- INVESTIGATIVE & LITIGATION SUPPORT SERVICE PROVIDER –

DATA PROTECTION SUPERVISORY AUTHORITY

www.ico.org.uk

DATA PROTECTION

UK GENERAL DATA PROTECTION REGULATION

AS PER ASSOCIATION OF BRITISH INVESTIGATORS MODEL DOCUMENT [AS ADAPTED 08-APR-22]

IP Forensics [GB] Limited
Registered Office: 5/6 Harington Place, Bath, BA1 1HF
Telephone: 0044 117 904 7201
Email: info@ipfgb.co.uk
Data Protection registration: Z3622809

IP FORENSICS GB

PART 1: PRIVACY NOTICE

1. The purpose of this Privacy Notice is to protect the rights and privacy of living individuals and to ensure that personal data is not processed by IP Forensics GB Limited [hereafter IPFGB] without the person's knowledge or consent, unless otherwise permitted. The Privacy Notice also sets out individuals' rights under the data protection legislation.

2. This document sets out the Data Protection Policy for IPFGB and should be read in conjunction with record of processing activities annexed hereto.

3. IPFGB 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. IPFGB is committed to a policy of protecting the rights and privacy of individuals [including staff, course delegates, trainees and trainers, clients, subjects of investigations and others] in accordance with the data protection legislation.

5. IPFGB needs to process certain information about its staff, trainees and trainers, sub-contractors, and other individuals it has dealings with such as clients, and to comply with legal obligations and government requirements.

6. During its core business activities IPFGB 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. IPFGB will not process any personal data without first having been satisfied as to the lawful basis on which to process personal data which, when necessary, will be recorded in a Data Privacy Impact Assessment.

7. 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.

8. The policy applies to all Data Subjects. In the event of a breach of the data protection legislation or this Privacy Notice by a member of staff, IPFGB employment disciplinary procedures will apply otherwise it will constitute a breach of contract.

9. As a matter of good practice, other agencies and individuals working with and thus affiliated to IPFGB and who have access to personal information, will be expected to have read and comply with this Privacy Notice, the terms of which form part of the consultancy/agency agreement between IPFGB and that affiliate.

10. It is expected that departments who deal with external agencies will take responsibility for ensuring

that such agencies contract to abide by this policy.

11. Depending on the circumstances of the processing activity and who determines the purpose and means for the processing of an individual's personal data, IPFGB may be the Processor or Controller under the data protection legislation, when dealing with its core business activity as an Investigative, Risk Management & Litigation Support Service Provider. However, in certain circumstances IPFGB will be Joint Controller with the instructing client. There may be instances when acting under strict instructions, which also cover the purpose [the why] and means [the how] for the processing of all the personal data in the client provided case scenario, that IPFGB will be the Processor.

12. IPFGB is the Controller under the data protection legislation, when dealing with data of staff, clients, contractors, trainees and any other member or affiliate of IPFGB.

13. The Senior Management and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within IPFGB.

14. Compliance with data protection legislation is the responsibility of all members and affiliates of IPFGB who process personal information.

15. Each member of staff, clients, contractors, trainees and any other member or affiliate of IPFGB is responsible for ensuring that any personal data supplied to or handled by IPFGB is accurate and up to date.

16. Data Subjects have the following rights regarding data processing and the data that are recorded about them [unless an exemption applies]:
    - 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 making 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 prevailing 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 prevailing data protection legislation has been contravened.

17. For criminal offence data, explicit written consent of the Data Subject must be obtained unless an alternative lawful basis for processing exists and IPFGB has ensured that it has an additional condition for processing this type of data, under Schedule 1 of the Data Protection Act 2018, for example, to safeguard vulnerable individuals or children, assess people's suitability for employment, or assess whether a person can access services such as housing or insurance.

18. IPFGB will not keep any comprehensive register of criminal convictions.

19. For special category data processing is prohibited, unless the Data Subject has given explicit consent or one of the permitted conditions set out in the data protection legislation are met.

20. IPFGB 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 based on misleading information will not be a valid basis for processing.

21. There must be some active communication between the parties. Consent cannot be inferred from no response to a communication.

22. In most instances consent to process personal, special category or criminal offence data is obtained routinely by IPFGB [e.g. when a member of staff or consultant signs a Service or Consultancy Agreement].

23. Any IPFGB forms [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.

24. 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.

25. **CONSENT GIVEN CAN BE WITHDRAWN AT ANY TIME BY GIVING IPFGB WRITTEN NOTICE.**

26. If any member or affiliate of IPFGB is in any doubt about these matters, they should consult a director.

27. All staff and affiliates of IPFGB are 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.

28. 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.

29. 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 screensavers and manual records should not be left where they can be accessed by unauthorised persons.

30. 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.

31. This Privacy Notice also applies to staff and affiliates of IPFGB 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 IPFGB should take particular care when processing data at home or in other locations outside the offices of IPFGB or its affiliated locations.

32. Members of IPFGB and / or other Data Subjects have the right to access any personal data which are held by IPFGB in electronic format and manual records which form part of relevant filing system held by IPFGB about that person.

33. Any individual who wishes to exercise this right should apply in writing to a director or senior management. 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.

34. IPFGB 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 prevailing data protection legislation or other statute or Court Order or where disclosure of data is required for the performance of IPFGB contractual duty or otherwise exempt. All staff and affiliates should exercise caution when asked to disclose personal data held on an individual to a third party.

35. The prevailing data protection legislation permits certain disclosures without consent to a Competent Authority, such as law enforcement agencies.

36. IPFGB undertakes its services in accordance with the data protection good practice policies, codes, and guides published by the Association of British Investigators.

37. For reasons of personal security and to protect IPFGB 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 Privacy Notice 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 senior managers;
    - The recordings will be accessed only by a director or an appointed senior manager:
    - 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.

GLOSSARY OF TERMS

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 Controller, includes name, address, telephone number, identity number. Also includes expression of opinion about the individual, and of the intentions of the Controller in respect of that individual.

Special category data

Different from ordinary personal data [such as name, address, telephone] and relates to data revealing or concerning:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Data concerning a natural person's sex life or sexual orientation.

The processing of special category data will require one of 10 separate conditions to be met. In addition to the Article 6 lawful basis the processing of the special category data must be necessary for the purpose IPFGB has identified and that they are satisfied there is no other reasonable and less intrusive way to achieve this purpose.

Five of the 10 conditions also require IPFGB to meet additional conditions and safeguards as set out under schedule 1 of the Data Protection Act 2018. The conditions must be determined and set out in a written record [Data Protection Impact Assessment] prior to processing commencing to assess the risk.

IPFGB will rarely process special category data but may find some cases where it is, for example, the data subject has provided explicit consent or in legal claims, contemplated legal claims or legal advice and more likely where the reasons are of substantial public interest [with a basis in law].

The substantial public interest condition will also require IPFGB to meet one of 23 specific conditions as set out in Part 2 of Schedule 1 of the Data Protection Act 2018, including and of more relevance to IPFGB [1] preventing or detecting unlawful acts, [14] preventing fraud, and [20] insurance.

Criminal offence data

Personal data relating to criminal offences are in addition to the lawful basis under Article 6 of the UK GDPR requirement subject to additional conditions because of the potentially significant impact that the processing of such data can have upon the data subject. The additional conditions [there are currently 28 to choose from] are set out in Schedule 1 of the Data Protection Act 2018 and the ICO website. It is important to note that this type of data is treated differently to other types of data, eg special category data. The ICO has explained that this is because the interests of society at large and the need to protect the public from criminal activity are likely to mean that the use of criminal offence data can be justified in a wider variety of circumstances, despite the potential impact on individual rights.

The processing of the criminal offence data must be necessary for the purpose IPFGB has identified and that they are satisfied there is no other reasonable and less intrusive way to achieve this purpose.

Data Subject

Refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Controller or Joint Controller

Means the natural or legal person, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Put simply, the Controller determines what information is needed and why. The Controller's responsibilities are greater than the Processor's.

Processor

Is a person or organization who deals with personal data as instructed by a Controller for specific purposes and services offered to the Controller that involve personal data processing. The status of the service provider as Controller or Processor may vary depending on the activity and needs to be reassessed for each processing of an individual's data.

Third Party

Any individual/organisation other than the Data Subject, the Controller, Joint Controller, Processor, or the agents/sub-contractors appointed by any of them when permitted by the Controller or the client.

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.

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 prevailing data protection legislation 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.

Investigative Service Provider ['Professional Investigation']

The Private Security Industry Act 2001 defines investigations as:

.... to any surveillance, inquiries or investigations that are carried out for the purpose of:

obtaining information about a particular person or about the activities or whereabouts of a particular person; or

obtaining information about the circumstances in which or means by which property has been lost or damaged

Litigation Support Services

An investigation agency client portfolio will inevitably include members of the legal profession and thus potentially forms part of the judicial process. Lawyers rely on outsourced investigative services for a number of reasons; primarily as part of their own case handling for lay, professional or commercial clients in contentious scenarios in contemplation of, or part of on-going legal proceedings. This work is referred to within the judicial system as "Litigation Support" and often includes activities that process personal data.

Privacy

Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion: **Physical privacy** – interference such as surveillance and the taking of biometric information, and **Informational privacy** – the ability of a person to control, edit, manage, and delete information about themselves and to decide how and to what extent such information is communicated to others.

Data protection law

The UK General Data Protection Regulation as applied in the UK and The Data Protection Act 2018.

BACK TO TOP

DATA PROTECTION PRINCIPLES

PRINCIPLES

Principle 1. Lawfulness, fairness, and transparency.

Principle 2. Purpose limitation.

Principle 3. Data minimization.

Principle 4. Accuracy.

Principle 5. Storage limitation.

Principle 6. Integrity & confidentiality [security]

Principle 7. Accountability.

All processing of personal data must be done in accordance with the seven data protection principles as explained by the Association of British Investigators guidance, [CLICK HERE to download].

BACK TO TOP

PART 2: RECORD OF PROCESSING ACTIVITIES

- INVESTIGATIVE & LITIGATION SUPPORT SERVICE PROVIDER –

DATA PROTECTION SUPERVISORY AUTHORITY IS THE INFORMATION COMMISSIONER'S OFFICE [ICO]

WWW.ICO.ORG.UK

1. **Nature of work – Professional investigation in the private sector, risk management and litigation support services.**

2. **Date: 08-Apr-22**

3. **Description of processing**

3.1. The following is a broad description of the way this organisation processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have with the organisation, check the Privacy Notice that the organisation has provided above, or contact the organisation to ask about your personal circumstances.

3.2. Reasons/purposes for processing information

We process personal information to enable us to:

- provide investigatory, risk management & litigation support services on the written instructions of a client;
- to maintain our own accounts and records;
- and to support and manage our employees, trainees, and contractors.

4. **Type/classes of information processed**

4.1. We process information relating to the above reasons/purposes. This information may include:

- personal details
- the investigation brief, results, and related information
- lifestyle and social circumstances
- family details
- goods and services
- financial details
- education and employment and/or business details

4.2. We also process special category or criminal classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- trade union membership
- religious or other beliefs
- criminality

5. **Who is the information processed about?**

5.1. We process personal information about:

- customers and clients, including prospective clients
- witnesses
- the subjects of investigations
- business contacts
- advisers and other professional experts
- suppliers/contractors
- employees

6. **Who the information may be shared with?**

6.1. We sometimes need to share the personal information we process with the individual themself and also with other organisations. Where this is necessary, we are required to comply with all aspects of the data protection legislation.

What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

6.2. Where necessary or required we share information with the following, which may include our clients and/or contractors:

- financial organisations
- credit reference, debt collection and tracing agencies
- law enforcement
- professional investigators
- government
- business associates and other professional bodies and advisers
- suppliers/contractors
- current, past, or prospective employers
- education and examining bodies
- family, associates, or representatives of the person whose personal data we are processing

7. Trading and sharing personal information

7.1. Personal information is traded and shared as a primary business function. For this reason, the information processed may include name, contact details, family details, financial details, employment details, and goods and services and where appropriate special category or criminal data. This information may be about customers and clients.

7.2. The information may be traded or shared with business associates and professional advisers, agents, service providers, customers and clients, and traders in personal data.

8. Undertaking research

8.1. Personal information is also processed in order to undertake research.

8.2. For this reason, the information processed may include name, contact details, family details, lifestyle and social circumstances, financial details, goods and services.

8.3. The special category or criminal data types of information may include sexuality, physical or mental health details, racial or ethnic origin and religious or other beliefs.

8.4. This information is about survey respondents. Where necessary or required this information may be shared with clients, contractors, other service providers, survey and research organisations.

9. Consulting and advisory services

9.1. Information is processed for consultancy and advisory services that are offered.

9.2. For this reason, the information processed may include name, contact details, family details, financial details, and the goods and services provided.

9.3. This information may be about clients.

9.4. Where necessary this information is shared with the data subject themselves, business associates and other professional advisers, current, past or prospective employers and service providers.

10. Transfers

10.1. It may sometimes be necessary to transfer personal information overseas.

10.2. When this is needed information may be transferred to countries or territories around the world.

10.3. Any transfers made will be in full compliance with all aspects of the data protection law.

BACK TO TOP