Orion Investigations & Intelligence Limited

General Data Protection Regulation

Data Protection Compliance Policy

February 2018

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

2. This Policy supersedes all previous Data Protection policies issued by Orion Investigations & Intelligence Limited (the 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. Martyn Meekums of Orion Investigations & Intelligence Limited is registered as a Data Controller with the ICO. The core business of the Company is an Investigation Agency.

5. Orion Investigations & Intelligence Limited complies with the 8 Key Principals of GDPR Data Protection (see Paragraph 13 below) .

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 GDPR.

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

8. To comply with the law, information about individuals (known as personal data) will be collected and used fairly and transparently, stored safely and securely, and will not be disclosed to any third party unlawfully.

orionInvestigations.co.uk

9. Categories of Personal Data

   The Company may process Personal Data and Sensitive Personal Data

   Personal Data

   Under GDPR, Personal Data is defined as "any information relating to an identified or identifiable natural person". This may include your name, date of birth, address or other location indicator, email address, vehicle details, telephone number, IP address.

   Sensitive Personal Data

   Sensitive personal data is defined as "data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation."

10. 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 the Company processes personal data:

    (a) Consent: the individual has given clear consent for the Company to process their personal data for a specific purpose.

    (b) Contractual Necessity: the processing is necessary for a contract the Company has with the individual, or because the individual has asked the Company to take specific steps before entering into a contract.

    (c) Legal obligation: the processing of personal data is necessary for the Company 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 in the Company'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.

12. The Company will only 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

    Contractual Necessity – In every case where the Company engages with a new client, it is essential the Company conducts due diligence to verify the client's identity and credentials to ensure they have lawful reasons to request an investigation. Unless the client provides personal data to the Company which confirms true identity, the Company will not engage with that individual.

It is essential the Company obtains and retains sufficient personal data in respect of staff and contractors to enable contracts to be raised and payments to be made.

The "contractual " lawful basis permits the processing of personal data that takes place prior to the Company entering into a contract if an individual requests information from the Company about a particular service, the processing of that individual's personal data is permitted for the purposes of responding to that enquiry.

Legal Obligation – The Legal Obligation applies to the Company Data Controller only. The legal obligation must be binding in nature. For example, the "compliance with legal obligations" lawful basis does not apply where a governmental authority requests access to personal data, but the controller's compliance with that request is not legally mandatory.

A "legal obligation" in this context means a legal obligation arising under EU law or the laws of a Member State. A legal obligation to process personal data arising under the laws of a non-EU jurisdiction does not provide a lawful basis for processing personal data.

Vital Interests – The Company may be required to process personal data and sensitive personal data relating to individuals suspected of presenting a serious threat of physical harm another individual(s) or suspected of presenting a serious threat to the health, safety, welfare of another individual(s).

Legitimate Interests – The Company may be required to process personal data and sensitive personal data relating to individuals who are subject of investigation because there are reasonable grounds to suspect a breach of UK Law; EU Law and EU Member States' Law or because it is assessed the data may otherwise be required in legal proceedings at Court, Tribunal or other judicial capacity. GDPR Art.9(2)(f) states data may be processed where it is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity.

13. **Key Principles of Data Protection**

The 8 key Principals of the General Data Protection Regulations shall be adhered to at all times by Orion Investigations & Intelligence Limited staff, and the Company's agents. The Company, its Staff and its affiliates will adhere to:

Principle 1

Personal data shall be processed fairly, lawfully and transparently in relation to the Data Subject. In particular, data 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 limited to what is necessary 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"). Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.

Principle 5

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

The Data Controller will regularly review the length of time the Company retains personal data and if the purpose or purposes the Company holds the information is no longer necessary, the data will be securely destroyed.

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 EU 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

13. 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 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
    - In the event of complaint by a Data Subject concerning our processing of personal data will invite complaint 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.

14. 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.

15. 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 or unless there is a lawful requirement to do so.

orioninvestigations.co.uk

16. Personal Data in respect of individuals being investigated by the Company, and details of investigations, will only be shared with staff and with affiliates of the Company 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.

17. 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.

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

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

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

21. 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.

22. 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

23. Personal data concerning identities of individuals and information in respect of the nature of enquiries made by Orion Investigations & Intelligence Limited 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.

24. The Data Controller will be responsible for regularly reviewing records of investigations, assessing whether there continues to be justification that it is absolutely necessary to retain the personal data and to decide whether to redact (remove personal data) or securely destroy the documents relating to an investigation.

25. 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 securely 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.

26. When a decision is made to destroy documents the Data Controller will issue a Destruction Certificate confirming material has been destroyed in all formats. When a Destruction Certificate is issued, it shall be the responsibility of the Data Controller for

orioninvestigations.co.uk

Orion Investigations & Intelligence Limited 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.

27. 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.

28. 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.

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

30. A Data Protection Impact Assessment (DPIA) will be carried out when

    i. using new technologies; and
    ii. the processing is likely to result in a high risk to the rights and freedoms of individuals.
    iii. Processing that is likely to result in a high risk includes (but is not limited to):
    iv. systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
    v. large scale processing of special categories of data or personal data relation to criminal convictions or offences.

       This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.
    vi. large scale, systematic monitoring of public areas (CCTV).

    It is unlikely Orion Investigations & Intelligence Limited will be required to conduct a DPIA for reasons other than (i) and (iv)

Martyn Meekums
Data Controller,
Orion Investigations & Intelligence Limited.

9 February 2018