Cellulite Slayer Limited

GDPR Policy

1. Introduction

This Data Protection Policy (this "policy") sets out the obligations of Cellulite Slayer Limited ("Cellulite Slayer", "we", "us", "our") regarding data protection and the rights of individuals whose personal data we collect, use and process in the course of our business activities.

This policy applies to all Cellulite Slayer employees, workers and contractors ("personnel", "you", "your"). Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action, up to and including termination for serious offences.

This policy has been prepared with due regard to the data protection laws applicable to Cellulite Slayer and our personal data processing activities. These data protection laws include the General Data Protection Regulation (EU Regulation 2016/679) and the Data Protection Act 2018 (the "law").

This policy should be read together with the Cellulite Slayer Website Privacy Policy.

2. Policy Statement

Cellulite Slayer places high importance on respecting the privacy and protecting the personal data of individuals with whom we work including our clients, end customers and employees. We are committed to the fair, lawful and transparent handling of personal data and to facilitating the rights of individuals. Our policy is to comply not only to the letter of the law, but also to the spirit of the law.

3. Scope

This policy applies to all personal data processed by Cellulite Slayer Limited whether held in electronic form or in physical records, and regardless of the media on which that data is stored. It applies to personal data we process as a controller and personal data we process as a processor (on behalf of our customers).

Cellulite Slayer Limited is registered as a data controller with the Information Commissioner's Office having registration number ZB182218.

4. Definitions

"**Personal data**" means any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in

particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"**Process**" or "**processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Sensitive personal data**" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, biometric data (where use to identify a data subject), data concerning health, data concerning a natural person's sex life or sexual orientation; and personal data relating to criminal convictions and offices.

5. Responsibilities

Key data protection responsibilities within Cellulite Slayer are as follows:

- The Cellulite Slayer Managing Director is accountable for ensuring we meet our data protection obligations;
- The Managing Director is responsible for implementing and enforcing this policy;
- The Managing Director is responsible for ensuring that personnel under their management are made aware of adhere and to this policy;
- All personnel working with personal data over which they have decision making authority are responsible for ensuring it is kept securely, is accessible only to those who need to use it and is not disclosed to any third party without the authorisation of the Managing Director; and
- All personnel are required to read, understand, and adhere to this policy when processing personal data on our behalf.

6. Data Protection Principles

The following data protection principles shall govern the collection, use, retention, transfer, disclosure, and destruction of personal data by Cellulite Slayer:

- **Principle 1 - Fair, Lawful & Transparent**
  Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Principle 2 - Purpose Limitation**
  Personal data must only be collected and processed for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- **Principle 3 - Data Minimisation**
  Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Principle 4 - Accuracy:**
  Personal data must be accurate and kept up to date.

- **Principle 5 - Storage Limitation:**
  Personal data which permits identification of data subjects (i.e., data which has not been anonymised) must be kept for no longer than is necessary for the purposes for which the personal data are processed.

- **Principle 6 - Security:**
  Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

7. Data Processing Obligations

Cellulite Slayer as a Processor

Where Cellulite Slayer is a data processor, we may only process personal data in accordance with the controller's documented instructions as set out in a data processing agreement. We may only transfer personal data out of the UK and appoint sub-processors as permitted by the data processing agreement.

Personal data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Access to the personal data must be limited only to personnel who are subject to an obligation of confidentiality and who need access to carry out their assigned duties.

We must assist the controller to meet their compliance obligations under applicable laws including for the purposes of:

1. Ensuring the security of processing, including by implementing appropriate technical and organisational measures.
2. Supporting the facilitation of subject rights of data subjects whose personal data we hold;
3. Enabling the controller to notify data protection authorities following a breach of personal data presenting a risk to affected data subjects;
4. Enabling the controller to notify affected data subjects following a breach of personal data presenting a high risk to their rights and freedoms; and
5. Supporting data protection impact assessments carried out by the controller as appropriate.

Upon termination of the data processing agreement we must delete or return personal data as set out at Section 12 of this policy.

We must also support the controller to demonstrate accountability and compliance with applicable laws by providing them with all information necessary to demonstrate compliance by Cellulite Slayer and allow for and participate in audits by the controller or their representative.

Cellulite Slayer as a Controller

Where Cellulite Slayer is the data controller, data subjects must be provided with information notifying them of the purposes for which Cellulite Slayer will process their personal data (a "privacy notice"). When personal data is obtained directly, the privacy notice shall be provided to the data subject at the time of collection. When personal data is obtained indirectly, the privacy notice shall be provided to the data subject as soon as possible (and not more than one calendar month) after it is obtained from a third party. The privacy notice must explain what processing will occur and must also include the information set out at Schedule 1.

Use of the personal data by Cellulite Slayer must match the description given in the privacy notice and be limited to what is necessary for the specific purposes stated. Where our lawful basis for processing is based on our legitimate interests, we may only process the personal data if our legitimate interests are not outweighed by the interests, rights and freedoms of the data subjects in question. A legitimate interest assessment must be performed to confirm this.

We must not collect or process any more personal data than is strictly necessary for the purposes of the processing ("data minimisation") as set out in our privacy notice and must ensure that data minimisation continues to be applied throughout the lifetime of the processing activities.

Personal data must be kept accurate and up to date. The accuracy of personal data must be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps are to be taken without delay to amend or erase that data, as appropriate. Personal data must not be kept for any longer than is necessary for the purpose for which that data was originally collected and processed. When the data is no longer required, all reasonable steps must be taken to securely erase or dispose of it without delay, as set out at Section 12 of this policy.

Personal data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

8. Accountability

Only those personnel that need access to, and use of, personal data in order to carry out their assigned duties correctly will be permitted access to personal data we hold. All personnel handling personal data on behalf of Cellulite Slayer must be:

- Made fully aware of both their individual responsibilities and Cellulite Slayer's responsibilities under this policy and applicable law, and be provided with a copy of this policy;
- Appropriately trained to do so and suitably supervised, with training to be provided upon starting with Cellulite Slayer and refresher training to be provided at least annually; and
- Bound to handle the personal data in accordance with this policy and the law by contract.

The methods of collecting, holding and processing personal data by personnel, or other parties working on our behalf, are to be regularly evaluated and reviewed by line managers.

All consultants, agencies and other parties working on our behalf and handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as applicable to Cellulite Slayer personnel arising out of this policy.

When using a data processor (or, where permitted, a sub-processor), a binding contract must be implemented between Cellulite Slayer and the data processor setting out the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data and categories of data subject; and the obligations and rights of the controller. Processor contracts must also include the terms set out at Schedule 2.

Data Processor RoPA

Where Cellulite Slayer is a data processor, the RoPA will incorporate the following information:

- The name and contact details of the data processor and of each controller on behalf of which we are acting as data processor and of our Data Protection Officer;

- The categories of processing carried out on behalf of each controller;
- Details of any transfers of personal data to countries outside the European Economic Area ("EEA") including all mechanisms and security safeguards;
- Descriptions of the technical and organisational measures we have implemented to ensure the security of personal data.

9. Risk Management

Cellulite Slayer will monitor the risks to data subjects associated with all existing and planned personal data processing activities and implement appropriate technical and organisational measures to safeguard data subjects and ensure the data protection principles set out in this policy are met. This risk led approach to data protection will be applied across all Cellulite Slayer business activities to ensure data protection by design and by default.

Where the risks to rights and freedoms of data subjects associated with any existing or planned personal data processing to be carried out by Cellulite Slayer are potentially high or where otherwise required by applicable law or a data protection authority in a member state in which we operate, Cellulite Slayer will carry out a Data Protection Impact Assessment ("DPIA"). A record of DPIAs shall be kept, to include details of the outcome, the names of the parties signing off the DPIA recommendations and the date of next review.

Where a controller carries out a DPIA in relation to a processing activity in Cellulite Slayer is a data processor, we will provide all information and assistance to the controller as is reasonably required for the purpose of the DPIA.

10. Data Subject Rights

Data subjects have the following rights regarding personal data processing and the data that is collected and held about them:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights with respect to automated decision-making and profiling.

Requests by data subjects to exercise their rights must be facilitated as set out in the Cellulite Slayer Data Subject Rights Procedure.

Where Cellulite Slayer is the data controller, we are responsible for facilitating data subjects' rights. Where we are a data processor, we must assist the controller to facilitate data subjects' right as appropriate.

11. Protection of Personal Data

All personnel must comply with the following when working with personal data:

- Personal data must be handled with care at all times and must not be shared with any colleague, who does not have access to it, or with any third party without authorisation;
- Physical records must not be left unattended or on view to unauthorised employees, agents, contractors or other parties at any time and must not be removed from the business premises without authorisation;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- All physical copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked filing cabinet, drawer, box or similar;
- All electronic copies of personal data are to be stored securely using passwords which are changed regularly, and which do not use words or phrases that can be easily guessed or otherwise compromised;
- Personal data must not be transferred to any device personally belonging to an employee or transferred or uploaded to any personal file sharing, storage, communication or equivalent service (such as a personal cloud service);
- Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this policy and the law (which may include demonstrating that all suitable technical and organisational measures have been taken and entering in to a data processor contract with Cellulite Slayer);
- All personal data stored electronically shall be backed-up regularly and securely; and
- Under no circumstances must any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

12. Data Retention & Destruction

Cellulite Slayer as a Data Processor

Where Cellulite Slayer is a data processor, we may only retain personal data for the duration of the data processing agreement. Upon termination of the data processing agreement, we must, at the choice of the controller, delete or return all the personal data to the controller and delete all existing copies unless otherwise required to store a copy by UK law.

Cellulite Slayer as a Data Controller

Where Cellulite Slayer is the data controller, we may only retain personal data for as long as is reasonably required.

Once personal data records have reached the end of their life, they must be securely destroyed in a manner that ensures that they can no longer be used.

13. International Data Transfers

We will only transfer ('transfer' includes making available remotely) personal data from the UK where:

- the transfer is to a country (or an international organisation) that the European Commission has determined ensures an adequate level of protection;
- an International Data Transfer Agreement has been put in place;
- standard contractual clauses adopted by the European Commission have been put in place between the entity in the EEA and the entity located outside the EEA and the UK recognised transfer addendum has been added;
- binding corporate rules have been implemented, where applicable; or where
- the transfer is otherwise permitted by the law.

Where Cellulite Slayer is a data processor, transfers of personal data outside the UK shall only be made with the controller's agreement.

14. Data Breach Notifications

All personal data breaches must be reported immediately to the CEO and must be added to the register of personal data breaches.

Cellulite Slayer as a Data Processor

Where Cellulite Slayer is a data processor, and a personal data breach occurs, and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the controller must be notified immediately with further information about the breach provided as soon as information becomes available.

Cellulite Slayer as a Data Controller

Where Cellulite Slayer is the data controller, and a personal data breach occurs which is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the appropriate data protection authority must be notified of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of data subjects, all affected data subjects are to be informed of the breach directly and without undue delay.

Irrespective of whether Cellulite Slayer is a data processor or a data controller, all data breach notifications must be handled strictly in accordance with the Cellulite Slayer Personal Data Breach Procedure and be added to the Cellulite Slayer Personal Data Breach Register.

15. Implementation & Policy Management

This policy shall be deemed effective as of 25th May 2018. No part of this policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This policy will be reviewed annually and following any personal data breach by the Managing Director.

16. Version & Revision History

Version	Date	Author	Summary of Revisions
1.0	07/11/2021	Contractor	First Version

Schedule 1
Privacy Notices

Privacy notices for data subjects shall include:

1. Details of the data controller including, but not limited to, the identity of its Data Protection Officer, where applicable;
2. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
3. Where applicable, the legitimate interests upon which Cellulite Slayer is justifying its collection and processing of the personal data;
4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
5. Where the personal data is to be transferred to one or more third parties, details of those parties;
6. Where the personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including but not limited to the safeguards in place;
7. Details of the length of time the personal data will be held (or, where there is no predetermined period, details of how that length of time will be determined);
8. Details of the data subject's rights;
9. Where applicable, details of the data subject's right to withdraw their consent to the processing of their personal data at any time;
10. Details of the data subject's right to complain to a data protection authority;
11. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
12. Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

Schedule 2
Processor Contracts

Contracts with data processors who will process the personal data must set out the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data and categories of data subject; and the obligations and rights of the controller. They must also include terms requiring the processor to:

a) only act on the written instructions of the controller;
b) ensure that people processing the data are subject to a duty of confidence;
c) take appropriate measures to ensure the security of processing;
d) only engage sub-processors with the prior consent of the controller and under a written contract;
e) assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR (or other applicable laws);
f) assist the controller in meeting its GDPR obligations (or obligations under other applicable laws) in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
g) delete or return all personal data to the controller as requested at the end of the contract; and
h) submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the controller immediately if it is asked to do something infringing the GDPR (or other applicable laws).