



Orion Investigations & Intelligence Limited

Privacy Notice

February 2018

This Notice should be read in conjunction with the Orion Investigations & Intelligence Limited Data Protection Policy dated February 2018.

The GDPR sets out the information that we should supply and when individuals should be informed.

The information we supply is determined by whether or not the Company obtained the personal data directly from individuals.

The information we supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language and
- free of charge.

Data Controller

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

Contact details are:

info@orioninvestigations.co.uk

Tel: 01273 921617

Gemini House
136-140 Old Shoreham Road
Brighton & Hove
BN3 7BD

Purpose of the processing and the lawful basis for the processing of personal data

The Company may process personal data only if it 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, 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 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 they are bona fide, 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.

Categories of Personal Data

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 your name, date of birth, address or other location indicator, email address, vehicle details, telephone number, IP address.

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.”

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 Limited.

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 GDPR (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')

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.

The existence of each of data subject's 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

The source the personal data originates from and whether it came from publicly accessible sources

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

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 anytime. 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.

9 February 2018