The Order of Malta Volunteers – Data Protection Policy

(registered company no. 09801949, registered charity no. 1164242)

POLICY REFERENCE	
Function	For information and guidance
Status	Approved & issued
Scope	Trustees/directors, OMV Committee, Volunteers
Owner	Emily van Lier
Version	2.0
Date approved by board	January 2018
Date for review	January 2019

Introduction

1. Data Protection legislation imposes strict obligations on the Order of Malta Volunteers ("the OMV" or "the Charity") that are designed to protect the rights of individuals with regard to the safeguarding of their personal data.

2. The Secretary of the OMV Committee has been appointed as the Data Protection Manager ("the DPM") and has direct responsibility for ensuring that all these obligations have been fulfilled with the support of the Trustees.

3. A breach of this policy represents serious misconduct and may be the subject of disciplinary action.

4. This policy applies to the Directors/Trustees of the Charity and to all the Charity's volunteers. The OMV Committee must ensure that the contents of this policy are communicated to all the Charity's Volunteers. This communication must be evidenced in writing and refreshed on an annual basis.

5. The Charity is committed to complying with privacy and data protection laws, including:

   (a) the General Data Protection Regulation ("the GDPR") and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Bill 2017;
   (b) the Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including, without limitation, E-Privacy Regulation 2017/0003; and
   (c) all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office ("ICO") or any other supervisory authority (together "the Legislation").

This policy sets out what the Charity does to protect individuals' personal data.

Definitions

Authorised Locations	A place approved by the DPM for the storage of Personal Data.
Data Access Request	A formal request from a Data Subject to access Personal Data. These do not need to be in writing and there is a limited time period under law to respond to them.
Data Subject	The living individuals to whom the Personal Data relates. A data subject need not be a UK national or resident.

External Data Processors	Third party organisations or individuals that provide the OMV with data processing services. These may include: ● Data archiving/destruction ● Website hosting services ● Courier and dispatch services ● Confidential waste destruction ● Management Information Systems ("MIS") ● Any outsourcing activity
Personal Data	Any data that relate to and can, whether on their own or in conjunction with other information, specifically identify an individual living person. Personal data include, for example, names and addresses, e-mail addresses, as well as personal, health or performance records. They also include opinions about individuals as well as facts and also apply to corporate contacts. Personal data include data held electronically on a computer or network, data held in hard copy paper format and web-based data. It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Processing	This is a wide-ranging term that, in practice, covers any use of Personal Data, including: ● obtaining, recording, holding and carrying out any operation(s) on the Personal Data ● organisation or alteration of the Personal Data ● retrieval, disclosure or use of the Personal Data All such data processing activities will constitute Processing within the meaning of data protection laws.
Sanctions	Disciplinary measures.
Sensitive Personal Data	Any information about an individual's physical or mental health, racial or ethnic origin, sexual life or orientation, political views, religion, philosophical or similar beliefs, trade union membership, or genetic or biometric data.
Volunteer	Any person who attends a designated OMV activity in a voluntary capacity.

Policy

6. The OMV Secretary is responsible for the implementation and operation of this policy and performs the role of Data Protection Manager (DPM). The Trustees commit to providing the necessary training and support.

7. The DPM will regularly ensure that the OMV Committee members are aware of the Data Protection Policy and are adhering to it, and will provide training where necessary.

8. Anyone processing Personal Data must comply with the six data protection principles set out in the GDPR. We are required to comply with these principles (summarised below), and show that we comply, in respect of any Personal Data that we deal with as a data controller.

9. Personal Data must be held and processed in accordance with the Data Processing Document.

10. Personal Data must not be held longer than is necessary. Personal Data should be destroyed or erased when no longer needed. If you think that the Charity is holding out-of-date Personal Data or would like to know how long they are being held, please contact secretary@omv.org.uk

11. Personal Data must be kept accurate and up to date. All processing of Personal Data must be adequate, relevant and not excessive for the specific purposes for which the data were obtained. The most appropriate time for informing the Data Subject of the purposes of collection is at the time the Personal Data are collected.

12. Reasonable steps must be taken to ensure the accuracy and quality of Personal Data and to prevent them from becoming out of date. Periodic reviews of the information held should be completed to ensure on-going accuracy. If Personal Data are found to be out of date or inaccurate, they must be corrected as soon as is reasonably possible.

13. Any processing of Personal Data must be necessary to achieve the purpose for which they were collected. The Data Subject must not be misled or deceived with regards to the purposes or extent of the processing of their Personal Data. If Personal Data are to be processed for a new purpose that the Data Subject is not aware of, the Data Subject should be informed of this beforehand.

14. Directors, members of the OMV Committee and Volunteers must not process or store Sensitive Personal Data unless this is necessary and then only if the individual has explicitly consented. A record of that consent must be retained and be available for inspection for at least two years after the Sensitive Personal Data are no longer being processed or stored.

15. Personal Data must be stored and managed securely and all those involved must take precautions against physical loss or damage or unlawful processing. They must also ensure that both access to and disclosure of Personal Data is restricted as appropriate. In particular:

    i. When physical Personal Data are left unattended, they must be secured – for example, within locked office furniture. Personal Data in electronic form must be inaccessible when left unattended and must be password-protected.
    ii. Files containing Personal Data must not be left in open view.
    iii. Personal Data may be stored on our Cloud-based database, hosted by Zoho EU.
    iv. Personal Data stored on this database should not be downloaded onto personal devices and should be accessed via the Cloud only.
    v. Only those volunteers for whom it is necessary should be given access to Personal Data on the Cloud.
    vi. All volunteers given access to the Cloud should ensure that they select an appropriately secure password and that they do not share this with any other individual or save this on their device. The Cloud database should not be accessed on public/shared devices.
    vii. When dealing with Sensitive Personal Data, more rigorous security measures are likely to be needed. For instance, if Sensitive Personal Data (such as details of an individual's health or race) are held on a memory stick or other portable device, they should always be encrypted.
    viii. Where it is necessary to print off and transport copies of any Personal Data (for example, for safety reasons to take on an activity), these data should be transported and stored securely (for example in a locked briefcase) and should be limited to what is absolutely necessary for the purpose.

16. Personal Data must not be disclosed, either orally or in writing or otherwise, to an unauthorised third party without a clear "need to know" reason being identified prior to disclosure and in accordance with the privacy notice provided to the Data Subject on our website. Personal Data must always be transferred in a secure manner. The degree of security required will depend on the nature of the data. The more sensitive and confidential the data, the more stringent the security measures should be.

17. The GDPR requires that when organisations transfer Personal Data outside the EEA they take steps to ensure that the data are properly protected. The Charity may transfer personal data outside the EEA when individuals participate in an Order of Malta International activity hosted by a country outside the EEA, such as the annual Holiday Camp.

18. A Data Subject must be given notice of the purposes for which their Personal Data are being processed. Personal Data must only be processed for these purposes. To comply with this principle, the Charity should provide a Data Subject with the privacy statement every time it receives Personal Data from an individual. This includes telling them:

    i. the type of information the Charity will be collecting (categories of Personal Data concerned);
    ii. who will be holding their information (i.e. the OMV, including contact details and the contact details of the Data Protection Manager);
    iii. why the Charity is collecting their information and what it intends to do with it (for instance, to process donations or send them mailing updates about activities);
    iv. the legal basis for collecting their information (for example, whether the Charity is relying on their consent, or on legitimate interests or on another legal basis);
    v. if the Charity is relying on legitimate interests as a basis for processing, what those legitimate interests are;
    vi. whether the provision of their Personal Data is part of a statutory or contractual obligation and details of the consequences of the Data Subject not providing those data;
    vii. the period for which their Personal Data will be stored or, if that is not possible, the criteria that will be used to decide that period;
    viii. details of the people or organisations with whom the Charity will be sharing their Personal Data;
    ix. if relevant, the fact that the Charity will be transferring their Personal Data outside the EEA and details of relevant safeguards; and
    x. the existence of any automated decision-making, including profiling, in relation to the Personal Data.

19. Where the Charity obtains Personal Data about a person from a source other than the person himself/herself, the Charity must provide that individual with the following information in addition to that listed under paragraph 18 above:
    (a) the categories of Personal Data that the Charity holds; and
    (b) the source of the Personal Data and whether this is a public source.

20. In addition, in both scenarios (where Personal Data are obtained both directly and indirectly) the Charity must also inform individuals of their rights outlined below, including the right to lodge a complaint with the ICO and the right to withdraw consent to the processing of their Personal Data.

21. This privacy statement may be provided in a number of places including on web pages, in mailings or on application forms. The Charity must ensure that the privacy statement is concise, transparent, intelligible and easily accessible.

22. Data Subjects have the right, subject to certain exceptions and procedural requirements, to access Personal Data that are being processed about them, to be informed of uses made of the information, details of any transfers and how long the Personal Data will be stored, through the means of a Data Access Request. The Board of Trustees of the Charity is required by law to respond to such a request within 30 days, either by providing the data or explaining why it is subject to a relevant exemption. The Charity cannot charge a fee for providing this information.

23. Any Director/Trustee, member of the OMV Committee or Volunteer receiving a Data Access Request must immediately forward it to the DPM. Under no circumstances should

anyone respond directly to a Data Access Request unless they are specifically requested to do so by the DPM.

24. A Data Access Request may be received in any number of forms, including a telephone call, email or letter. In the case of a telephone call, the Data Subject should be asked to submit the Data Access Request in writing to the DPM. The DPM should be notified of the request and of your response.

25. Data Subjects have the right to require the Board of Trustees of the Charity to correct any inaccurate data held about them. The Board of Trustees is usually legally required to respond to such a request within 30 days of receiving it; but this should be done as soon as reasonably practicable. Any requests to correct inaccuracies must be forwarded immediately to the DPM. The Board of Trustees has a legal obligation to comply with such requests, provided that the Data Subject has been satisfactorily identified. The person receiving the request should take reasonable steps to identify the Data Subject before forwarding the request to the DPM.

26. Data Subjects' rights must be observed. The Directors/Trustees, members of the OMV Committee and Volunteers must take all reasonable steps to ensure that they are aware of and respect these rights. These include the right:

    i. to be told, where any information is not collected from the person directly, any available information as to the source of the information;
    ii. to be told of the existence of automated decision-making;
    iii. to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;
    iv. to have all Personal Data erased (the right to be forgotten) unless certain limited conditions apply;
    v. to restrict processing where the individual has objected to the processing;
    vi. to have inaccurate data amended or destroyed; and
    vii. to prevent processing that is likely to cause substantial damage or distress to Data Subject or to anyone else.

27. No Director/Trustee, member of the OMV Committee or Volunteer is authorised to deal with an External Data Processor without the approval of the DPM, who must ensure that they adopt appropriate technical and organisational security measures to safeguard Personal Data and that these measures are managed appropriately.

28. Accessing, deleting or otherwise using any information that is not part of the duties of a Director/Trustee, member of the OMV Committee or Volunteer or doing so without prior authority is a serious disciplinary offence.

Contacting supporters

29. The Charity should ensure that it complies with all relevant legislation, and particularly the Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, when contacting supporters for the purposes of direct marketing. Direct marketing has a wide definition and will include any communications that promote the aims or ideals of the Charity, including fundraising materials and invitations to events.

30. When sending marketing materials, the Charity should remember that people have the right to ask the Charity to stop processing their Personal Data for direct marketing purposes. The Charity should record all such requests on a "suppression list" and refrain from contacting those people. The Charity must comply with requests within a reasonable time and should comply with most requests within 28 days.

31. The Charity should never send marketing materials to an individual or organisation who has told the Charity via registration with the Mailing Preference Service ("MPS") that they do not want mailings unless that individual or organization has consented to the Charity sending such mailings, for example by ticking an opt-in box agreeing to receive the Charity's marketing materials or by providing their address knowing that it would be used for marketing purposes.

32. When individuals' Personal Data are added to the Charity's fundraising and associated databases, the Charity will ensure that such individuals are notified of who the Charity is, what the Charity will use their information for and anything else necessary to make sure the Charity is using their information fairly. The Fundraising Regulator's Code of Fundraising Practice also requires an opt-out statement to be placed on every fundraising communication. This statement must be the same size of the donation amount or, if none, a minimum font size 10.

33. The Charity must have consent before making any kind of approach by email or SMS/text.

34. Any such emails/SMS/texts should provide clear instructions for unsubscribing from future emails/SMS/texts of that kind (for example, by providing an unsubscribe link or an email address to which to reply).

35. These principles apply to unsolicited direct marketing by fax, email and SMS/text message, as well as by automated telephone messages.

36. The Charity should never make marketing telephone calls to an individual or organisation who has told the Charity they do not want to receive calls from the Charity or that they do not want to receive calls to any number registered with the Telephone Preference Service ("TPS") or the Corporate Telephone Preference Service ("CTPS") unless they have consented to the Charity making such calls (for example, by ticking an opt-in box agreeing to the Charity's marketing calls or by providing their telephone number in the knowledge that it would be used for marketing purposes).

37. Individuals can give consent to receiving unsolicited calls which overrides TPS registration. Particular care needs to be taken in the case of calling numbers obtained from a third party list, in order to ensure that the individual has consented to calls specifically from the Charity. If there is any doubt about the validity of such consent, the numbers should be screened against the TPS list before calling. Mobile numbers can also be registered on the TPS and so must also be screened where necessary.

38. The new Fundraising Preference Service ("FPS") has now been launched. More detail can currently be found here (https://www.fundraisingregulator.org.uk/support-advice-for-donors/the-fundraising-preference-service/). The Charity will comply with the FPS by ensuring that any notifications received informing the Charity that a supporter has opted out of marketing communications from the Charity will be acted upon. be suppressed

39. All communications must include information on how to contact the Charity.

Disputes

40. Anyone who has a concern or complaint regarding the application of this policy should contact the DPM in the first instance. In the event that the DPM cannot address the concern, the concern or complaint should be referred to the Chairman of the Board of Trustees of the Charity. This does not impact or override any legal remedies available.

41. Data Subjects have the right to make a complaint to the ICO. The Charity must inform Data Subjects of this right as set out elsewhere in this policy.

Notification

42. Although there is no obligation for the Charity to make an annual notification to the ICO under the GDPR, the Charity should consult the ICO where necessary when it is carrying out "high risk" processing.

43. The Charity should report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary within 72 hours. The Charity should also prepare a serious incident report and send it to the Charity Commission in the event of a breach. The Charity should also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of individuals.

Record keeping

44. The Charity must keep a record of its data processing activities to demonstrate that the it is complying with this policy. These records will include: the purpose of processing; descriptions of categories of Data Subjects and categories of Personal Data; details of transfers to third countries; and retention periods of Personal Data.

45. Please contact secretary@omv.org.uk for further information about what must be retained and for how long.

Review

46. The policy owner must keep up to date with relevant legislation and government guidance and update this policy whenever necessary. The Board of Trustees of the Charity must approve the revised version.

47. The policy owner must review the policy at the end of December each year and either submit a revised policy for board approval or confirm in writing to the Chairman of the Board of Trustees that the current version of this policy is still fit for purpose.

48. The Board of Trustees must formally review and re-approve this policy at least annually.