Data Protection & Retention Policy

1. **Introduction**
   This Policy sets out the obligations of Rose Yoga, regarding data protection and the rights of clients ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

   The GDPR defines "personal data" as 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.

   This Policy sets Rose Yoga's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Rose Yoga, its employees, agents, contractors, or other parties working on behalf of the Rose Yoga.

   Rose Yoga is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. **The Data Protection Principles**
   This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:
   1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
   2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
   3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
   4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. **The Rights of Data Subjects**
   The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):
   1. The right to be informed (Part 12).
   2. The right of access (Part 13);
   3. The right to rectification (Part 14);
   4. The right to erasure (also known as the 'right to be forgotten') (Part 15);
   5. The right to restrict processing (Part 16);
   6. The right to data portability (Part 17);
   7. The right to object (Part 18); and
   8. Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. **Lawful, Fair, and Transparent Data Processing**
   1. The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:
      1. The data subject has given consent to the processing of their personal data for one or more specific purposes;
      2. The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
      3. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
      4. The processing is necessary to protect the vital interests of the data subject or of another natural person;
      5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
      6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject

is a child.

5. **Specified, Explicit, and Legitimate Purposes**
    1. Rose Yoga collects and processes the personal data set out in Part 21 of this Policy.
    2. Rose Yoga only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).
    3. Data subjects are kept informed at all times of the purpose or purposes for which Rose Yoga uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. **Adequate, Relevant, and Limited Data Processing**
   Rose Yoga will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. **Accuracy of Data and Keeping Data Up-to-Date**
    1. Rose Yoga shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.
    2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. **Data Retention**
    1. Rose Yoga shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
    2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
    3. For full details of Rose Yoga's approach to data retention, including retention periods for specific personal data types held by Rose Yoga, please refer to Part 21 of this Policy

9. **Secure Processing**
   Rose Yoga shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. **Accountability and Record-Keeping**
    1. Rose Yoga's Data Protection Officers is Rosie Moss
    2. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, Rose Yoga's other data

protection-related policies, and with the GDPR and other applicable data protection legislation.

3. Rose Yoga shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
    1. The name and details of Rose Yoga, its Data Protection Officers, and any applicable third-party data processors;
    2. The purposes for which Rose Yoga collects, holds, and processes personal data;
    3. Details of the categories of personal data collected, held, and processed by Rose Yoga, and the categories of data subject to which that personal data relates;
    4. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
    5. Details of how long personal data will be retained by Rose Yoga (please refer to Rose Yoga's Data Retention Policy); and
    6. Detailed descriptions of all technical and organisational measures taken by the Rose Yoga to ensure the security of personal data.

11. **Data Protection Impact Assessments**
    1. Te Rose Yoga shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.
    2. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
        1. The type(s) of personal data that will be collected, held, and processed;
        2. The purpose(s) for which personal data is to be used;
        3. The Rose Yoga's objectives;
        4. How personal data is to be used;
        5. The parties (internal and/or external) who are to be consulted;
        6. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
        7. Risks posed to data subjects;
        8. Risks posed both within and to Rose Yoga; and
        9. Proposed measures to minimise and handle identified risks.

12. **Keeping Data Subjects Informed**
    1. Rose Yoga shall provide the information set out in Part 12.2 to every data subject:
        1. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
        2. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
            1. if the personal data is used to communicate with the data subject, when the first communication is made; or
            2. if the personal data is to be transferred to another party, before that transfer is made; or
            3. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

2. The following information shall be provided:
    1. Details of Rose Yoga including, but not limited to, the identity of its Data Protection Officers;
    2. The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
    3. Where applicable, the legitimate interests upon which the Rose Yoga 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 European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
    7. Details of data retention;
    8. Details of the data subject's rights under the GDPR;
    9. Details of the data subject's right to withdraw their consent to the Rose Yoga's processing of their personal data at any time;
    10. Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
    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 or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. **Data Subject Access**
    1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which Rose Yoga holds about them, what it is doing with that personal data, and why.
    2. Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to rosie_moss@hotmail.com
    3. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
    4. All SARs received shall be handled by Rose Yoga's Data Protection Officers.
    5. Te Rose Yoga does not charge a fee for the handling of normal SARs. Rose Yoga reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. **Rectification of Personal Data**
    1. Data subjects have the right to require Rose Yoga to rectify any of their personal data that is inaccurate or incomplete.
    2. Rose Yoga shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Rose Yoga of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
    3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. **Erasure of Personal Data**
    1. Data subjects have the right to request that Rose Yoga erases the personal data it holds about them in the following circumstances:
        1. It is no longer necessary for Rose Yoga to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
        2. The data subject wishes to withdraw their consent to Rose Yoga holding and processing their personal data;
        3. The data subject objects to Rose Yoga holding and processing their personal data (and there is no overriding legitimate interest to allow the Rose Yoga to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
        4. The personal data has been processed unlawfully;
        5. The personal data needs to be erased in order for the Rose Yoga to comply with a particular legal obligation
    2. Unless Rose Yoga has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
    3. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**
    1. Data subjects may request that Rose Yoga ceases processing the personal data it holds about them. If a data subject makes such a request, Rose Yoga shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
    2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. **Data Portability**
    1. Rose Yoga does not process personal data using automated means.

2. Where data subjects have given their consent to Rose Yoga to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between Rose Yoga and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
3. To facilitate the right of data portability, Rose Yoga shall make available all applicable personal data to data subjects in the following formats:
    1. PDF.
    2. WORD/EXCEL.
4. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
5. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. **Objections to Personal Data Processing**
    1. Data subjects have the right to object to Rose Yoga processing their personal data based on legitimate interests, direct marketing (including profiling),
    2. Where a data subject objects to Rose Yoga processing their personal data based on its legitimate interests, Rose Yoga shall cease such processing immediately, unless it can be demonstrated that Rose Yoga's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
    3. Where a data subject objects to Rose Yoga processing their personal data for direct marketing purposes, Rose Yoga shall cease such processing immediately.

19. **Automated Decision-Making**
    1. Rose Yoga does not use uses personal data in automated decision-making processes.

20. **Profiling**
    1. Rose Yoga does not use personal data for profiling purposes.

21. **Personal Data Collected, Held, and Processed including Retention Periods**
    The following personal data is collected, held, and processed by the Rose Yoga

Type of Data	Purpose of Data	Review Period	Retention Period
Contact Details	To communicate with clients	Annually	6 years
Billing Data	Ability to invoice	Annually	6 years
Bank Account Details	Ability to set up S/O & D/D	Once ceases to be a client	6 years
Client Data	Provided & used to provide consultancy services	Annually	6 years

22. **Data Security - Storage**

Rose Yoga shall ensure that the following measures are taken with respect to the storage of personal data:

1. All electronic copies of personal data should be stored securely using passwords and data encryption;
2. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
3. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Rose Yoga where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to Rose Yoga that all suitable technical and organisational measures have been taken).

23. **Data Retention**

1. As stated above, and as required by law, Rose Yoga shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

2. Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

3. When establishing and/or reviewing retention periods, the following shall be taken into account:
    1. The objectives and requirements of Rose Yoga;
    2. The type of personal data in question;
    3. The purpose(s) for which the data in question is collected, held, and processed;
    4. Rose Yoga's legal basis for collecting, holding, and processing that data;
    5. The category or categories of data subject to whom the data relates;
    6. Professional Indemnity Insurance; Ability to carry out consultancy services; HMRC.

4. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

5. Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period

where a decision is made within Rose Yoga to do so (whether in response to a request by a data subject or otherwise).

6. In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

24. **Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Upon the expiry of the data retention periods set out below in Part 21 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

1. Personal data stored electronically (including any and all backups thereof) shall be deleted securely

2. Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely

3. Personal data stored in hardcopy form shall be shredded by cross shredder in office

4. Special category personal data stored in hardcopy form shall be shredded by office cross shredder.

25. **Data Security - Use of Personal Data**

Rose Yoga shall ensure that the following measures are taken with respect to the use of personal data:

1. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of Rose Yoga requires access to any personal data that they do not already have access to, such access should be formally requested from Rose Yoga
2. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of Rose Yoga or not, without the authorisation from Rose Yoga
3. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
4. 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; and

5. Where personal data held by Rose Yoga is used for marketing purposes, it shall be the responsibility of Rose Yoga to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

26. **Data Security - IT Security**
Rose Yoga shall ensure that the following measures are taken with respect to IT and information security:
    1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
    2. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Rose Yoga, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
    3. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Rose Yoga's IT staff shall be responsible for installing any and all security-related updates as soon as possible after the updates are made available by the publisher or manufacturer unless there are valid technical reasons not to do so; and
    4. No software may be installed on any Rose Yoga-owned computer or device without the prior approval of the owner of Rose Yoga.

27. **Organisational Measures**
Rose Yoga shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:
    1. All employees, agents, contractors, or other parties working on behalf of the Rose Yoga shall be made fully aware of both their individual responsibilities and the Rose Yoga's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
    2. Only employees, agents, sub-contractors, or other parties working on behalf of Rose Yoga that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Rose Yoga;
    3. All employees, agents, contractors, or other parties working on behalf of Rose Yoga handling personal data will be appropriately trained to do so;
    4. All employees, agents, contractors, or other parties working on behalf of Rose Yoga handling personal data will be appropriately supervised;
    5. All employees, agents, contractors, or other parties working on behalf of Rose Yoga handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
    6. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

7. All personal data held by Rose Yoga shall be reviewed periodically, as set out in Rose Yoga's Data Retention Policy;
8. The performance of those employees, agents, contractors, or other parties working on behalf of Rose Yoga handling personal data shall be regularly evaluated and reviewed;
9. All employees, agents, contractors, or other parties working on behalf of Rose Yoga handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
10. All agents, contractors, or other parties working on behalf of th Rose Yoga 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 those relevant employees of Rose Yoga arising out of this Policy and the GDPR; and
11. Where any agent, contractor or other party working on behalf of Rose Yoga handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Rose Yoga against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

28. **Data Breach Notification**
    1. All personal data breaches must be reported immediately to Rose Yoga's Data Protection Officers.
    2. If 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 Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
    3. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
    4. Data breach notifications shall include the following information:
        1. The categories and approximate number of data subjects concerned;
        2. The categories and approximate number of personal data records concerned;
        3. The name and contact details of Rose Yoga's data protection officer (or other contact point where more information can be obtained);
        4. The likely consequences of the breach;
        5. Details of the measures taken, or proposed to be taken, by Rose Yoga to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

29. I**mplementation of Policy**

    This Policy shall be deemed effective as of 01.01.2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.