IP Forensics (GB) Data Protection Policy

It is the overarching principle of IP Forensics (GB) that the firm will adhere to the data protection legislation in the country in which it is operating; in this case the General Data Protection Regulation which came into force on 25-May-18.

Each and every individual employed directly by IPFGB and each and every sub-contractor must ensure that before processing Personal or Confidential Information, it must:

Management:

1. Have signed a valid Client contract, statement of work, or purchase order containing privacy and security data protection language that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Client Personal Information and categories of Data Subjects and the obligations and rights of the Client. IPFGB must present a valid Client contract, statement of work or purchase order containing the necessary description of Processing activities.

2. Assign responsibility and accountability for compliance with the Client Supplier Data Protection Requirements to a designated person within the company. IPFGB will identify the person charged with ensuring its compliance with the Data Protection Requirements. The authority and accountability of this person is clearly documented.

3. Ensure that all persons authorised to Process Client Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, Valid Client contract, statement of work or purchase order with confidentiality obligations.

4. Establish, maintain, and perform annual privacy training for employees that will have access to Client Personal Information. IPFGB educates employees initially and periodically on basic privacy and security principles. Proof that such training is conducted takes the form of training materials and/or records of attendance.

5. Process Client Personal Information only in accordance with Client's documented instructions including with regard to transfers of Personal Information to a third country or an international organisation, unless required to do so by applicable law; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Documented evidence of instructions, e.g. as set out in a contract, statement of work or purchase order, or captured as part of an electronic system used in the provision of the services.

6. Immediately inform the Client if, in its opinion, an instruction infringes applicable law. A contractual obligation on IPFGB to inform Client if, in the IPFGB's opinion, an instruction infringes applicable law.

Notice:

7. IPFGB will use the Client Privacy Statement when collecting Personal Information on the Client's behalf. The privacy notice is conspicuous and

available to Data Subjects to help them decide whether to submit their Personal Information to IPFGB. Privacy notices are readily available on and offline (www.ipfgb.co.uk) as needed, clearly dated and provided at or before the time of data collection.

8. When collecting Client Personal Information via a live or recorded voice call, IPFGB is prepared to discuss the applicable data collection, handling, use, and retention practices with Data Subjects. IPFGB demonstrates that data collection, handling, use, and retention are discussed with the Data Subject when Personal Information is collected via telephone.

9. A large amount of Data is gathered without the subject's consent during an investigation. This is allowed under Article 23 of the terms of the General Data Protection Regulation which includes information gathered in the prevention, detection or prosecution of Criminal Offences.

Choice and Consent:

10. Where IPFGB relies on consent as its legal basis for processing data, we will obtain and document a Data Subject's consent prior to collecting that Data Subject's Personal Information. IPFGB will explain the process for the Data Subject to consent or decline to provide Personal Information and the consequences of either action.

11. IPFGB captures any required Data Subject consent before or at the time of collecting Personal Information. We document and manage contact preferences and implement and manage changes to those preferences. Systems and procedures exist to manage Data Subject consent and contact preferences.

12. Document and manage changes to a Data Subject's contact preferences in a timely fashion. IPFGB monitors management of Data Subject consent to ensure effectiveness of systems and processes.

13. Obtain and document a Data Subject's consent for any new use of that Data Subject's Personal Information. IPFGB ensures that if consent was not given, there is no additional use or processing.

14. We do not use cookies and so will not leave them on your computers or other devices you may use.

Collection:

15. IPFGB will monitor the collection of Client Personal and Confidential Information to ensure that the only information collected is that required to perform the service(s) procured by Client. Systems and procedures exist to specify the Personal and Confidential Information necessary. IPFGB monitors collection to ensure effectiveness of systems and procedures.

16. If IPFGB procures Personal Information from third parties on behalf of the Client, IPFGB will validate that the third-party data protection policies and practices are consistent with IPFGB's contract with the Client and the GDPR requirements. IPFGB can demonstrate due diligence was performed regarding the third party's data protection policies and practices.

17. Before collecting sensitive Client Personal Information (data revealing 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), the necessity for collecting this information must be documented in an executed supplier contract with Client. IPFGB obtains and documents Client consent before collecting sensitive Personal Information.

Retention:

18. IPFGB ensures that Client Personal and Confidential Information is retained for no longer than necessary to provide the services unless continued retention of the Client Personal Information is required by law. IPFGB complies with documented retention policies or retention requirements specified by the Client in the contract, statement of work or purchase order.

19. IPFGB ensures that, at the Client's sole discretion, Client Personal or Confidential Information in our possession or under our control is returned to the Client or destroyed upon completion of services or upon the Client's request. Upon request, IPFGB will provide the Client with a certificate of destruction signed by an officer of the IPFGB. When the destruction of Client Personal or Confidential Information is necessary, IPFGB will burn, pulverise, or shred physical assets containing Client Personal Information so that the information cannot be read or reconstructed. Within applications, processes are in place to ensure that when data is removed from the application either explicitly by users or based on other triggers such as the age of the data, that it is securely deleted. IPFGB maintains records of the disposition of Client Personal and Confidential Information (e.g., return to Client for destruction).

20. As mentioned at paragraph 9 above we gather data without consent allowed under Article 23 of the GDPR. This information will be retained for historical research and or training purposes until such time as it is no longer required.

Data subjects:

21. Data Subjects have rights to access, delete, edit, export, restrict, and object to processing of their Personal Information ("Data Subject Rights"). When a Data Subject seeks to exercise their rights under applicable law in respect of their Client Personal Information, IPFGB will:

22. Assist the Client, through appropriate technical and organisational measures, insofar as possible, to fulfil its obligations to respond to requests for Data Subjects seeking to exercise their rights under applicable law.

23. Respond to all Data Subject Rights requests without undue delay. IPFGB conducts periodic tests to ensure they can support Data Subject rights.

24. Unless otherwise directed by the Client, IPFGB will refer all Data Subjects who contact us directly to the Client to exercise their Data Subject Rights. IPFGB will communicate to the Data Subject the steps that person must take to gain access to or otherwise exercise their rights vis-à-vis their Client Personal Information. IPFGB communicates the steps to be taken to access the Personal Information, as well the methods available to update the information.

25. When responding directly to the Data Subject we will validate the identity of the Data Subject making the request.

26. Secure permission from the Client to continue use of government-issued identifiers (for example, Social Security numbers) for authentication.

27. Once a Data Subject has been authenticated, IPFGB will: Determine whether it holds or controls Client Personal Information about that Data Subject. IPFGB has procedures in place to establish whether Personal Information is being held.

28. IPFGB will make a reasonable effort to locate the Client Personal Information requested and keep sufficient records to demonstrate that a reasonable search was made. IPFGB will respond to requests in a timely manner.

29. IPFGB will record the date and time of requests and the actions taken by us in response to such requests. We will provide records of Data Subject requests to Client upon request. IPFGB maintains records of requests for access and documents changes made to Personal Information.

30. Once a Data Subject has been authenticated and we have validated that we have the Client Personal Information requested, IPFGB will:

31. For requests to obtain a copy of Personal Information, provide the Client Personal Information to the Data Subject in an appropriate printed, electronic or verbal format. IPFGB supplies Personal Information to the Data Subject in a format that is understandable and in a form convenient to the Data Subject and IPFGB.

32. If their request is denied, at the Client's direction, we will provide the Data Subject with a written explanation that is consistent with any relevant instructions previously provided by Client. We will document instances where requests are denied and retain evidence of the Client review and approval.

33. IPFGB will take reasonable precautions to ensure that Client Personal Information released to a Data Subject cannot be used to identify another person. We will demonstrate that reasonable precautions are taken so that another person cannot be identified from the information released.

34. If a Data Subject and IPFGB disagree about whether Client Personal Information is complete and accurate, IPFGB will escalate the issue to the Client and cooperate with the Client as necessary to resolve the issue. IPFGB will document instances of disagreement and escalation of issues to the Client.

Disclosure to Third Parties:

35. If IPFGB intends to use a subcontractor to Process Client Personal and Confidential Information, IPFGB will: obtain the Client's express written consent prior to subcontracting services or making any changes concerning the addition or replacement of subcontractors.

36. Remain fully liable to the Client for the performance of any subcontractor. Contractual undertaking on IPFGB to remain liable to the Client for its subcontractors.

37. Document the nature and extent of Client Personal and Confidential Information sub-Processed by subcontractors, ensuring that the information collected is required to perform the service(s) procured by the Client. IPFGB maintains documentation concerning the Client Personal and Confidential Information disclosed or transferred to subcontractors.

38. IPFGB ensures the subcontractor uses Client Personal Information in accordance with a Data Subject's stated contact preferences. Systems and processes are in place to ensure the subcontractor uses the Client Personal Information solely for the designated purpose and in accordance with Data Subject contact preferences.

39. IPFGB will limit the subcontractor's Processing of Client Personal Information to those purposes necessary to fulfil our contract with the Client.

40. We will promptly notify the Client of any court order compelling the disclosure of Client Personal Information by the subcontractor and, as permitted by law, provide the Client the opportunity to intervene before filing any response to the order or notice. IPFGB will demonstrate that the Client has been contacted, when permitted, prior to allowing any disclosure of Client Personal Information by a subcontractor in response to a court order.

41. IPFGB will review complaints for indications of any unauthorised or unlawful Processing of Client Personal Information. Systems and processes are in place to address complaints concerning unauthorised use or disclosure of Client Personal Information by a subcontractor.

42. We will notify the Client promptly upon learning that a subcontractor has Processed Client Personal and Confidential Information for any purpose other than providing Client-related services to the Client or its suppliers. IPFGB will demonstrate that the Client has been notified when subcontractors have used Client Personal Information for unauthorised purposes.

43. IPFGB will promptly take action to mitigate any actual or potential harm caused by a subcontractor's unauthorised or unlawful Processing of Client Personal and Confidential Information. We will demonstrate that appropriate action has been taken when subcontractors have used Client Personal and Confidential information for unauthorised purposes or disclosed Personal or Confidential Information.

44. Before accepting any Personal Information from a third party, verify that the data collection practices of a third party are consistent with the GDPR. Documented processes are in place to verify third parties.

45. IPFGB will confirm that the only Personal Information collected from third parties is that required to perform the service(s) procured by Client and in accordance with third-party data collection practices. Documented processes are in place to limit the transfer of Client Personal Information from third parties to only that needed to perform the contracted services.

Quality:

46. IPFGB will maintain the integrity of all Client Personal Information, ensuring it remains accurate, complete and relevant for the stated purposes for which it was Processed. Information is validated when collected, created and updated. Systems

and processes are in place to verify accuracy on an on-going basis and correct as necessary.

47. IPFGB will ensure that the minimum amount of Personal Information required to fulfil the stated purpose is collected.

Monitoring and Enforcement:

48. IPFGB will immediately notify the Client upon becoming aware of a Personal Information Breach or security vulnerability related to IPFGB's handling of Client Personal or Confidential Information.

49. IPFGB will not issue any press release or any other public notice that relates to a Personal Information Breach involving Client Personal or Confidential Information without getting Client approval unless expressed by law or regulatory requirement.

50. IPFGB will implement a remediation plan and monitor the resolution of Personal Information Breaches and vulnerabilities related to Client Personal Information to ensure that appropriate corrective action is taken on a timely basis.

51. IPFGB has an established formal complaint process for responding to all data protection complaints involving Client Personal Information. We have a documented process to handle complaints and notify the Client.

52. IPFGB will notify the Client of any complaints related to Client Personal Information. We will maintain records of complaints that demonstrate timely response.

53. IPFGB will record and respond to all data protection complaints related to Client Personal Information in a timely manner unless given specific instructions by Client. Upon request, provide the Client with documentation of resolved and unresolved complaints. We will retain documentation of open/closed complaints.

54. IPFGB will take the nature of supplier information into account and assist the Client in ensuring compliance with its obligations under applicable law (including but not limited to data security, Personal Information Breach, data protection impact assessments and consultation with government, regulatory and supervisory authorities).

55. IPFGB will make available to the Client all information necessary to demonstrate compliance with the obligations under applicable law and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by Client.

Security:

56. INFORMATION SECURITY PROGRAM. IPFGB will establish, implement, and maintain an information security program that includes policies and procedures, to protect and keep secure Client Personal and Confidential Information in accordance with good industry practice and as required by applicable law. IPFGB's security program will meet the standards captured below, requirements 56 -76. IPFGB will use VeraCrypt encryption software on all computers on which Client Personal and Confidential Information is stored. All mobile phones will be protected by passwords or other security measures.

57. Perform annual network security assessments that include:

    • Review of major changes to the environment such as a new system component, network topology, firewall rule, etc.
    • Conduct vulnerability scans.

58. IPFGB will define, communicate and implement a mobile device policy that secures and limits use of Client Personal or Confidential Information accessed or used on a mobile device. Provide a mobile device policy and demonstrate use where Client Personal or Confidential Information data handling requires use of a mobile device.

59. All Assets used to support the delivery of Client's services must be accounted for and have an identified owner. IPFGB is accountable for maintaining an inventory of these information assets; establishing acceptable and authorized use of the assets; and providing the appropriate level of protection for the assets throughout their life cycle.

    The Inventory of these assets to include:
    - Location of device
    - Data Classification of the data on the asset
    - Record of asset recovery upon termination of employment or business agreement
    - Record of disposal of data storage media when its no longer required.

    Review the Inventory of device assets used to support delivery of Client services.

60. Establish and maintain access rights management procedures to prevent unauthorized access to Client Personal or Confidential Information under supplier control.
    The plan to include:
    • Access control procedures
    • Identification procedures
    • Lockout procedures after unsuccessful attempts
    • Password reset as often as necessary but no longer than every 70 days.
    • Provide user awareness of protecting their authentication credentials.
    • Robust parameters for selecting authentication credentials.
    • Deactivation of user accounts on employment termination within 48 hours.
    o Includes internal/external access, media, paper, technology platforms, and backup media.

    Establish a process to review user access to Client Personal and Confidential Information, enforcing the principle of least privilege:
    The process to include:
    • Clearly defined user roles
    • Procedures to review and justify approval of access to roles.
    • Procedures to remove user access to roles when access is no longer needed.

61. Define and automatically implement patch management procedures that prioritize security patches for systems used to process Client Personal and Confidential Information, include:

    Be able to demonstrate that security patches are applied.

62. Install anti-virus and anti-malware software on equipment connected to the network used to process Client Personal and Confidential Information, including but not limited to servers, production and training desktops to protect against potentially harmful viruses and malicious software applications. Update the anti-malware definitions daily or as directed by the anti-virus/anti-malware supplier.

63. Monitor information systems in use within the company network where Client Personal or Confidential Information is handled—for intrusions and other unauthorized activity.
Demonstrate effectiveness of monitoring systems, supporting documentation is available.

64. Promptly communicate Investigation results from incident response to senior management and to Client. Systems and processes must be in place to communicate incident response investigation results to Client.

65. System administrators, operations staff, management and third parties must undergo annual security training.

Establish a security training program that includes:
• Annual training for incident response.
• Simulated events and automated mechanisms to facilitate effective response to crisis situations.
Incident prevention awareness such as risks associated with downloading malicious software.

66. IPFGB will ensure that backup planning processes protect Client Personal and Confidential Information from unauthorized use, access, disclosure, alteration and destruction. Document response and recovery procedures detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level based on management approved information security continuity objectives. Define and implement procedures to periodically back up, securely store, and effectively recover critical data.

67. Establish and test business continuity and disaster recovery plans.

A disaster recovery plan must include the following
• Defined criteria to determine if a system is critical to the operation of IPFGB's business
• List critical systems based on the defined criteria that must be targeted for recovery in the event of a disaster.
• Defined disaster recovery procedure for each critical system that ensures an engineer who does not know the system could recover the application in under 72 hours.
Annual (or more frequent) testing and review of disaster recovery plans to ensure recovery objectives can be met.

68. Authenticate the identity of an individual before granting that individual access to Client Personal or Confidential information.

69. IPFGB will protect Client Personal and Confidential Information in transit across networks with encryption using Transport Layer Security (TLS) or Internet Protocol Security (IPsec). These methods are described in the NIST 800-52 and NIST 800-

57; an equivalent industry standard can also be used. IPFGB will require delivery of any Client Personal Information transmitted via unencrypted means.

70. All IPFGB client devices (laptops, workstations, etc.) that will access or handle Client Personal or Confidential Information will employ disk based encryption.

71. Systems and procedures will be in place to encrypt Client Personal information, noted below, at rest (when stored) using current industry standards such as that described in the NIST 800-111 standard.
Encrypt the following types of Client Personal Information at rest:
• credential data (e.g. username/passwords)
• payment instrument data (e.g. credit card and bank account numbers)
• government issued identifier data (e.g, social security or driver's license numbers)

72. When processing credit cards on Client's behalf, adhere to the applicable credit card handling standards per card issuer.

73. IPFGB will store physical assets of Client Personal and Sensitive Information in an access-controlled environment. Systems and processes are in place to manage physical access to digital, hard copy, archival, and backup copies of Client data. Chain of custody is tracked for the movement and destruction of physical media containing Client data.

74. Anonymize all Client Personal Information used in a development or test environment. Client Personal Information will not be used in development or test environments; when there is no alternative, it must be sufficiently anonymized to prevent identification of Data Subjects or misuse of Personal Information.