COASTAL INVESTIGATION SERVICES

PROCESS SERVERS / INVESTIGATORS - AGENTS TO THE LEGAL PROFESSION
MEMBER OF THE ASSOCIATION OF BRITISH INVESTIGATORS
REGISTERED UNDER THE DATA PROTECTION ACT
PRINCIPAL – JERRY KILSHAW

General Data Protection Regulation
Data Protection Compliance Policy

1. This Policy has been formulated from the Guidance published on the Information Commissioner's Office website and from the Association of British Investigators model policy for members use.

2. This Policy supersedes all previous Data Protection Policies issued by Coastal Investigation Services (The said company)

3. As a matter of good practice, other agencies and individuals working with the Company, and contractors, who have access to personal information, otherwise known as Personal Data, will be expected to read and comply with this policy.

4. Jerry Kilshaw of Coastal Investigation Services is registered as a Data Controller with the ICO. The core business of the Company is an Investigation Agency.

5. Coastal Investigation Services complies with the Principals of UK Data Protection and the European Union Data Protection Union.

6. The Company is committed to a policy of protecting the rights and privacy of individuals, in particular the data subjects of investigations in accordance with the General Data Protection Regulation.

7. The Company needs to process certain information about its staff, contractors and other individuals it has dealings with such as clients, subjects of instructions for administrative purposes to comply with legal obligations and government requirements.

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

9. All personal data will be processed and retained in accordance with the Principals of Data Protection.

10. Under the Data Protection Act 1998 and for the purposes of this Policy, "Personal Data" is defined as:

Data which relates to a living individual who can be identified

- from those data, or
- from those data and from other information which is in the possession of, or likely to come into the possession of, the Data Controller

- and includes any evidence of opinion about the individual or any indication of the data controller or any person in respect of the individual

11. Under GPDR the Company is required to state its lawful basis for processing Personal Data

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:
(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you 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 for you 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 your 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 if you are a public authority processing data to perform your official tasks.)

12. The Company may be required to process personal data for the following reasons
Consent – including written consent to process and retain personal data and sensitive personal data agreed by Clients, Company Staff, Contractors
Vital Interests – The Company may be required to process personal data and sensitive personal data relating to individuals suspected of presenting a threat of physical harm another individual(s) or suspected of presenting a threat to the health, safety, welfare or finances of another individual(s).
Legitimate Interests – The Company may be required to process personal data and sensitive personal data relating to individuals who are being investigated because they are suspected of breaching UK or EU Criminal Law or Civil Law or because it is assessed the data may otherwise be required in legal proceedings at Court or at a Tribunal.

Key Principles of Data Protection

13. The 8 key Principals of the General Data Protection Regulations shall be adhered to at all times by Coastal Investigation Services staff, and the Company's agents. We will adhere to:

Principle 1
Personal data shall be processed fairly, lawfully and transparently, in particular, shall not be processed unless at least one of the conditions in Paragraph 12 above are met.

Principle 2
Personal data shall be obtained only for specified lawful purposes in Paragraph 12 and shall not be further processed in any manner not compatible with that process.

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed (“data minimisation”)

Principle 4
Personal data shall be accurate and, where necessary, kept up to date (“accuracy”)

Principle 5
Personal Data will not to be kept longer than is necessary for the purpose ('storage limitation')

Coastal Investigation Services shall:
Regularly review the length of time we keep personal data and
if we consider the purpose or purposes we hold the information is no longer necessary we will securely delete information.

Principle 6
Personal data shall be processed in accordance with the Rights of data subjects

Principle 7
Appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction ('integrity and confidentiality')

Principle 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.

Other Considerations

14. In accordance with Principle 6, Data Subjects have the following rights regarding data processing and the data 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 the purposes of direct marketing
•To be informed about mechanics of automated decision taking processes that will significantly affect them. (No automatic decision process will be taken by the Company)
•Not to have significant decisions that will affect them taken solely by automated process
•To aply 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

•In the event of a complaint by a Data Subject concerning our processing of personal data, we invite a complaint for to us to resolve. If we are not able to resolve the complaint we will advise the Data Subject to direct the complaint to the ICO.
•The Company will maintain a Complaints Procedure Policy, which will be available on request.

15. Consent to process personal and sensitive data will be obtained when an individual signs a Service or Consultancy Agreement. This will be in the form of a stand alone consent document, which the individual will be invited to sign to confirm they agree to the Company processing their Personal Data.

16. Personal Data in relating to our Clients or to our Contractors (affiliates) will never be shared with third parties who are not directly employed by the Company, unless with the Client/Contractor's prior written agreement.

17. Personal Data in respect of individuals being investigated by the Company, and details of investigations, will only be shared on the strict principle of "need to know". This may be in electronic or paper format. The data will be securely and safely stored by the individual receiving the data. The data will be destroyed immediately when the individual in receipt of the data no longer has good reason to retain it. The Data Controller is responsible for ensuring destruction of data shared with and retained by third parties who will confirm in writing that all data held has been destroyed when directed to do so.

18. All staff and affiliates of the Company are responsible for ensuring that any personal data (on others) which they hold is kept securely and that data is not disclosed to any unauthorised third party. Personal data will not be shared with any third parties, including law enforcement agencies, unless authorised by statute or Court Order.

19. When it is necessary to store personal data in electronic format, it shall only be stored on password protected devices.

20. Data stored in hard copy must only be kept in a locked drawer or filing cabinet.

21. If it is necessary to transfer personal data, it will only be done via secure email or via password protected memory stick or disc.

22. If personal data, or any other details of an investigation, being electronically transferred by email is assessed as sensitive, the document(s) containing the data must be password protected to minimise the risk of compromise.

23. Regulations permit certain disclosures to be made to Law Enforcement without consent of a Data Subject 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 of 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 interests of the individual – life and death situations

24. Personal data concerning identities of individuals and information in respect of the nature of enquiries made by the company shall be retained in electronic or other durable format only for as long as absolutely necessary. Documents may be retained in redacted format to remove Personal Data in order comply with lawful requirements to prepare / provide records/ evidence for Company tax and audit purposes.

25. The Data Controller will be responsible for regularly reviewing records of investigations, assessing whether it is absolutely necessary to retain the personal data and for redacting or destroying the documents relating to an investigation.

26. A record will be made each time a Review is undertaken. If the Review establishes that there is no longer justification to retain personal data, the relevant electronic and hard copy personal data relating to the individual and the investigation shall be destroyed or in limited cases, such as criminal investigations, where it is assessed the data may be required at a future date, the personal data and evidential material may be archived. The grounds to continue to retain data shall be recorded.

27. When a decision is made to destroy documents the Data Controller will issue a Destruction Certificate confirming material has been destroyed in all durable formats. When a Destruction Certificate is issued, it shall be the responsibility of the Data Controller from the company to ensure that all personal data held in electronic or hard copy formats is destroyed, and that all staff and agents who are likely hold personal data relating to the data subject are instructed to destroy all electronic and hard copy records they may hold. Those staff and agents shall confirm to the Data Controller when they have complied with the instruction.

28. When personal data is destroyed a Destruction Certificate will be issued, confirming the date and rationale for destroying the data. If the data was collected on behalf of another organisation, a copy of the Destruction Certificate shall be forwarded to that Organisation.

29. All new systems and software introduced by the Company will be assessed to ensure the system or software is compliant with the principles of GPDR.

30. The Company Data Controller will notify all identified breaches of data processing to the Information Commissioners Office within 72 hours.

Jerry Kilshaw
Data Controller
1st February 2018