

C & L INVESTIGATIONS PART OF THE C AND L GROUP

DATA PROTECTION POLICY

1. The purpose of this Policy is to protect the rights and privacy of living individuals and to ensure that personal data is not processed by *The Agency* without the person's knowledge or consent, unless otherwise exempt.
2. This document sets out the Data Protection Policy for *The Agency (and the named Member of the Association of British Investigators)* and should be read in conjunction with *The Agency's* Privacy Notice.
3. *The Agency* complies with the requirements of the prevailing data protection legislation with regard to the collection, storage, processing and disclosure of personal information and is committed to upholding the core data protection principles.
4. *The Agency* is committed to a policy of protecting the rights and privacy of individuals (includes staff, course delegates, clients, subjects of investigations and others) in accordance with the data protection legislation.
5. *The Agency* needs to process certain information about its staff, trainees, sub-contractors and other individuals it has dealings with such as clients, for administrative purposes (e.g. to recruit and pay staff), and to comply with legal obligations and government requirements.
6. During the course of its core business activities *The Agency* will be instructed to process the personal data of individuals who are identified in clients' instructions or during the course of the investigation undertaken pursuant to such instructions. *The Agency will not process any personal data* :
 - (a) **WITHOUT first having undertaken a Data Privacy Impact Assessment**, and
 - (b) without the CONSENT of the data subject or
 - (c) unless there is a specific legitimate interest ¹ except where such interests are overridden by the

¹ It is the policy of *The Agency* to accept instructions that involve the processing of personal data only in circumstances that fall into at least one of the following categories:

- National Security
- Public Security
- The Enforcement of Civil Law Claims
- Defence

interests or fundamental rights of the data subject or

(d) the circumstances are exempt or

(e) *The Agency* has exemption.

Furthermore to comply with the law, information processed about individuals must be kept to the minimum, collected and used fairly, be accurate, used solely for the purpose intended, stored safely, securely including protection against unauthorised or unlawful processing, loss, destruction or damage, using appropriate technical measures such as encryption or in password protected devices, retained for no longer than necessary 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 legislation or this Policy by a member of staff, *The Agency* employment disciplinary procedures will apply otherwise it will constitute a breach of contract.
8. As a matter of good practice, other agencies and individuals working with and thus affiliated to *The Agency* 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 Agency* and that affiliate.
9. It is expected that departments who deal with external agencies will take responsibility for ensuring that such agencies contract to abide by this policy.
10. *The Agency* is the Data Processor under the data protection legislation, when dealing with its core business as an Investigation Agency, Trainer and/or Security Consultant and the client is the Data Controller.
11. *The Agency* is the Data Controller under the data protection legislation, when dealing with data of staff, clients, contractors, trainees and any other member or affiliate of *The Agency*. For this purpose *The Agency* has duly registered with the Information Commissioner as a Data Controller and for *The Agency* purposes.
12. A Privacy officer, named above, has been appointed and is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for staff, clients, contractors, trainees, any other member or affiliate of *The Agency* or any data subject of an investigation.

-
- Prevention, Investigation, Detection or Prosecution of Criminal Offences
 - Matters of General Public Interest including Monetary, Taxation, Budgetary and Public Health objectives

13. The Senior Management and Heads of Departments and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within *The Agency*. .
14. Compliance with data protection legislation is the responsibility of all members and affiliates of *The Agency* who process personal information.
15. Each member of staff, clients, contractors, trainees and any other member or affiliate of *The Agency* is responsible for ensuring that any personal data supplied to or handled by *The Agency* is accurate and up-to-date.
16. 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 data protection legislation.
 - To take action to rectify, block, erase or destroy inaccurate data.
 - To request the Information Commissioner to assess whether any provision of the data protection legislation has been contravened.
17. Wherever possible or unless exempt, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent.
18. *The Agency* 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.
19. 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.

20. In most instances consent to process personal and sensitive data is obtained routinely by *The Agency* (e.g. when a member of staff or consultant signs a Service or Consultancy Agreement).
21. Any forms produced by *The Agency* (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.
22. 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, unless an exemption applies. **CONSENT GIVEN CAN BE WITHDRAWN AT ANY TIME BY GIVING THE AGENCY WRITTEN NOTICE.**
23. If any member or affiliate of *The Agency* is in any doubt about these matters, they should consult the Privacy Officer.
24. All staff and affiliates of *The Agency* are equally 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.
25. All personal data should be accessible only to those who need to use it. Those concerned 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 electronic, password protected, or
 - Kept on disks which are themselves kept securely.
26. 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 persons.
27. 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 wiped clean before disposal.

28. This policy also applies to staff and affiliates of *The Agency* 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 Agency* should take particular care when processing data at home or in other locations outside the offices of *The Agency* or its affiliated locations.
29. Members of *The Agency* and / or other data subjects have the right to access any personal data which are held by *The Agency* in electronic format and manual records which form part of relevant filing system held by *The Agency* about themselves.
30. Any individual who wishes to exercise this right should apply in writing to the Privacy Officer. *The Agency* will make no charge for data subject access requests. Any such request will normally be complied with within 30 days of the receipt of the written request supported by proof of identity and address.
31. *The Agency* 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 data protection legislation or other statute or Court Order or where disclosure of data is required for the performance of *The Agency* contractual duty or otherwise exempt. **All staff and affiliates should exercise caution when asked to disclose personal data held on another individual to a third party.**
32. The prevailing data protection legislation permits certain disclosures without consent to a Competent Authority, such as law enforcement agencies.
34. For reasons of personal security and to protect *The Agency* premises and the property of staff, trainees and other visitors, close circuit television cameras may be in operation in several areas. The presence of these 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 the Data Protection Officer;
 - 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 (for example 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". Personal data as defined, and covered, by the Act 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 six data protection principles.

- 1. Personal data shall be processed fairly, lawfully and transparently.**

Data processing will not be lawful unless it satisfies at least one of the following processing conditions:

- **Consent** – The data subject has provided valid consent for the processing.
 - **Contract** – The processing is necessary for the performance of a contract.
 - **Legal obligation** – The processing is necessary for compliance with a legal obligation to which the controller is subject.
 - **Legitimate interest** – The processing is necessary for the purposes of the legitimate interests pursued by the Data Controller, the client or *The Agency*, except where such interests are overridden by the interests or fundamental rights of the data subject. Fraud prevention, cybersecurity and direct marketing are examples of the type of activities that might constitute legitimate interests.
 - **Vital interest** - The processing is necessary to protect the data subject's vital interests, such as in a medical emergency.
 - **Public interest** – Processing is necessary for a task carried out in the public interest.
2. **Purpose limitation** - Data processing must relate to a specific, explicit and legitimate purpose. Data must not be processed in a manner that is incompatible with the stated purpose/s. Generic purpose statements will not be compatible with the data protection legislation.
 3. **Data minimisation** - Data collected must be limited to what is necessary. It must be adequate, relevant and not excessive, having regard to the stated purpose for which data is being processed.
 4. **Accuracy** - Data must be kept accurate and up to date. Controllers must be able to correct personal data 'without undue delay'.
 5. **Storage limitation** - Data should not be kept for any longer than is necessary. Data retention policies should establish time limits for erasure, although it is permissible to retain data for longer periods for archive or statistical purposes only.
 6. **Integrity and confidentiality** - Personal data must be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing, loss, destruction or damage, using appropriate technical or organisational measures.