International Symposium on Military Operational Research (ISMOR)

Data Protection Policy

Document History

Version	Date	Description	Completed by
DRAFT 0.1	12/12/17	Initial draft	J Rawle
DRAFT 0.2	08/01/18	Second draft incorporating comments from S Shepherd	J Rawle
Version 1	15/01/18	Initial version incorporating comments from P Starkey	J Rawle

Context

The International Symposium on Military Operational Research (ISMOR) is an annual residential event, currently held at Royal Holloway University of London (RHUL). ISMOR provides a forum for military OR specialists in government, industry and academia to publicise their work, network and share best practice at an unclassified level.

ISMOR is self-funding and is financially managed by The ISMOR Foundation Ltd., a non-profit making company formed for this specific purpose.

The management and delivery of ISMOR is achieved by a volunteer organising committee, headed by the ISMOR Chair, working in cooperation with RHUL.

RHUL is an experienced venue and conference provider contracted to provide conference booking and administration services prior to the event, and administrative support throughout the event.

The ISMOR Foundation Ltd needs to gather and use certain information about individuals including potential and actual symposium delegates, suppliers, employees, volunteers and other people ISMOR has a relationship with or may need to contact.

This policy describes how this personal data will be collected, handled, and stored to meet the company's data protection standards and comply with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Data Protection

The Data Protection Act 1998 (the Act) has two principal purposes:

- to regulate the use by those (known as data controllers) who obtain, hold and process personal data on living individuals; and
- to provide certain rights (for example, of accessing personal information) to those living individuals (known as data subjects) whose data is held.

The cornerstones of the Act are the eight data protection principles, which prescribe:

- guidelines on the information life-cycle (creation/acquisition; holding; processing; querying, amending, editing; disclosure or transfer to third parties; and destruction ('the life-cycle');

- the purpose for which data are gathered and held; and
- enshrined rights for data subjects.

The Act applies to the company, the Data Controller for the purposes of the Act, and to anyone who holds personal information in a structured way so that retrieval is easy. The company is fully committed to abiding, not only by the letter, but also by the spirit of the Act, and, in particular, is committed to the observation, wherever possible, of the highest standard of conduct mandated by the Act. This policy has been written to acquaint employees and volunteers with their duties under the Act and to set out the standards expected by the Company in relation to processing of personal data and safeguarding individuals' rights and freedoms.

Personal data means data which relate to a living individual who can be identified from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Training and Awareness:

- the policy will be brought to the attention of new employees and volunteers; and
- briefing of changes and any additional training requirements will be given when required.

Responsibilities

The Data Protection Officer is responsible for the maintenance and implementation of this policy. The Data Protection Officer undertakes the duties of the Data Controller.

All employees and volunteers are expected to:

- read, understand and abide by this policy document;
- understand how to conform to the standard expected at any stage in the life-cycle;
- understand how to conform to the standard expected in relation to safeguarding data subjects' rights (e.g. the right to inspect personal data) under the Act;
- understand what is meant by 'sensitive personal data', and know how to handle such data;
- contact the Data Protection Officer if in any doubt, and not to jeopardise individuals' rights or risk a contravention of the Act.

The Data Protection Principles

The Data Protection Principles, in summary, are:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised unlawful processing of personal data and against accidental loss or destruction of, damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Life Cycle Process

Step	Principles	Process
Acquisition of personal data	1, 2, 3	Those wishing to obtain personal data must comply with guidelines issued from time to time by the Data Protection Officer and, in particular, should tell data subjects the purpose(s) for which they are gathering the data, obtain their explicit consent, and inform them that the Company will be the data controller for the purposes of the Act and the identities of any other persons to whom the data may be disclosed. If sensitive personal data are being collected, explicit consent is not only best practice, it is mandatory. No more data should be collected than is necessary for the purpose(s) declared.
Holding / safeguarding / disposal of personal data	4, 5, 7	Data should not be held for longer than is necessary. Personal data should be reviewed periodically to check that it is accurate and up to date and to determine whether retention is still necessary. Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures that need to be taken.
Processing of personal data	1, 2	In this particular context, 'processing' is used in the narrow sense of editing, amending or querying data. In the context of the Act as a whole, 'processing' is very widely defined to include acquisition, passive holding, disclosure and deletion. Personal data must not be processed except for the purpose(s) for which it was obtained or for a similar, analogous purpose. If the new purpose is very different, the data subjects consent must be obtained.
Disclosures and transfers	1, 2, 7, 8	**Disclosures**. The Company's policy is to exercise its discretion under the Act to protect the confidentiality of those whose personal data it holds. i. Employees of, and volunteers working on behalf of, the Company may not disclose any information about symposium delegates, suppliers or other employees or volunteers, including information as to whether or not any person is or has been an employee of the company unless they are clear that they have been given authority by the company to do so. Particular care should be taken in relation to any posting of personal information on the Internet. ii. No employee of the company may provide references to prospective employers or others without the consent of the individual concerned. It is therefore essential that where the

		Company is given as a referee, the subject of the reference should provide the Company with the necessary notification and consent. iii. No employee may disclose personal data to the police or any other public authority unless that disclosure has been authorised by the Company's Data Protection Officer. **Transfers**. Personal data should not be transferred outside the Company, and in particular not to a country outside the European Economic Area. i. except with the data subject's consent; or ii. unless that country's data protection laws provide an adequate level of protection; or iii. adequate safeguards have been put in place in consultation with the Data Protection officer; or iv. in consultation with the Data Protection Officer, it is established that other derogations apply.
Destruction of personal data	5, 7	Personal data must not be held for longer than necessary; and when such data has been earmarked for destruction, appropriate measures must be taken to ensure that the data cannot be reconstructed and processed by third parties.

Data Subjects' Rights of Access

The Company is fully committed to facilitating access by data subjects ('applicants') to their personal data, while bearing in mind the need to protect other individual's rights of privacy. All applicants will be expected to fill in a Subject Access request form, available from the Data Controller. A template Data Subjects Access Request is attached under Annex A.

Review

This policy will be updated by the Data Protection Officer to take account of changes in the law and guidance issued by the Information Commissioner. Review of the Policy will be undertaken by the Board of Directors on its annual compliance review.

Data Protection Contacts

For general enquiries about the Company's Data Protection Policy and for formal subject access requests under the Act:

Data Protection Officer and Data Controller: Peter Starkey, Managing Director

Disciplinary Consequences of this Policy

Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA in contravention of paragraph 4.4.2 above) or any other breach of Section 55 of the data Protection Act 1998 by employees will be treated seriously by the company and may lead to disciplinary action up to and including dismissal.

Complaint Handling

Complaints will be handled in accordance with the procedures the Data Protection Act 1998.

Annex A DATA SUBJECTS ACCESS REQUEST TEMPLATE

The Data Protection Officer
The ISMOR Foundation Ltd
Grove House
Lutyens Close
Chineham Court
Basingstoke
RG24 8AG

[Your full address]
[Phone number]
[The date]

Dear Sir or Madam

Subject access request

[Your full name and address and any other details to help identify you and the information you want.]

Please supply the information about me I am entitled to under the Data Protection Act 1998 relating to: [give specific details of the information you want, for example

- the contact details we hold for you;
- emails between you and us (between 1/6/17 and 1/9/17)]

If you need any more information from me, or a fee, please let me know as soon as possible.

It may be helpful for you to know that a request for information under the Data Protection Act 1998 should be responded to within 40 days.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer.

If you need advice on dealing with this request, the Information Commissioner's Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk.

Yours faithfully

[Signature]