UNIFIED DATA PROTECTION POLICY

POLICY REFERENCE	
Function	For information and guidance
Status	Approved & issued
Scope	Trustees, Employees, Members, Companions, Volunteers
Owner	Chancellor
Version	1.0
Date initially approved by board	12/3/25
Date of last board review	
Date of next board review	March 2030

1. Scope

The Association of British Members of the Sovereign Military Hospitaller Order of Malta, registered charity number 1103567, registered address at 13 Deodar Road, London SW15 2NP and the Grand Priory of England and the Grand Priory of the Blessed Adrian Fortescue of the Order of Malta Trust, registered charity number 1166645, registered address 67 Castletown Rd, London W14 9HG, are committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data, as well as safeguarding the rights and freedoms of persons whose information BASMOM and the GPE may process pursuant to the UK General Data Protection Regulation 2020 (UK GDPR), the Data Protection Act 2018 (DPA) and any other applicable legislation. In this document, all such legislation is collectively referred to as 'data protection legislation'.

This policy applies to all Members, employees and volunteers of the organisations, and any other persons that are authorised to access the data for which the organisations are the controller.

This policy should be read in conjunction with the following BASMOM and GPE policies:

- Safeguarding policy
- Data Breach Policy

2. Definitions used in this policy

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

Data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Data Protection Lead/accountable person: is the member of the organisation's staff who oversees data protection obligations and procedures

Data subject: refers to any living person who is the subject of personal data (see below for the definition of 'personal data') held by the organisation. A data subject must be identifiable by name, ID, address, online identifiers or other factors such as physical, physiological, genetic, mental, economic or social factors

Information Commissioner's Office (ICO)*:* the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

Personal data: means any information that identifies, directly or indirectly, a data subject

Processing: refers to any action taken in relation to personal data including, but not limited to, collection, adaptation, alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise

Special categories of data: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, biometric data (where used for identification purposes),
data concerning health, data concerning a person's sex life or sexual orientation

1. The appointment of a Data Protection Lead

The organisations have appointed the internal position of the Vice Chancellor as the Data Protection Lead.

2. The seven principles of data protection

BASMOM and the GPE are committed to adhere to Article 5 of the UK GDPR which lists the seven principles of data protection:

- **Lawfulness, fairness and transparency:** the organisation is committed to process data lawfully, fairly and in a transparent manner
- **Purpose limitation**: the organisation collects personal data for specified, explicit and legitimate purposes. The organisation doesn't further process data in a manner that is incompatible with those purposes
- **Data minimisation:** the organisation is committed to process data that is adequate, relevant and limited to what is necessary
- **Accuracy:** personal data is kept accurate and up to date
- **Storage limitation:** the organisation is committed to keeping personal data for no longer than necessary
- **Integrity and confidentiality**: the organisation processes data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage

- **Accountability**: the organisation is able to demonstrate compliance

3. IT Policy and security measures

There are several IT measures that BASMOM and the GPE put in place to help ensure the security of its data, including (but not limited to):

- Providing staff with email guidance and training, ensuring they are aware of when to use BCC function (e.g. when sending emails to more than one service user)
- Using strong passwords
- Using multi-factor authentication where possible
- Regularly updating software
- Using secure wi-fi and avoiding the use of unsecure public wi-fi

For more information on security measures and IT provisions, please refer to the organisations' IT policy.

1. Physical security

There are also several physical security measures that BASMOM and the GPE put in place, including (but not limited to):

- clear desk policy to avoid people leaving confidential data on their desk
- locked filing cabinets, drawers or lockers for confidential paperwork
- automatic screen shut down when staff members are away from their desk
- arrangements for shredding paper
- shredding and disposing of manual records which have passed their retention as 'confidential waste'

4. Confidentiality

BASMOM and the GPE operate under a policy of confidentiality. BASMOM and the GPE are committed to providing confidential services to their stakeholders and ensuring that all personal data about guests, volunteers, staff, Members, trustees and other stakeholders is treated as confidential and is collected, processed and retained in line with the data protection law. In certain situations, information may need to be shared with third parties, for example to protect the welfare and safety of any young people that are part of the service delivery.

5. Accountability - demonstrating Compliance

In accordance with law requirements, the organisations keep records so that they can demonstrate the steps taken to comply with the GDPR:

- **Record of Processing Activities (ROPA) spreadsheet** identifies information such as the category of personal data processed for each data subject, the lawful basis of the processing, data retention, data storage, who is responsible for the data and who has access to the data
- **The Activity, Incident and Risk reporting spreadsheet** keeps a log of key information such as discussions and decisions about data protection, identified risks, any personal data breaches and response, training of staff and volunteers, requests to exercise any rights by data subjects and management of those requests, notifications to the ICO
- **Legitimate Interests' Assessments** (LIA) that have been carried out

- **Data Protection Impact Assessments** (DPIA) that have been carried out to justify the approach where processing poses particular risks (such as processing of special category of data)
- **Data Protection Policy** which includes most procedures relating to data protection
- **Privacy Notice** for data subjects
- **Data Processing Agreements** with databases, CRM and cloud providers and other data processors
- **Data Sharing Agreements** (also called information sharing protocol) with other data controllers or joint controllers
- **Appropriate Policy Document** which must be completed in some circumstances outlined by the DPA (2018) when processing special category of data or criminal records

6. The six lawful bases for processing personal data (including special category of data)

BASMOM and the GPE process personal data by identifying a 'lawful basis' chosen from the six possibilities set out in Article 6 of the UK GDPR:

- with the consent of the data subject
- for a contract involving the data subject
- to meet a legal obligation
- to protect any personal vital interests
- for government and judicial functions
- in the organisation's legitimate interests provided the data subject's interests are respected

The most common lawful bases that the organisations identify are consent, contract, legal obligation and legitimate interest. The lawful bases for the different processing activities are recorded in the Record of Processing Activities (ROPA) spreadsheet which is maintained and reviewed annually.

When data processing poses particular risks, such as the processing of special category data, the organisations will complete a Data Protection Impact Assessment (DPIA) to justify their data protection approach.

When processing special category data or criminal records without the consent of the data subject, data protection law requires controllers to identify another lawful basis under Article 6 of the UK GDPR other than consent, supported by one of the exemptions of Article 9 (2) which might need to be further supported by the DPA 2018. When processing criminal records, the lawful basis identified in Article 6 needs to be additionally supported by the DPA (2018).

The organisations may complete an Appropriate Policy document for the processing of special category data and criminal data without consent of the data subjects as required by law.

7. Data subjects and data specifications

The organisations collect personal information from different groups of data subjects:

- Members
- Companions
- Volunteers
- Guests
- Employees

- Donors
- Job applicants

Our privacy notice and ROPA explain the different kinds of data we collect and the lawful basis for processing them. We process normal category data and we may also collect special category data and criminal data.

Criminal record is not formally special category data, however under the Data Protection Act 2018, criminal record data receives the same additional protection as special category data.

8. Additional compliance obligations

BASMOM and the GPE are committed to comply with additional obligations in reference to the UK GDPR and the Data Protection Act 2018. These include:

- Breach notification
- Data subject's rights
- Risk assessment
- By design and by default

Breach notification procedures
Article 4.12 of the UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, authorisation, and authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

In case of a data breach please refer to the Breach Management Policy.

2. Data subjects' rights

BASMOM and the GPE are fully aware of the data subject rights described in Articles 15 - 22 of the UK GDPR, and these are listed in the privacy notice.
The data subjects' rights include:

1. The right to be informed
2. The right of access
3. The right of rectification
4. The right to be forgotten (erasure)
5. The right to restrict processing
6. The right to data portability
7. The right to object processing
8. Rights in relation to automated decision making and profiling

Additional rights of data subjects include:

- The right not to receive direct marketing
- The right to claim damages should they suffer any loss as a result of a breach
- The right to complain and the right to request that the ICO carry out an assessment

If data subjects wish to exercise any rights, they can contact the organisation at: dataprotection@orderofmalta.org.uk They are reminded of their rights and how to exercise them in the

privacy notice they receive. All activity organisers and employees are trained to recognise an incoming request to exercise any right, to understand when the right applies and to pass it on without delay to the designated person.

All requests from data subjects to exercise any rights are recorded in the 'Activity, Incident and Risk reporting spreadsheet'.

Under certain circumstances, mostly described in Schedules 2-4 of the DPA (2018), the organisation may not need to comply with the request by a data subject to exercise one of their rights. Those circumstances will be assessed on a case-by-case basis.

1. The right to be informed

Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. The organisation is committed to comply with this right and they do so via the privacy notice.

2. The right of access and SAR procedure

A data subject has the right to make access requests in respect of personal data that is held and disclosed. To understand how we deal with Subject Access Requests, please view our SAR section on our data protection policy.

3. The right of rectification

BASMOM and the GPE are aware of the provisions in Article 16 of the UK GDPR - if the data subject becomes aware that the organisation is holding incorrect information about them, they have the right for it to be corrected, and if their information is incomplete, they can also submit additional information to be added.

4. The right to be forgotten (erasure)

If a data subject asks the organisation to delete their information, as stated in Article 17 the organisation will do so without undue delay when:

a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
b) the data subject withdraws consent (if that is the basis on which the processing is taking place), and where there is no other legal ground for the processing
c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing
d) the personal data has been unlawfully processed
e) the personal data has to be erased for compliance with a legal obligation
f) the personal data has been collected in relation to the offer of online services to a child

In addition, if the organisation has made the information public, the organisation must try to have it erased in other locations as well. In conjunction with Article 19 of the UK GDPR, the organisation informs anyone to whom data has been disclosed, unless this 'proves impossible or involves disproportionate effort'. The organisation will also inform the data subject which recipients their data has been disclosed to, if they ask.

There are exceptions to the 'right to be forgotten' for reasons relating to freedom of expression, public health, archiving, research and statistics, legal claims and legal obligation.

There may also be circumstances where the organisation has no choice but to retain data, for example to mark a record for suppression to ensure that no direct marketing is sent to that individual in the future.

The organisation will process a request for erasure without undue delay, and within one month of receipt. The organisation gives particular weight to any request of erasure if the request relates to data collected from children.

5. The right to restrict processing

The data subject shall have the right to restrict processing of their personal data where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data
- the processing is unlawful, and the data subject opposes the erasure of the personal data, requesting the restriction of its use instead
- the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject

6. The right to data portability

This right applies when processing is based on consent or a contract between the organisation and the data subject, and the process and the processing is taking place 'by automated means'. It allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

Data subjects are entitled to receive from the organisation a copy of any personal data they have provided in a 'structured, commonly used and machine-readable format', so that they can provide the data to a different controller.

7. The right to object processing

Data subjects can object to any processing of their data that organisation is carrying out on the lawful basis of legitimate interests. The organisation will stop processing if not able to demonstrate 'compelling legitimate grounds'.

8. Rights in relation to automated decision making and profiling

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. Profiling refers to any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data subject's employment performance, economic status, whereabouts, health, personal preferences and behaviour.

The data subject has the right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling. The data subject has the right not to have

decisions made about them solely by automated processing if this has a significant effect on them, unless the decision is necessary in conjunction with a contract between the data subject and the controller, or the data subject has provided explicit consent.

BASMOM and the GPE do not currently undertake automated decision making.

9. The right not to receive direct marketing

Every data subject has the right not to receive direct marketing if that is their choice.

10. The right to claim damages in case of data breach

If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation.

11. The right to complain

If data subjects wish to make a complaint or share concerns, they are encouraged to liaise directly with the organisation. They can make a complaint or send an email to: dataprotection@orderofmalta.org.uk who will respond within 5 working days and lead on the resolution of the complaint within 28 days.

As stated in the privacy notice, we inform the data subject that they can also make a complaint to the ICO and request that the ICO carry out an assessment as to whether any of the provisions of the UK GDPR have been breached. Data subjects can remain anonymous if they wish.

3. Risk Assessment

Risk Assessment is an important part of the accountability of an organisation. It is vital that the organisation is aware of all risks associated with personal data processing and it is via its risk assessment process that the organisation is able to assess the level of risk.

It is the policy of the organisation not to transfer or share data into an environment that is not considered compliant with UK or EU data protection law

Where personal data processing is carried out using new technologies, or when a high risk is identified in relation to the rights and freedoms of natural persons, the organisation is required to engage in a risk assessment of the potential impact, also known as a 'Data Protection Impact Assessment' (DPIA). More than one risk may be addressed in a single DPIA. The organisation has developed and agreed upon a procedure for completing a DPIA. This procedure is always followed where there is a need to measure risk. The procedure is completed by the Data Protection Lead and, if necessary, the opinion of a professional Data Protection Practitioner is taken into account.

In addition to this, and if the outcome of a DPIA points to a higher risk than the organisation intended and personal data processing could result in distress and/or may cause 'damage' to the data subjects, it is for the Data Protection Lead to decide whether the organisation ought to proceed, and the matter should be escalated. In turn, the accountable person may escalate the matter to the regulatory authority (prior agreement) if significant concerns have been identified.

4. By design and by default

The goal of this principle would mean that in the organisation, everyone who starts a new project or sets up a system or process must ensure that they incorporate data protection as a matter of course, consulting the Data Protection Lead. Consideration of the data protection implications should be a standard check point before any project or system is signed off.

9. Protection of children

The UK GDPR does not treat children particularly differently from adults, but the organisation is committed to take appropriate precautions, in particular:

- When you are considering 'legitimate interests' as lawful basis, the organisation will be particularly careful not to override the interests of the data subject
- When providing information to children about how their data will be processed, the organisation ensures that they will genuinely be able to understand it
- Requests to exercise data subject's right will have a particular weight when involving data around children

10. Dealing with Subject Access Requests

Under Article 15 of the UK GDPR – right of access, a Data Subject Access Request (DSAR or SAR) allows individuals to confirm the accuracy of personal data, check the legality of processing to allow them to exercise rights of correction or objection if necessary, and also request to see any personal data that we hold about them.

***Recognising a Subject Access Request*:** SARs can be made verbally or in writing, including by social media. Data subjects can make their request to any part of your organisation, they do not have to direct it to a specific person or contact point. A request does not have to include the phrases 'subject access request', 'right of access' or 'Article 15 of the UK GDPR'. Third-parties may submit SARs on behalf of individuals, but they must have clear permission from the data subject e.g. written permission or a power of attorney document. If there is no evidence that a third-party is authorised to act on behalf of an individual, you are not required to comply with the SAR, however you should still respond to them explaining this.

***Informing the Data Protection Lead*:** Members of staff etc. should inform BASMOM and the GPE's Data Protection Lead on dataprotection@orderofmalta.org.uk **as soon as possible** if they receive a data subject access request. The Data Protection Lead is the person responsible to deal with and respond to SARs.
Time frame: The organisations have **one month** to respond to an SAR. You must acknowledge the receipt of a data subject request and confirm that the organisation is looking into the request and will respond within the statutory timeframe.
Refusing an SAR/exemptions: the organisations may refuse to provide the information to the data subject if an exemption applies. A SAR may also be refused if the request is manifestly unfounded or excessive. It must take into account the circumstances of the request, including: the nature of the requested information and the context of the request.

Please refer to the ICO guidance on exemptions here. Each request should be assessed individually, and if refused, the individual must be informed of the reasons, their right to complain to the ICO, and their

option to seek a judicial remedy. If only part of the request is exempt, a response will be provided with redactions, along with information on their right to complain or pursue legal action.

***Processing and Extensions**:* The organisation will provide their response on the equivalent date in the following month, or earlier if the month is shorter and there's no equivalent. Any delays caused by the data subject may be added to the month. There may be some circumstances where the organisations can take longer than one month to fulfil the request, up to a **maximum two further months** where the request is complex, or if the organisations receive a high number of requests from the same individual e.g. other types of requests relating to individuals' rights.

If the organisations need to extend the response deadline, they must inform the data subject of any such extension within one month of receipt of the request

***Identify relevant personal data and perform redactions*:** identify the data that has been requested in the SAR and gather it. As a general rule, personal data relating to other individuals should not be disclosed unless their permission has been obtained to release it, or it is reasonable to comply without consent. Therefore, if this is within the requested information, it is advisable to generally redact such information. The organisation will pay particular attention to not affect the rights or freedoms of others, including trade secrets or intellectual properties such as copyright. Please refer to: ICO guidance on redactions.

Providing the data to the data subject: the organisation will provide a copy of the personal data held on the data subject, but it might not be provided in the format or document in which it is held. The response should include:

a) Confirmation that personal data about them is being processed.
b) A copy of that personal data.
c) Details of the purpose of the processing.
d) Categories of the personal data concerned e.g. does it include any special categories or sensitive personal information?
e) The period the personal information will be stored for, or what the criteria is for determining the period of storage.

Communication and Costs for Data Subject Requests: Communication with data subjects must be clear, concise, and accessible, and can be provided in writing, electronically, or orally with identity verification. The organisation will not charge for the first copy of personal data but may charge a reasonable fee for additional copies or if the request is excessive or unfounded. The organisation may charge a fee for requests that are excessive, unfounded, or repetitive, demonstrating the request's nature and considering administrative costs.

Recording responses: Data Subject Access Requests must be tracked and recorded by BASMOM and the GPE for accountability purposes.

11. Registration with the ICO and fees

The organisations have registered with the Information Commissioner as they engage in the processing of personal information identifying data subjects directly or indirectly.

The organisations pay an annual fee to the ICO, as required by law.

12. Data sharing - working with other organisations

As with any other organisation, BASMOM and the GPE may collaborate with:

- data processors
- joint controllers
- separate controllers

All third parties we work with who have or may have access to personal data of our data subjects will either comply with this policy, or we will ensure that their data protection policy aligns with this policy.

13. International Data Transfer

Where personal data is stored outside of the UK and the EU, safeguards to protect personal data may include, but are not limited to, the UK Addendum used in conjunction with the EU Standard Contractual Clauses (SCCs), or UK International Data Transfer Agreement (IDTAs). Such safeguards will be subject to Transfer Risk Assessments (TRAs).

14. Cookie Policy

Please view the cookie policy on our website to understand the different cookies we use on our website.

15. Changes to this policy

This Policy is updated by the Data Protection Lead when required. It is reviewed annually by the Data Protection Lead and the board of trustees will review at least every five years.