Data Protection Policy

Issued by: avv. Luca Malatesta (Emso Eric Data Protection Officer)	***Issue date: 2019/05/25***
Reviewed by:	**next review date: 2020/05/25**
Approval by:	**Approval date:**

1. General Policy Statement

1.1 The European Multidisciplinary Seafloor and water column Observatory (EMSO) is committed to the protection of individuals' rights and privacy. The processing of personal data such as the collection, recording, use, and storage of personal information must be dealt with lawfully and correctly in accordance with this policy. All information containing personal data must be protected against unauthorised access, accidental loss or destruction, modification or disclosure.

1.2 The EMSO regards the lawful and correct treatment of personal data as important to its successful operation, and to maintain confidence with our staff and other stakeholders.

2. Purpose and Scope

2.1 The EMSO needs to process certain personal data in order to carry out its functions. These data relate to:

- Staff in relation to their contract of employment;
- Prospective applicants to process applications and ensure they are properly informed of the working opportunities
- Visitors to the EMSO including those coming to EMSO events
- Contractors
- Other third parties with whom it has dealings.

2.2 The EMSO needs to collect, store, use, transfer and dispose of this data in order to fulfil its purpose.

In this regard, such policy has been drawn up to ensure that all data is processed in accordance to the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Italian legislative decree no.101/2018, which together form the Data Protection Legislation. This Policy sets out what the EMSO is required to do to ensure correct and lawful processing of personal data, to ensure that all staff, contractors and other workers who process personal data on behalf of the EMSO are doing so in accordance with the Data Protection principles.

2.3 The Policy applies to all staff, governors, suppliers, contractors and others with whom the EMSO has dealings.

3. Relationships with other policies, procedure and guidance

3.1 This policy should be read in conjunction with the:

- Records Management Policy and the EMSO's Records Retention Schedule;
- The Information Security Policy;
- E-mail Etiquette Guide
- Breaches Reporting Procedure
- Staff Guidance on Data Protection
- Code of Practice on Research Ethics

4. Definitions

Data Protection Legislation
"Data Protection Legislation" refers to both the REGULATION (EU) 2016/679 and Italian legislative decree no.101/2018.

Personal Data
"Personal Data" means 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Special Category Data
"Special Category data" consists of personal data relating to:
- ethnic origin
- physical and mental health (including, for example, details of the reasons for an individual's sick leave)
- sex life
- genetics
- biometrics (where used for ID purposes)
- religion or belief
- political opinion
- Trade Union membership

Greater protections are required when processing this data.

Processing
"Processing" means obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data.

Data Subject
"Data subject" means an individual who is the subject of the personal data.

Data Controller
"Data controller" means a person who or organisations which (either alone or jointly or in common with other persons/organisations) determines the purposes for which, and the manner in which, any personal data is processed. In this case, this means the EMSO or nominated individuals acting on behalf of and with the authority of the EMSO.

Data Processor
"Data Processor" means any person (other than a member of staff) or organisation who processes data on behalf of the EMSO.

Data Protection Impact Assessment
"Data Protection Impact Assessment" means a formal assessment of the impact of processing on the individual including the risks and any impact on their rights and freedoms.

Breach
A "breach" is any incident, or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data.

Privacy statement
A "privacy statement" is a document informing the data subject of the legal basis, purposes of processing etc.

Information Commissioner
The Information Commissioner oversees the implementation of Data Protection Legislation.

Staff
Unless otherwise applicable, all references to staff include all current, past and prospective staff, full time, part time staff and Members of the Board of Governors as well as agency workers, temporary workers and contractors.

5. What is Data Protection?

5.1 Data Protection is concerned with making sure that organisations handle personal data in a responsible way. It sets out legal obligations on how personal data is to be handled in relation to its collection, usage, storage, destruction, transfer and disclosure.
5.2 The Legislation applies to any information about a living individual (e.g. staff members, contractors and visitors etc.). Essentially, staff who handle any information about people as part of their job will need to comply with this Data Protection Policy.

6. What is personal data?

6.1 Personal data can be either factual (such as name, address, telephone, images and photographs) or an expression of opinion about the individual (such as a performance appraisal or comments on scripts) including any intentions of the data controller or any other person in respect of that individual. The definition now also include genetic information biometric data used for identification purposes.
6.2 Personal data covers any information which relates to an individual in any format (written or oral). Examples include:

- a staff or other individuals file
- an E-mail about someone
- Information provided orally about the staff's personal circumstances.

6.3 'Special categories' data is data which is more sensitive and therefore requires more protection is:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

6.4 Data relating to criminal offences and convictions is not classed as special categories data but must be treated in a similar way2.

7. Data Protection Principles

7.1 The GDPR sets out the main principles for organisations when processing data. In accordance with Article 5 of the GDPR, the EMSO must ensure that personal data is:
a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation (EU) 2016/679 in order to safeguard the rights and freedoms of individuals;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7.2 As well as being responsible for compliance, the EMSO also has the obligation under Article 5 of the Regulation (EU) 2016/679 to be able to demonstrate compliance with the above principles.

8. Lawful basis for processing

8.1 The EMSO must determine the lawful basis for processing before starting any collection of personal data. The lawful bases for processing are set out in Article 6 of the Regulation (EU) 2016/679 and at least one of these must apply whenever personal data is processed:
(a) Consent: the individual has given clear consent to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract with the individual, or because they have asked the EMSO to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for the EMSO's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply when the EMSO is processing data to perform its official tasks).
8.2 In addition to having one of the lawful bases outlined above, the processing must also be necessary.
8.3 EMSO is a consortium of partners sharing in a common strategic framework scientific facilities (data, instruments, computing and storage capacity). The European Multidisciplinary Seafloor and water column Observatory (EMSO) aims to explore the oceans, to gain a better understanding of phenomena happening within and below them, and to explain the critical role that these phenomena play in the broader Earth systems. In undertaking these powers and related functions, the EMSO is acting as a public authority and will normally use public task for these function and cannot use legitimate interests as a legal basis for processing. However, when it is undertaking functions, it may use legitimate interests as a basis for processing if this is appropriate.

8.4 In order to process special categories data, the EMSO must also ensure that one of the following applies:
a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection4
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of EU or ITALY law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or ITALY law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or ITALY law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on EU or ITALY law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
8.5 Once the EMSO has determined the lawful basis for processing, this will be documented in the data records for each form of processing.
8.6 Where it is using legitimate interests as the basis for processing, this will be documented in a Legitimate Interests Assessment.

9. The rights of the individual

9.1 The EMSO must respect individuals' rights when processing personal data. These are enshrined in the legislation as follows:
1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

9.2 The rights above depend upon the lawful basis for processing. For example, the right to erasure only applies where the lawful basis for processing is consent. Where public task, legitimate interests, contractual basis or a legal requirement are used as the basis for processing, the right of rectification, restriction and the right to object are also limited to ensuring that the data is accurate before it can be processed.
9.3 The right to be informed is, however, a key right and applies in all circumstances (see Transparency below).

10. Data protection by default

10.1 Where the EMSO is undertaking new processing (eg it is collecting a new type of data or it is implementing a new system or process) it must consider building in data protection from the outset, including the organisational and technical measures to ensure appropriate security.
10.2 This may include undertaking a Data Protection Impact Assessment (DPIA) which is required for significant processing. Where a DPIA is not required, the EMSO must still consider the risks to the individual of processing and how these risks will be mitigated and to

document this assessment. This is undertaken by use of the Data Processing Form available from IT. The Information Security Manager will advise on what is required.
10.3 New processing must be approved before collection is started and signed off by the Data Protection Officer.

11. Data minimisation

11.1 Under GDPR, the EMSO has an obligation to ensure that it collects only what data is necessary. Those who are collecting data should, therefore, ensure that it is limited to what is required.
11.2 Staff are required to assess whether any data being collected is necessary for the proposed purpose. Where processing can take place without this data it should not be collected.

12. Transparency

12.1 The EMSO needs to provide specific information to people about how it processes their personal data. This information needs to be actively provided to individuals in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

12.2 To provide this information the EMSO must provide a privacy statement. The EMSO must ensure that the statement is targeted to the particular audience, particularly children. It has been determined by the ITALY Government that the age at which children can consent to the use of their data is 13.
12.3 The Privacy Statement must include the following:

- The name and contact details of the EMSO
- The contact details of the data protection officer
- The purposes of the processing
- The lawful basis for the processing
- The categories of personal data obtained
- The recipients or categories of recipients of the personal data
- The details of transfers of the personal data to any third countries or international organisations
- The retention periods for the personal data
- The rights available to individuals in respect of the processing
- The right to withdraw consent
- The right to lodge a complaint with a supervisory authority
- The source of the personal data
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data
- The details of the existence of automated decision-making, including profiling.

12.4 The Privacy Statements must be published on the EMSO website and made available to the data subjects. Where processing is taking place that is not covered in an existing statement, a Privacy Statement for that processing must be published.
12.5 In addition to the privacy statement, the EMSO is also required to inform data subjects of the purposes and use of data at the point of collection. Any EMSO forms (whether paper-based or web-based) that gather data on an individual should contain a summary of the Privacy Statement which explains the following:

- Why the data is being gathered and how the data will be used

- To whom the data may be disclosed to within the EMSO and to any outside third parties
- Consent where this the legal basis of processing

12.6 Staff may only process data for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Legislation. This means that personal data must not be collected for one purpose and then used for another purpose. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. The only exception to this is the use of research data.

13. Staff Responsibilities for data protection

13.1 The EMSO as a corporate body is the data controller and staff have the responsibilities as set out below to deliver its commitment to the protection of rights and privacy of individuals (including staff and others) in the processing of personal data.
13.2 Members of the EMSO Executive must be assured that this policy is being appropriately implemented in their areas of responsibility.
13.3 Heads of Central Mangement Office are responsible for developing and maintaining good information handling practice within the EMSO in accordance with this Policy and the Information Security Policy. They must maintain accurate records of the data processed in their department in accordance with the requirements of this policy and the Records Management Policy. They must ensure that individuals are clear about what data they hold through an appropriate Privacy Notice. They are also responsible for ensuring that all staff are trained in Data Protection and are aware of their responsibilities.
13.4 Staff: All staff or others who process personal data must ensure that they understand their obligations under this Policy and how to protect personal data and that they follow the guidance provided at all times.
13.5 All staff are responsible for reporting any breach or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data directly to the Data Protection Officer.
13.6 Data Protection Officer is the responsible for the management of data protection matters and for the development of specific guidance and practice on data protection issues for the EMSO. The tasks of the DPO are as follows:

- to inform and advise the EMSO and its employees about their obligations to comply with the Regulation (EU) 2016/679 and other data protection laws;
- to monitor compliance with the Regulation (EU) 2016/679 and other data protection laws, and with the EMSO's data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, contractors etc).

14. Authority to collect data

14.1 Apart from Central Services, no other Departments should routinely be collecting and storing staff personal data except for one off instances such as correspondence, field trips for health, safety purposes and attendance monitoring.
14.2 Managers should only collect staff data as advised by the Human Resources Department.
14.3 Personal data to be used in research projects may only be collected after approval by the EMSO Research Ethics Committee.

15. Data Protection Training

15.1 It is mandatory for staff to undertake Data Protection Training. On-line E Learning Data Protection training and data protection seminars will be held to assist members of staff with an understanding of their legal duty under the legislation. Staff in key roles will be provided with additional Data Protection training.
15.2 Data Protection training will be a part of a new member of staff's induction.
15.3 Failure to complete any mandatory Data Protection training may give rise to disciplinary action.

16. Data processors

16.1 The EMSO uses data processors, usually to store data and/or operate software on its behalf. Examples include Microsoft, Blackboard and Turnitin. Where it uses a data processor, the EMSO is still responsible for data protection and liable for any data transferred.
16.2 The EMSO is also liable for the data processor's compliance with the legislation and must only appoint processors who can provide sufficient guarantees that the requirements of the legislation will be met and the rights of data subjects protected. It must, therefore, ensure that there is an appropriate written contract with the data processor. The contract is important so that both parties understand their responsibilities and liabilities.
16.3 Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller and which must, as a minimum set out the following:

- only act on the written instructions of the EMSO;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the EMSO and under a written contract;
- assist the EMSO in providing subject access and allowing data subjects to exercise their rights under the Regulation (EU) 2016/679;
- assist the EMSO in meeting its Regulation (EU) 2016/679 obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a Member State.

17. Documentation

17.1 To comply with the legislation and the requirements for documentation, the EMSO has a Records Management Policy which documents the location and retention of all records within the EMSO within a records retention schedule.
17.2 Additional details set out below must be documented for all personal data and this is the responsibility of Heads of Central Services or Heads of School where they are undertaking processing that is unique to their school/college.

- The purposes of processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- Location of personal data.

- A description of the technical and organisational security measures.

17.3 Where consent is used as the lawful basis for processing, records of consent must be retained:
17.4 The EMSO must also document:

- Controller-processor contracts;
- Data Protection Impact Assessment reports;
- Legitimate Interest Assessments
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data, covering: - the condition for processing in the Data Protection Bill - the lawful basis for the processing in the GDPR - the retention and erasure policy document.

18. Security

18.1 The legislation requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.
18.2 The IT Services department and the Information Security Manager in particular is responsible for working with data owners to ensure appropriate security measures are in place.
18.3 All staff are responsible for ensuring personal data are kept securely and accessible only to those who need to use it. Appropriate security measures are to be taken to prevent accidental loss of, or damage to, personal data. This will mean the use of passwords or encryption for electronic documents and keeping papers under lock and key.
18.3 The transport of personal data in any format (laptop, hard copy, memory stick etc.) should be avoided as far as possible. This applies especially to special categories data, large volumes of personal data, or information which could cause particular harm or distress if lost. Only in exceptional circumstances should this information be transported outside of EMSO premises. Staff who do so should always ensure that it is kept with them at all times. Staff should:

- Where possible use remote login to their EMSO account to access information as an alternative to transporting data.
- Only carry the minimum amount of personal data (e.g. avoid carrying the whole file if only one document is needed).
- It is the EMSO's intention that all mobile devices (laptops, smartphones, tablets) and external storage media (USB sticks, external hard drives, DVDs, CDs, etc.) used to transport personal data and special categories data outside the EMSO will be secured by deploying strong encryption.

18.4 Any loss/theft must be immediately reported to the Data Protection Officer and the Information Security Manager as this represents a breach of this policy and must be recorded and reviewed for any action required.
18.5 When working remotely staff should:

- Use secure remote access facilities (VPN) instead of carrying work home;
- Never save documents containing personal data to a personal PC
- Consider that the means of connection may not always be secure/

18.6 All staff is to ensure that they comply with the requirements set out in the Information Security and supporting policies. These policies are the EMSO's response to the legal obligation under the Legislation to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. They

provide guidance on the usage and security procedure to follow when using the EMSO's IT systems.

19 International Transfers

19.1 In accordance with the Legislation, the EMSO may not transfer personal data to countries outside of the European Economic Area (EEA) (the European Union Member States along with Iceland, Liechtenstein and Norway) unless the country or territory has an adequate level of protection for personal data.

19.2 There are however a number of non-EEA countries recognised by the European Commission to have adequate level of personal data protection ("approved countries"). Transfer of information to these countries will not breach the Data Protection Legislation. Information on the European Commission's list of approved countries is available on the Information Commissioners website (https://www.garanteprivacy.it/).

19.4 The EMSO may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. These adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by ICO and approved by the Commission;
- compliance with an approved code of conduct approved by the ICO;
- contractual clauses agreed authorised by the ICO; or

19.5 The legislation permits that a transfer, or set of transfers, may also be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under ITALY or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The EMSO may not rely on the first three of these reasons when the lawful basis for processing is public task, eg for the provision of higher education or research. In these cases therefore, the EMSO must have a provision outlined in 19.4 in place before any transfer is made.

20. Breaches

20.1 All breaches of data protection should be reported to the Data Protection Officer and the Information Security Manager using the Breach Reporting Process.

20.2 It is essential that staff report a breach or potential breach immediately. This allows quick action to be taken to address the breach, as well as allowing the EMSO to comply with its obligation to report breaches.

20.3 If there has been clear negligence or intent with regard to any breach of the Data Protection Policy by members of staff, the EMSO will consider the circumstances and decide how best handle the next steps. Where a staff member has been negligent without mitigation, this will be dealt with in accordance with the EMSO's disciplinary procedures. All factors will be taken into account when determining appropriate action, including whether the beach was reported promptly.
20.4 In addition, a breach of the Policy may expose the EMSO and individual concerned to criminal or civil liabilities. In addition to any EMSO liability, staff may also personally liable. Data subjects may also apply to court for compensation if they have suffered damage from such a loss.

21. Data Storage, Retention and Disposal

21.1 It is the responsibility of the relevant senior manager to ensure that centralised records are maintained to meet the needs and reasonable expectations of EMSO, and external bodies. For members of staff, Human Resources has the responsibility of ensuring that centralised records are maintained.
21.2 Central databases should be used to avoid duplication of information and to increase data security. All local databases maintained by staff in the course of their duties containing personal data (including those using reference numbers for individuals rather than names) must be adequately secure (see Section 18).
21.3 The EMSO is required to ensure that all data is accurate and up-to-date. Staff has a responsibility to regularly update their records either through MyView or Blackboard.
21.4 The EMSO should not retain personal data for longer than is necessary. This means that personal data should be destroyed or deleted when it is no longer required.
21.5 The Records Retentions Policy and Schedule sets out the retention period for different types of documents. Staff should regularly review their records to ensure that the documents they hold are destroyed within the relevant destruction time limit in accordance with the Records Retention Schedule. Where the documentation contains personal information, the destruction must take place confidentially (e.g. shredding, disposal as confidential waste, secure electronic deletion).

22. Disclosure

22.1 Staff must not disclose personal data to a third party except in limited cases where there is a legal or statutory duty to do so or where it is in an individual's vital interests. All staff must therefore take care to ensure that personal data is not disclosed to unauthorised third parties which includes family members of the data subject, friends, government bodies and the Police in certain circumstances without the data subject's consent.
22.2 Where the Police are requesting data, this must be dealt with by the EMSO Secretary on receipt of the required form.
22.3 Where regular disclosures are made there must be a documented procedure and the data subject must be informed.

23. Rights of Access

23.1 Staff and other data subjects about whom the EMSO holds or uses personal data have a legal right to access that information and request a copy of the data in permanent form. Any person wishing to exercise their right of access formally should complete the "Data Subject Access Form" and submit it along with evidence of proof of identity to prevent unlawful disclosure of personal data to either the Compliance Officer or the Data Protection Officer An electronic copy of the Data Subject Access Form can be obtained from the EMSO's website.
23.2 By law, the EMSO has one month from receipt of the request and proof of identity, in which to respond to subject access requests, in any event the EMSO will endeavour to respond as quickly as possible. In limited circumstances, the EMSO may not be able to release personal data because exemptions under the Legislation are applicable, or the disclosure of the data would release personal data relating to other individuals.

23.3 The EMSO is committed to openness and current members of staff may view their personnel file, at no charge, by either making an appointment to visit the Human Resources office or requesting copies of their personnel file.
23.4 Staff who receive a request for personal information from an individual (data subject) or a third party acting on behalf of a data subject, they should be directed to the Subject Access Request form.
23.5 Where a third party is acting on behalf of a data subject, written authorisation from the data subject must be provided to confirm that the third party is acting on their behalf.
23.6 All requests should be passed to the EMSO Secretary or nominee where the data subject is seeking information about themselves, even if they do not mention the data protection.

24. E-mail and Social Media Usage

24.1 All staff should follow the EMSO's Information Security Policy and related policies and guidance such as the E-mail Etiquette Guide.
24.2 Staff should avoid using e-mail to send personal data or to express views about individuals. This is because e-mail is an insecure medium and the sender has no control over the storage or use of the message after it has been sent.
24.3 Staff must not communicate internally using social media including Facebook or WhatsApp as the EMSO has no control over these systems.
24.4 The EMSO reserves the right to monitor the use of its e-mail facilities and other internet traffic in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

25. CCTV

25.1 The EMSO operates close circuit television cameras (CCTV) across its offices and buildings, for the security and safety of its staff. The EMSO's use of CCTV is set out in a separate Policy. This Policy deals specifically with the collection and retention of personal data obtained through the use of CCTV to ensure compliance with the Data Protection Legislation.
25.2 The EMSO is committed to the protection and security of personal data especially as applied in the use, operation and monitoring of CCTV images. As such:

- All security staff involved in the recording, observation and capture of images must act in an ethical and lawful manner in accordance with legislation and must receive adequate training to ensure their understanding of compliance legislation.
- Only authorised persons involved in the monitoring or investigation can view CCTV images.
- All recorded material will be treated as confidential and unless required for evidence will only be kept in accordance with CCTV policy guidelines.
- CCTV will not be retained for longer than necessary in accordance with the data protection principles.
- Data is stored and managed automatically by the CCTV digital recorders which use software programmed to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces a minimum of 1 month rotation in data retention.

25.3 If CCTV images are retained beyond the retention period, they are to be stored in a secure place to which access is controlled and are to be erased when no longer required.

26. Direct Marketing

26.1 Any department or service that uses personal data for direct marketing purposes must inform the data subject of this at the time of collection of the information. The lawful basis of processing will normally be consent and the data subject must be provided with the opportunity to opt in and to object to the use of their data for direct marketing purposes.
26.2 In the case of sending information to enquirers and applicants where they would reasonably expect the EMSO to use their data in this way, data may be used to send these

individuals electronic communications. They must be provided with a simple way to object to the use of their data in this way in any communication.

26.3 Direct Marketing must also be in line with the Privacy and Electronic Communications Regulations (PECR).

27. Research

27.1 Personal data for research purposes is collected on the basis of public task. Collection of special categories data is on the basis that it is for research purposes. Consent to being part of the research study must still be collected. No collection of data is permissible until ethical approval has been given by the EMSO Research Ethics Committee.

27.2 Personal data collected for research purposes must not be used in forming any decisions about a particular individual, and must not be used in any way that will, or is likely to, cause distress to any data subject.