Data Protection Policy

1. This data protection policy is designed to ensure that the rights to privacy of individuals are protected. Reeth Medical Ltd is committed to the principles set out in the General Data Protection Regulation and has reviewed its personal data processing activities so as to carry on its business as a Private Medical Services provider in compliance with the provisions of the Regulation.

2. **Data protection lead:** this person is responsible for ensuring compliance with policies and procedures on data protection, for providing any staff training, for conducting audits, risk assessments and data protection impact assessments, for responding to requests from data subjects and dealing with data breaches. He or she also handles queries and complaints from data subjects about the processing of their data, including from any members of staff. The name of the data protection lead is Marie Brookes.

3. ***Data subject:*** an individual whose personal data is processed.

   Reeth Medical Ltd processes personal data belonging to those who wish to obtain expert advice in relation to legal issues or disputes, and also individuals linked in any way to the circumstances giving rise to those issues. The personal data of any members of staff is also processed.

4. ***Personal data:*** any information from which a living individual can be identified, either directly or indirectly. It is not limited to names and identification numbers, or to photographs or addresses.

   The categories of personal data Reeth Medical Ltd processes include:

Legal cases

- Names, addresses, dates of birth and other personal data contained in witness statements and other evidence relevant to the legal issues;

- Health information contained in medical records, together with information on sex, race and ethnic origin;

- Personal data in invoices and copy receipts, accounting records, tax and VAT returns and related information;

- Copy passports, driving licenses, utility bills and other documents used to check identity;

5. **Special category data:** information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic and biometric data, health information and data in relation to a person' s sex or sexual orientation.

   The special category personal data Reeth Medical Ltd holds includes:

- Medical and other health records
- Information on sex, race and ethnic origin

6. ***Processing:*** covers any activity involving personal data, including holding, storage and destruction. The Information Commissioner says it is difficult to image an activity involving personal data that does not fall within the definition.

7. Reeth Medical Ltd processes personal data in order to carry out its work as an expert witness and when carrying out other functions necessary to its business.

8. The data processing activities include: compiling expert reports, taking copies of identity documents and storing them in files or online, sending and receiving emails internally and externally, submitting invoices and filing them with receipts, uploading documents onto the cloud, using a customer relationship management system, archiving and destroying information.

9. ***Sharing of personal data:*** Reeth Medical Ltd shares personal internally, and also externally only when necessary to achieve its business purposes. In particular, it shares data with the following:

- Confidential waste disposal companies
- Website providers
- Cloud storage providers
- IT support providers
- Accountants and other professional advisers
- HMRC
- VAT Commissioner
- Companies House

There is no transfer of data abroad.

10. ***Data controller:*** decides the why and the how of personal data processing. A controller can be a sole trader, a partnership, a private or public limited company or a large multi-national organization. It decides why it needs to collect personal data and how to process it. Marie Brookes is a data controller for the purposes of this policy.

11. ***Data processor:*** processes personal data in accordance with the written instructions of the data controller. Most of the organisations that Reeth Medical Ltdshares personal data with are processors.

12. ***Legitimising conditions:*** The processing of personal data is unlawful unless a legitimising condition, or lawful basis, applies. Reeth Medical Ltd generally relies on the following legitimising conditions:

- Legitimate interest as a business
- Contract (with employees)
- Consent

When processing special category data, Reeth Medical Ltd generally relies on one of the following additional legitimising conditions

- Legal claims
- Explicit consent

Reeth Medical Ltd avoids relying on the consent basis where possible. In order to be valid, consent must be freely given and as easily withdrawn as it was to give it.

13. ***Data protection principles:*** Where there is a lawful basis for processing personal data, Reeth Medical Ltd takes proportionate steps to ensure it carries out its personal data processing activities in accordance with the various conditions or principles contained in the GDPR.

14. ***Accountability:*** This principle is designed to ensure that data protection is embedded in an organisation at all levels of decision making and becomes fundamental to its culture. Not only must Reeth Medical Ltd comply with the General Data Protection Regulation but it must be able to show it complies. It is for this reason that this policy, and the appended policies have been written..

15. **Data protection by design:** This is an aspect of the accountability principle. It means that data protection risks are evaluated and eradicated

and reduced at the very earliest stage, whenever there is a significant change in processes or procedures which entail a risk to data subjects. Examples: a substantial upgrade to an IT system, the introduction of CCTV cameras, outsourcing such as engaging a new cloud provider. Data Protection Impact Assessments are carried out by the data protection lead in these and other circumstances where there is likely to be a high risk to data subjects.

16. ***Data protection by default: minimisation:*** Another important principle is data minimisation. In other words, no more data should be collected, shared and stored than is strictly necessary. The retention periods for the personal data Reeth Medical Ltd stores are up to six years, as necessary. A schedule of retention periods is appended to this policy.

17. ***Security:*** This is one of the most important principles. Reeth Medical Ltd has taken physical, organisational and technical measures to ensure that its personal data is secure. Hard copy as well as electronic data is processed in accordance with Reeth Medical Ltd's security policy, attached to this policy.

18. It is important that all members of staff comply with the security policy. Failure to do so is a disciplinary offence that may result in dismissal.

19. ***Personal data breach:*** The data protection lead is responsible for responding to personal data breaches. He or she notifies the Information Commissioner as necessary, and also data subjects where the risk to them is high.

20. Breaches which carry any risk to data subjects must be reported to the Information Commissioner's Office (ICO) within 72 hours, together with a summary of the nature of the breach, the steps taken to reduce the risk to data subjects, and measures to prevent the breach from happening again. Reeth Medical Ltd's data breach policy is attached.

21 ***Rights of data subjects:*** Data subjects have eight rights which include:

- Right to be informed about what Reeth Medical Ltd does with personal data;
- Right of access to personal data by means of a subject access request;
- Right to rectification of inaccurate data, and to add to the information Reeth Medical Ltd holds about the data subject if it is incomplete;
- Right to erasure, otherwise known as the right to be forgotten;
- Right to restrict the processing of personal data;

- Right to object to the processing Reeth Medical Ltd carries out based on its legitimate interest.

Reeth Medical Ltd must respond to requests from data subjects within one month. The procedure for responding to requests is appended to this policy.

22. ***Human Resources:*** is responsible for processing the personal data of members of staff. It is stored in hard copy files that are stored securely/electronic files stored securely in the cloud. Access to these files is restricted. Special category data, such as medical records, is further restricted as appropriate. Special category data stored electronically are encrypted. No personal data is shared outside Human Resources, other than with the member of staff's manager.

23. All members of staff receive training in data protection.

24. **Data Protection Risk Register:** All personal data processing activities are recorded in the data protection risk register.

25. Personal data breaches are recorded in the risk register, whether they are reportable or not.

26. The risk register contains a copy of all audits, risk assessments and Data Protection Impact Assessments.

27. The data protection lead holds the risk register.

28. **Enforcement and disciplinary action:** Failure to comply with the General Data Protection Regulation is a criminal offence in many cases and can result in large fines. It is important that all staff are aware of this policy, receive training in data protection, and that this policy is properly implemented.

29. Any staff failure to comply with this and its associated policies is a disciplinary offence which may lead to disciplinary action and dismissal.