriate.

8. Access Requests

All individuals who are the subject of personal data held by The Radiant Hand are entitled to:

- Ask what information we hold and why.
- Ask how to gain access to information held.
- Be informed as to how to keep it up to date.
- Be informed as to how the company is meeting its data protection obligations.

- View any information held by The Radiant Hand, pertaining to the individual who has made the request.

If an individual contacts The Radiant Hand requesting this information, this is known as a subject access request.

- Subject access requests from individuals should be made via email to info@theradianthand.co.uk for the attention of the Data Protection Officer.
- The Data Protection Officer will confirm receipt of the request within 72 hours and aim to provide the relevant data within 14 days.
- The Data Protection Officer will verify the identity of anyone making a subject access request before handing over any information.

9. Disclosing Data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the individual data subject.

Under these circumstances, The Radiant Hand will disclose the information requested. However the Data Protection Officer will confirm the request is legitimate in the first instance, seeking assistance from the Director and legal advice where necessary.

10. Providing Information

The Radiant Hand aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, The Radiant Hand has a Privacy Statement, setting out how data relating to individuals is used by the company.