



Orion Investigations & Intelligence Ltd®

Privacy Policy

This Policy should be read in conjunction with the Orion Investigations & Intelligence Ltd® Data Protection Policy and Information Security Policy. These Policies are available on the Company website, and on written request.

For the purpose of this document Orion Investigations & Intelligence Ltd® Directors, Employees and sub-contractors are collectively referred to as Agents.

Purpose

The purpose of this policy is to ensure Orion Investigations & Intelligence Ltd® complies with UK Law in relation to the protection of personal data and information concerning any individual recorded, retained and processed, and respects the Privacy of all individuals it has dealings with including our clients, agents, professional contacts, and individuals subject of Company activities.

The Company will process personal data only if at least one of the following reasons applies:

Consent – including written consent to process and retain personal data and sensitive personal data agreed in writing by Clients and Agents.

Contractual Necessity – In every case where the Company engages with a new client, it is essential the Company conducts due diligence to confirm the client's true identity so as to be certain the client is who they claim to be. Unless the client provides personal data to the Company which confirms their bona fide to the satisfaction of the Company, 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.

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 to another individual or suspected of presenting a threat to the health, safety, welfare of another individual.

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.

Legal Obligation – The Legal Obligation applies to the Company Data Controller only. The 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.

The Company will record and retain information voluntarily provided in the course of its business by: Clients, Agents, Professional Contacts, and individuals subject of investigation/ action

Categories of Personal Data and Collection Methods

The company may process Personal Data and Sensitive Personal Data.

What is Personal Data?

Under GDPR, Personal Data is defined as “any information relating to an identified or identifiable natural person”. This may include their name, date of birth, address or other location indicator, email address, vehicle details, telephone number, IP address, and includes photographs and video of individuals obtained in public places.

We are likely to collect information about individuals subject of action where it is necessary for our legitimate interests by use of open-source research and legal access of official records. We may use third party providers to acquire data. The purpose of this information collection may be to identify individuals, assist us in the performance of our lawful activities, or minimise physical risks to Orion Investigations & Intelligence Ltd® Staff and sub-contractors.

What is 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.”

Information we Do Not Collect

We do not collect any Special Categories of Personal Data about individuals, this includes details about race or ethnicity, religious or philosophical beliefs, political opinions, trade union membership. We do not collect information about children of individuals subject of action.

Use of Information

Orion Investigations & Intelligence Ltd® will only record information where it is voluntarily provided or where we have “legitimate interest” in accordance with GDPR legislation. We consider and balance any potential impact on an individual (both positive and negative) and their rights before we process personal data for our legitimate interests.

We do not process personal data for activities where our interests are overridden by the impact on the individual (unless we have consent or are otherwise required or permitted to by law).

Visits to the Orion Investigations & Intelligence Ltd® Website

In the case of visits to the Orion Investigations & Intelligence Ltd® webpages, we may use Cookies to track and optimise webpage behaviour. Should a person object, they are free to turn off cookies in their local browser. In the case of communication via our website requesting contact will record the details provided by the potential client.

Compliance with the law

Sometimes, we must process personal information to comply with a statutory obligation. For example, we may be required to give information to legal authorities if they so request or if they have the proper authorisation such as a search warrant or court order. This may include personal information held about individuals.

A record will be retained to identify the source of personal data processed. A record will be maintained to identify whether personal data is retained as a contractual or statutory requirement.

Sharing of Personal Data

Personal Data and Sensitive Personal Data relating to Company staff, Contractors, and Clients will never be shared with individuals or bodies outside of the Company unless there is a lawful requirement to do so. Personal Data in respect of individuals in these categories will only be processed with their written consent.

Personal Data in respect of individuals subject of investigation will only be shared on a strict need to know basis with individuals who are directly undertaking investigative activities for Orion Investigations & Intelligence Ltd®.

Transfers to third country and safeguards

In accordance with GDPR Principle 8

Personal data shall only be transferred to countries or territories who are signatories to GPDR (The UK and EU Member States), unless that non-EU 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.

The Company will undertake due diligence to confirm the appropriate levels of data protection are in place in every case when it is necessary to transfer personal data to a country or territory which is not a GDPR signatory.

Retention period or criteria used to determine the retention period

In accordance with GDPR Principle 5

Personal Data processed will not to be kept longer than is necessary for the purpose ('storage limitation'). Data obtained during the course of investigations will be destroyed after ONE year after conclusion of the investigation, unless there is a compelling operational, business or legal reason to retain the information for longer. Reasons for retention for longer periods will include: ongoing investigation; required as evidence or potential evidence at a Court or Tribunal.

The Company Data Controller will undertake regular reviews of personal data held to confirm it is absolutely necessary to continue processing or retaining the data, in accordance with the Lawful Basis outlined above. If it is assessed the necessity no longer exists, the data will be securely destroyed in all formats in which it is held. A Destruction Certificate will be issued to confirm destruction. If the Data Subject is a Company Staff member, Client or Contractor they will be notified of the destruction.

Data required to be retained for HMRC audit will be retained for FIVE years. This will include personal data concerning client identity, banking details, details of payments to the Company, and brief details of the matter.

Data Subject Rights

Data Subjects have the right to know what personal data has been processed by the Company and can apply in writing to the Data Controller for details personal data processed without charge. The personal data will be provided within one month of the first communication to the Data Controller.

Under certain circumstances, all data subjects have rights under data protection laws in relation to your personal data, these include:

Request Access - All data subjects have the legal right to request details of information held about them by the company. This enables them to receive a copy of the personal data that we hold about them and to check that we are lawfully processing it. Any subject access requests received by Orion Investigations & Intelligence Ltd® should be referred to the Data Controller (see below). The company will respond to any subject access requests promptly, and in any event within a month of the request.

Data Correction - You have the right to require us to rectify any inaccurate personal information we hold about you. You also have the right to have incomplete personal information we hold about you completed, by providing a supplementary statement to us.

Erasure of Data - This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. If you would like us to destroy information held about you, please let us know. However, please note that if you use any of our services which require you to provide personal information, deleting our records will mean that you will need to resubmit it to continue using such services. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Data Processing Restrictions

This enables you to ask us to suspend the processing of your personal data by a request in writing in the following scenarios:

If you want us to establish the data's accuracy.

Where you need us to hold the data even if we no longer require it because you need it to establish, exercise or defend legal claims; or you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

The right to withdraw consent at any time, where relevant

A Data Subject has the right to withdraw consent to their personal data being processed at any time. Immediate steps will be taken to securely destroy personal data relating to that Data Subject.

The right to lodge a complaint with a supervisory authority

A Data Subject may make a complaint to the Data Controller if he/she believes personal data processed is inaccurate or has been retained longer than necessary. If the Data Subject is not satisfied with the action taken to resolve the situation, he/she will be directed to lodge the complaint with the Information Commissioner's Office.

Automated Decision Making

All decisions relating to a Data Subject's personal data will only be made after personal assessment by the Data Controller. Decisions about personal data processing will never be made by an automated process.

Data Breach Notification

Orion Investigations & Intelligence Ltd® shall immediately inform the relevant parties/entities in writing and by e-mail of any Personal Data Breach of which the Company becomes aware, but in no case longer than 24 hours after it becomes aware of the Personal Data Breach. The notification to the relevant parties shall include all available information regarding such Personal Data Breach, including information on:

The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records.

The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects

Orion Investigations & Intelligence Ltd® shall promptly take all necessary and advisable corrective actions and shall cooperate fully with the relevant parties/entities in all reasonable and lawful efforts to prevent, mitigate or rectify such a breach.

Data Controller

The Data Controller for Orion Investigations & Intelligence Ltd is Martyn Meekums.

Contact details:

office@orioninvestigations.co.uk

Tel: 01273 921617

57 Newtown Road, Hove Brighton & Hove BN3 7BA

ENDS

Policy Date 01/12/2025