Data Protection Regulation

European Union

MODEL POLICY FOR MEMBERS USE

1. The EU Data Protection Directive enhances and broadens the scope of earlier regulations. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent, unless otherwise exempt.

2. This document is a model Data Protection Policy issued by the Association of British Investigators Limited for use by its EU members and the agencies under their respective control *(The Member).*

3. *The Member* complies with the requirements of the Data Protection regulations in force in *The Member's* jurisdiction with regard to the collection, storage, processing and disclosure of personal information and is committed to upholding the regulation's core Data Protection Principles.

4. *The Member* is committed to a policy of protecting the rights and privacy of individuals (includes staff, course delegates, and others) in particular the data subjects of investigations, in accordance with the Data Protection regulation.

5. *The Member* needs to process certain information about its staff, trainees, sub-contractors and other individuals it has dealings with as clients, subjects of instructions, for administrative purposes (e.g. to recruit and pay staff), and to comply with legal obligations and government requirements.

6. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

7. The policy applies to all data subjects. In the event of a breach of the Data Protection regulation or this Policy by a member of staff, *The Member's* employment disciplinary procedures will apply.

8. As a matter of good practice, other agencies and individuals working with and thus affiliated to *The Member*, and who have access to personal information, will be expected to have read and comply with this policy, the terms of which form part of the consultancy/agency agreement between *The Member* and that affiliate.

9. *The Member* is the Data Processor under the regulation, when dealing with its core business as an Investigation Agency and the client is the Data Controller.

10. *The Member* is the Data Controller under the regulation, when dealing with data of staff, clients, contractors, trainees and any other member or affiliate of *The Member* or in circumstances when The Member determines the manner in which and the purpose for which data is processed. For this purpose *The Member* has duly Notified the Information Commissioner.

11. Compliance with data protection regulation is the responsibility of all members and their contractors who process personal information.

12. Each member of staff, clients, contractors, trainees and any other member or affiliate of *The Member* is responsible for ensuring that any personal data supplied to or handled by *The Member* is accurate and up-to-date.

13. Data Subjects have the following rights regarding data processing and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the regulation.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Information Commissioner to assess whether any provision of the regulation has been contravened

14. Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent.

15. *The Member* understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

16. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from no response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

17. In most instances consent to process personal and sensitive data is obtained routinely by *The Member* (e.g. when a member of staff or consultant signs a Service or Consultancy Agreement).

18. Any forms (whether paper-based or electronic-based), that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data is to be published on the Internet as such data can be accessed from all over the globe.

19. If an individual does not consent to certain types of processing, appropriate action must be taken to ensure that the processing does not take place.

20. All staff and affiliates of *The Member* are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

21. All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerised, password protected, or
- kept on disks which are themselves kept securely.

22. Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

23. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be securely erased by overwriting the disc space before disposal.

24. This policy also applies to staff and affiliates of *The Member* who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and affiliates of *The Member* should take particular care when processing data in other locations outside the offices of *The Member* or its affiliated locations.

25. Members of *The Member* and / or other data subjects have the right to access any personal data which are held by *The Member* in electronic format and manual records which form part of relevant filing system held by *The Member* about that person, subject to exemptions.

26. Any individual who wishes to exercise this right should apply in writing to *The Member* who reserves the right to charge a fee for data subject access requests. Any such request will normally be complied with within 40 days of the receipt of the written request and, where appropriate, the fee.

27. *The Member* must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police, unless authorised under the terms of the regulation or other statute or Court Order or where disclosure of data is required for the performance of *The Member*'s contractual duty. All staff and affiliates should exercise caution when asked to disclose personal data held on another individual to a third party.

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

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

29. For reasons of personal security and to protect *The Member* premises and the property of staff, trainees and other visitors, close circuit television cameras may be in operation in several areas. The presence of cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- any monitoring will be carried out only by a limited number of specified staff;
- the recordings will be accessed only by approved personnel;
- covert monitoring should only be carried out temporarily where necessary to address specific issues of a serious nature;
- personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
- staff involved in monitoring will maintain confidentiality in respect of personal data.

Definitions

Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, identity number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) that makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data. Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data disclosure or otherwise making available of data.

Third Party

Any individual/organisation other than the data subject, the data controller (clients) or its agents.

Relevant Filing System

Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. **Please note that this is the definition of "Relevant Filing System" in the regulation. Personal data as defined, and covered, by the regulation can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.**

Principles - All processing of personal data must be done in accordance with the eight data protection principles.

1. **Personal data shall be processed fairly and lawfully.**
   Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. **Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.**
   Data obtained for specified purposes must not be used for a purpose that differs from those.

3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.**
   Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

4. **Personal data shall be accurate and, where necessary, kept up to date.**
   Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by *The Member* are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify *The Member* of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of *The Member* to ensure that any notification regarding change of circumstances is noted and acted upon.

5. **Personal data shall be kept only for as long as necessary.**

6. **Personal data shall be processed in accordance with the rights of data subjects under the Data Protection regulation.**

7. **Appropriate organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.**

8. **Personal data shall not be transferred to a country or a 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.**
   Data must not be transferred outside of the European Economic Area (EEA) - the twenty-seven EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Staff and/or contractors of *The Member* should be particularly aware of this when handling data that may be published on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

   EU States – Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.