

PRIVACY POLICY

Policy, scope and objectives

On May 2018 the General Data Protection Regulation entered force. Calm (registration software) has a Privacy Policy applicable for the use of Calm.

1.1 Statement

The management of the Vipassana association, located at Dhamma Mahi Vipassana Centre at 89350-Louesme in France, is committed to comply with all relevant EU laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information the Trust collects in accordance with the General Data Protection Regulation (GDPR).

1.2 Commitment

The trust is committed to complying with data protection legislation and good practice including:

- A. processing personal information only where this is strictly necessary for legitimate organizational purposes;
- B. collecting only the minimum personal information required for these purposes and not processing excessive personal information;
- C. providing clear information to individuals about how their personal information will be used and by whom;
- D. only processing relevant and adequate personal information;
- E. processing personal information fairly and lawfully;
- F. maintaining an inventory of the categories of personal information processed by the trust;
- G. keeping personal information accurate and, where necessary, up to date;
- H. retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organizational purposes;
- I. respecting individuals' rights in relation to their personal information, including their right of subject access;
- J. keeping all personal information secure; the data will be accessed only a minimum of times and by a minimum of people. Only when absolutely necessary.
- K. only transferring personal information outside the EU in circumstances where it can be adequately protected;
- L. the application of the various exemptions allowable by data protection legislation;

1.3 Purpose of Collecting and Storing the Data

The trust and it's volunteers (servers please see definitions below) collects and assesses the information for the following purposes;

1. to enable the Assistant Teacher or server on his/her behalf to assess if a student is suitable to be accepted for a course;
2. to enable the center management to plan accommodation, food and sometimes transport for the Student;
3. to enable proper guidance and assistance to be given to the student prior to, during and after a Vipassana Meditation course;
4. for legal reasons or for the performance of the contract which means to process information that is needed to provide the student or server with the service he/she requested;
5. in order to provide extra course related services after consent has been given for these services or legitimate interest of the organization has been demonstrated.
6. In order to provide newsletter services or to keep financial records (including donations)

For as far as the use of personal data is covered by the use of the Calm software, the Calm Privacy Policy and relevant instructions prevail.

Notification

European centers have chosen to use the Calm system for general registration. Calm is the lead controller for the general application process, the referral and special list, long course applications and for the use of additional software. Calm has notified the Data Protection Authority, "De Autoriteit Persoonsgegevens", in The Hague, The Netherlands, that it is a data controller and that it processes certain information about data subjects.

Calm has identified all the personal data that it processes and this is contained in the Data Inventory Register. The Data Protection Officer has been appointed by Calm and also for this Trust.

1.4 A copy of the DPA notification is retained by Data Protection Officer and the DPA Notification Handbook is used as the authoritative guidance for notification.

1.5 The DPA notification is renewed annually.

1.6 The Data Protection Officer (DPO) is responsible, each year, for reviewing the details of notification, in the light of any changes to the trusts activities (as determined by changes to the Data Inventory Register and the management review) and to any additional requirements identified by means of data protection impact assessments. The policy applies to all servers and student in this trust and to all third parties and suppliers.

Partners and any third parties working with or for the trust, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the trust without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less than those to which the trust is committed, and which gives the trust the right to audit compliance with the agreement.

2. Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Definitions used by the organisation (drawn from the GDPR)

Territorial scope – the GDPR will apply to all controllers that are established in the EU (European Union and the European Economic Area countries) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior to data subjects who are resident in the EU.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative center. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organization.

Processing – 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, organization, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Specific additional definitions

Student: Anyone who applies to or attends a Vipassana Meditation course led by an Assistant Teacher to S.N. Goenka.

Assistant Teacher: Anyone who has been appointed by S.N. Goenka, or his representatives, to conduct Vipassana Meditation courses, including Teachers.

Old Student: Anyone who has completed a Vipassana Meditation course under S.N. Goenka or one of his Assistant Teachers.

Server: an Old Student who is helping on a course or at a center.

3. Responsibilities under the General Data Protection Regulation

1. Calm is a controller under the GDPR.
2. The Vipassana association is a joint controller under GDPR.

3. The local trust is responsible for the processing of personal data outside Calm, the use of Calm, proper insurances for servers and cooperation with the PCP/DPO.
4. The Data Protection Officer and his local representatives (PCP) have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for students and servers seeking clarification on any aspect of data protection compliance.
5. Compliance with data protection legislation is the responsibility of all servers who process personal information.
6. Calm's Training Policy sets out specific training and awareness requirements in relation to specific roles and to servers working with of Calm.
7. Servers are responsible for ensuring that any personal data supplied by them, and that is about them, to Calm is accurate and up-to-date.
8. Generic e-mail addresses will not be used in Calm. Passwords may not be shared. Each account is given on an individual basis.

4. Risk Assessment and audits

Objective: To ensure that Calm is aware of any risks associated with the processing of particular types of personal information Calm has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing undertaken by other organizations on behalf of Calm. Calm shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, Calm shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Where, as a result of a Data Protection Impact Assessment, it is clear that Calm is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not Calm may proceed must be escalated for review to the Data Protection Officer. The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the board of the Calm Foundation or the supervisory board of the Calm Foundation..

Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Calm's documented risk acceptance criteria and the requirements of the GDPR.

5. Data protection principles

All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and Calm's policies and procedures are designed to ensure compliance with them.

5.1 Personal data must be processed lawfully, fairly and transparently.

The GDPR introduces the requirement for transparency whereby the Vipassana association has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the student in an intelligible form using clear and plain language. The specific information that must be provided to the student must as a minimum include:

1. the identity and the contact details of the Calm Foundation if applicable or the Vipassana association and, if any, of the representative;
2. the contact details of the Data Protection Officer;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. the period for which the personal data will be stored;
5. the existence of the rights to request access, rectification, erasure or to object to processing;
6. the categories of personal data concerned;
7. the recipients or categories of recipients of the personal data;
8. where applicable, that the Vipassana association intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
9. any further information necessary to guarantee fair processing.

5.2 Personal data can only be collected for specified, explicit and legitimate purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the DPA (Autoriteit Persoonsgegevens).

5.3 Personal data must be adequate, relevant and limited

The following applies;

1. The Data Protection Officer together with the Vipassana association is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.
2. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Data Protection Officer.
3. The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.
4. If data is given or obtained that is excessive or not specifically required by Calm's or the Vipassana association documented procedures, the Data Protection Officer is responsible for ensuring that it is securely deleted or destroyed in line with the deletion policy.

5. The Privacy Contact Person is qualified to act on behalf of the DPO while informing him or her.

5.4 Personal data must be accurate and kept up to date.

The following applies;

1. Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
2. The Vipassana association and Calm are responsible for ensuring that all servers are trained in the importance of collecting accurate data and maintaining it.
3. It is also the responsibility of individuals to ensure that data held by Calm and the Vipassana association is accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate at the date of submission.
4. Servers and students should notify the Vipassana association and Calm of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained. It is the responsibility of the Vipassana association in cooperation with Calm to ensure that any notification regarding change of circumstances is noted and acted upon.
5. The Data Protection Officer is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
6. On at least an annual basis, the Data Protection Officer will review all the personal data maintained by the Vipassana association, by reference to the Data Inventory Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed.
7. The Data Protection Officer is responsible for making appropriate arrangements that, where third party organizations may have been passed inaccurate or out-of-date personal information, for information them that the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.
8. The Privacy Contact person is qualified to act on behalf of the DPO while informing him or her.

5.5 identification and purpose limitation

1. Where personal data is retained beyond the processing date, it will be minimized in order to protect the identity of the student in the event of a data breach.
2. Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.
3. The Data Protection Officer must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written (which includes e-mail).

5.6 Personal data must be processed in a manner that ensures its security

1. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.
2. Calm's compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2013. Security controls will be subject to audit and review.
3. Other means of processing than Calm applied by the Vipassana association must have appropriate safeguards and are subject to approval of the PCP and DPO. This includes tools for data, newsletters etc.

5.8 Personal data transfer outside the Union

1. The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.
2. An assessment of the adequacy by the Vipassana association taking into account the following factors the nature of the information being transferred; the country or territory of the origin, and final destination, of the information; how the information will be used and for how long; the laws and practices of the country of the transferee, including relevant codes of practice and international obligations.
3. *Binding corporate rules*: Calm will adopt approved Binding Corporate Rules for the transfer of data outside the EU and or other measures such as the Privacy Shield for transfer to the United States. The Vipassana association will apply BCR for transfer when applicable.
4. *Model contract clauses*; Calm may adopt approved model contract clauses for the transfer of data outside of the EU. If Calm adopts the model contract clauses approved by the Data Protection Authority there is an automatic recognition of adequacy. The Vipassana association will apply contract clauses were applicable for the transfer to non EU- countries.
5. *Exceptions*; In the absence of an adequacy decision, including binding corporate rules, a transfer of personal data to a third country, or an international organisation, shall take place only on one of the following conditions:
 - the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
 - the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
 - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
 - the transfer is necessary for important reasons of public interest;
 - the transfer is necessary for the establishment, exercise or defence of legal claims;

- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

A list of countries that satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union*.

5.9 Accountability

The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

Specifically, controllers such as Calm but also the Vipassana association are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Processing Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer. That means that every trust in Europe has to appoint a DPO or the Calm DPO. The Privacy Contact Person's work as deputies for the DPO. Trusts outside the Union can appoint a Privacy Contact Person.

6. Students' rights

Students have the following rights regarding data processing, and the data that is recorded about them:

1. To make subject access requests regarding the nature of information held and to whom it has been disclosed.
2. To prevent processing likely to cause damage or distress.
3. To prevent processing for purposes of direct marketing.
4. To be informed about the mechanics of automated decision-taking process that will significantly affect them.
5. Not to have significant decisions that will affect them taken solely by automated process.
6. To sue for compensation if they suffer damage by any contravention of the GDPR.
7. To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
8. To request the DPA (Autoriteit Persoonsgegevens) to assess whether any provision of the GDPR has been contravened.
9. The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
10. The right to object to any automated profiling without consent.

Students may make data access requests. The procedure also describes how Calm and the Vipassana association will ensure that its response to the data access request complies with the requirements of the Regulation.

Also students have a right to object against processing. In regard to the RSL a Special Cases Committee will review entries according to Calm's procedures. If needed the Vipassana association will direct a student to the DPO, who can contact the Special Cases Committee for the review of an entry.

Complaints

Data Subjects who wish to complain to Calm or the Vipassana association about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer.

Data subjects may also complain directly to the DPA (de Autoriteit Persoonsgegevens). Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Data Protection Officer. The right to do this should be included in the complaints procedure and be communicated with the students and servers.

7. Consent

The Vipassana association understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

The Vipassana association understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by Calm and the Vipassana association using standard consent documents e.g. when a student applies for a course or a server applies to serve. Where Calm provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit – which may be no lower than 13). The same principles apply to the use of information from children outside the Calm system by the Vipassana association.

8. Security of data

All servers are responsible for ensuring that any personal data, Calm and non Calm for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Calm to receive that information and has entered into a confidentiality agreement. Personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- stored on (removable) computer media which are encrypted and should be anonymized or pseudomized wherever possible.
- dans une pièce pouvant être verrouillée avec un accès contrôlé; et/ou
- dans un meuble de classement ou un tiroir fermé à clé; et/ou
- si informatisées, protégées par un mot de passe conforme aux exigences internes prévues dans la Politique de Contrôle d'Accès; et/ou
- conservées sur un disque dur (externe), et seront cryptées et anonymisées ou pseudonymisées autant que possible.

Care must be taken to ensure that PC screens and terminals are not visible except to authorized servers.

Physical records may not be left where they can be accessed by unauthorised personnel and may not be removed from the working place without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Physical records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Servers must be specifically authorised to process data off-site, be aware of the data breach procedure and apply it when needed.

9. Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held in Calm in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by Calm, and information obtained from third-party organisations about that person.

Students also have a right to access information about them that is held by the Vipassana association This includes files about volunteer services, dana (if applicable), newsletters, lost and found, rideshare, children- courses, complains or other non- Calm information that is stored in the trust. For the request of Calm information the PCP and DPO can be contacted.

10. Disclosure of data

The Vipassana association will ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All servers should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conducting of the courses.

The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

11. Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a server is no longer active or a student has stopped applying for courses, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. Calm's data retention and data disposal procedures will apply in all cases covered by the use of Calm. In addition the retention period for physical applications is a maximum of 10 years unless there are clear indications about possible litigation.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure.

12. Data breach procedure

The Vipassana association has integrated a data breach procedure. Any breach must be reported to the PCP / DPO consistent with the approved policy.

13. Effective Date

This Privacy Policy is effective as of 26 May 2018. The Vipassana association reserves the right to adjust and / or redraw the policy. All servers in the trust are bound by the policy. This includes the trustees, temporary servers, long term servers, AT's and visiting AT's.

14. Communication

The policy will also be communicated with students and servers applying for courses in a understandable and comprehensive manner. A copy of this policy is available to all students and servers at request and can also be found on the web page of the Vipassana association.

15 Insurances

The Vipassana association will review the insurance policy applied to servers if it properly covers the misuse of personal data. If needed policies will be adjusted.

16. Manuals

The Vipassana association will review all applicable manuals and inform the relevant committee's and teachers about changes.