THE ASSOCIATION OF BRITISH INVESTIGATORS LIMITED
UK GDPR CODE OF CONDUCT
FOR INVESTIGATIVE & LITIGATION SUPPORT SERVICES

USEFUL CONTACTS:

CODE OWNER

The Association of British Investigators Limited ("ABI")
Brentano Suite, Catalyst House, Centennial Park, Elstree WD6 3SY
T: 020 8191 7500
E: secretariat@theABI.org.uk

MONITORING BODY / BODIES

1) Security Systems and Alarms Inspection Board (SSAIB)
   7-9 Earsdon Road, West Monkseaton, Whitley Bay, Tyne & Wear NE25 9SX
   T: 0191 296 3242
   E: monitoring.body@ssaib.co.uk

   Pending accreditation as a Monitoring Body by the ICO

[APPROVED BY:

The Information Commissioner ("ICO") on 15th October 2024.

[VERSION INFORMATION:

This is Version 1.0 of the Code and is dated 15th October 2024

PUBLISHING AND COPYRIGHT INFORMATION:

Published by ABI 13th November 2024

Table of Contents

1. Introduction

1.1 The UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 introduced significant new requirements in relation to how operators in the UK Investigative & Litigation Support Services sector are required to handle Personal Data. It is important that businesses and the public have confidence in the Personal Data handling practices of the sector. The ABI has worked in consultation with ABI Members and other stakeholders to produce this voluntary data protection code of conduct for Investigative & Litigation Support Services (the "Code").

1.2 The Code is issued under Article 40 of the UK GDPR. Monitoring compliance with the Code is carried out by an impartial Monitoring Body or "MB", which has an appropriate level of expertise in relation to the subject-matter of the Code and is accredited for that purpose by the ICO. As at the date of publication of the first edition of the Code, the Security Systems and Alarms Inspection Board ("SSAIB") is the only MB, pending its approval by the ICO, for the purposes of monitoring compliance with the Code. The SSAIB also delivers certification of the BS102000/2018 standard, which is a code of practice for the provision of investigative services.

1.3 The purpose of the Code is to enable Code Members (as defined below) to demonstrate the satisfactory working knowledge of and compliance with specific areas of Data Protection Law in the provision of Investigative & Litigation Support Services. Verified adherence to the Code is intended to give confidence to users of Investigative & Litigation Support Services that Code Members have demonstrated compliance with key aspects of Data Protection Law and a high standard of data protection and accountability in those key areas, to the satisfaction of an independent MB.

1.4 The Code builds on the existing standards and criteria required for ABI Membership. Code Members are not required to be ABI Members and Code Membership is available to any sector agency that meets the Code Member Criteria, whether affiliated to the ABI or not. Code Members must meet the

Code Member Criteria set out in Appendix I of this Code. ABI Members will be exempt from some of the Code Member Criteria which are already demonstrated by their full membership of the ABI.

1.5 The ABI has worked with the ICO to ensure the Code meets the requirements of Data Protection Law. Nothing in the Code affects the powers of the ICO in respect of the enforcement of Data Protection Law. For more information about codes of conduct generally, please see the ICO's guidance and register of UK GDPR codes of conduct [1].

1.6 The Code is in three parts, plus Appendices. Part A explains the scope, objectives, background, benefits and added value of the Code. Part B delivers guidance on the Key Issues on which this Code focuses as set out in paragraph 4.1 of Part A. Part C explains how the Code is managed, compliance is monitored and infringements dealt with. The Appendices provide details of the Code Member Criteria (Appendix I), a template DPIA (Appendix II), and further guidance on the lawful basis of legitimate interests and the requirements for consent (Appendix III).

1.7 The Code uses the term "must" where a Code Member's compliance is required, usually where it is a legal obligation. Where the Code uses the term "should", the requirement is not an absolute obligation but is what a Code Member is expected to do to comply effectively with the law. This means that a Code Member should comply with the requirement unless there is a good reason not to. If a Code Member chooses to take a different approach, it must be able to demonstrate that the alternative approach complies with the law. The Code uses the term "could" in relation to an option or example that a Code Member might consider to help it to comply effectively with the Code Member Criteria and Data Protection Law, but there are likely to be alternative means of compliance.

1.8 The UK GDPR is silent on the question of whether a code of conduct can recommend practices which are beyond those required by the law but there appears to be no barrier to this as long as it is clear which requirements of the

code of conduct are legal obligations and which are not legal obligations but represent good practice.

1.9 The ABI is a voluntary individual members' professional body. Its membership criteria are available on its website [2].

2. Definitions

ABI Member	Full member of the ABI, and "ABI Membership" shall be construed accordingly.
Appropriate Policy Document or APD	A document outlining a Code Member's compliance measures and retention policies in relation to the processing of Special Category Data and Criminal Offence Data.
BS102000	Code of practice and BSI standard for the provision of investigative services.
Client	The natural or legal person, public authority, agency, or other body requesting the Code Services.
Code Member	As defined in Part A paragraph 3.1 below. References to Code Members may include prospective Code Members as the context requires and permits and "Code Membership" shall be interpreted accordingly.
Code Member Criteria	The specific measurable controls set out in Appendix I against which the MB will assess compliance on application and within the review and monitoring process.
Code Review	The review of the Code by the ABI and MB in accordance with Part C paragraph 41 of the Code.
Code Review Framework	A framework for the review of the Code agreed between the ABI and MB in accordance with part C paragraph 41.1.
Code Services	Investigative and Litigation Support Services performed by the Code Member.
Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Please refer to Part B paragraph 10 of the Code for detailed discussion about the role of Controllers.
Criminal Offence Data	Personal Data relating to criminal convictions and offences or related security measures. It includes information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings. It may

	include information about an offence committed or alleged to have been committed, including sentencing, and related measures, such as bail conditions, community orders and their terms; or data relating to the absence of convictions. See Part B, paragraph 28 for further information.
Data Protection Officer or DPO	A data protection officer designated by a Controller or Processor pursuant to Article 37 of the UK GDPR.
Data Protection Law	All applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), each as amended.
Data Protection Principles	The principles set out in Article 5 of the UK GDPR.
DPA	The Data Protection Act 2018 as amended.
DPIA	A data protection impact assessment which is a risk assessment required under Data Protection Law to be carried out when processing of Personal Data is likely to result in a high risk to the rights and freedoms of Individuals. Please refer to Part B, paragraph 20.
General Business Administration	Internal business processing, such as Client onboarding, Client anti money laundering checks, Client verification, payroll, internal human resources and other administrative processes.
Individual	Any living individual who can be identified, directly or indirectly, in particular via an identifier such as a name, an identity number, location data, an online identifier or via one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.
Investigations	As defined in the Private Security Industry Act 2001 Schedule 2 s4(1) as: "any surveillance, inquiries or investigations that are carried out for the purpose of— (a) obtaining information about a particular person or about the activities or whereabouts of a particular person; or

	(b) obtaining information about the circumstances in which or means by which property has been lost or damaged" and in this Code "Investigative" and "Investigative Services" shall be interpreted accordingly.
Invisible Processing	Invisible processing occurs when Personal Data is obtained from somewhere other than directly from the Individual themselves, and the Individual is not provided with the privacy information set out in Article 14 UK GDPR. See lawful basis – additional important considerations in Part B paragraph 27 for further explanation and examples.
Joint Controllers	Two or more Controllers who jointly decide the purposes and means of processing.
Key Issues	The key issues which the Code will address as set out in Part A paragraph 4.1.
Legitimate Interest Assessment or LIA	A legitimate interest assessment as explained in Part B paragraph 31.
Litigation Support Services	Services, including Investigations, rendered by a Code Member to legal professionals in contentious scenarios in contemplation of, or during, legal proceedings.
Monitoring Body or MB	The body accredited by the ICO as having the appropriate level of expertise in relation to the subject-matter of the Code to carry out the monitoring of compliance with the Code. See Part C of the Code for further information about the role of the MB.
Personal Data	Information relating to an identified or identifiable Individual.
Principal	A principal of the Code Services business which may include an individual who has the ability to influence decisions relating to that business **and** has significant control over that business's data processing activities. The business may consist of one or more Code Members.
Processor	A natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of the Controller. Please refer to Part B, paragraph 11.

Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an Individual, data concerning health or data concerning an Individual's sex life or sexual orientation. Please refer to Part B, paragraph 29 for further information.
SSAIB	The Security Systems and Alarms Inspection Board www.ssaib.org, which is the first certification body to achieve product certification (under the UK Accreditation Service https://www.ukas.com/) for BS102000 (*code of practice for the provision of investigative services*).
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

PART A – EXPLANATORY STATEMENT

3. Scope

3.1 The Code applies to any business engaged in the provision of Code Services that:

- is affiliated to the ABI by membership of an Individual as Principal of the business; or
- is not an ABI affiliated business but the MB determines that the business's designated Principal meets the Code Member Criteria; and
- has demonstrated, to the satisfaction of the MB, competence, good practice, and compliance with Data Protection Law in accordance with the Code and the Code Member Criteria; and
- has been granted "Code Member" status by the MB and added to the ABI's register of Code Members [3].

3.2 The Code applies to the processing of Personal Data by a Code Member as a Processor, Controller, or Joint Controller for the purpose of providing Code Services. This may include but is not limited to the processing of Personal Data relating to enquiry subjects, witnesses, informants, or their affiliates.

3.3 The Code is designed to provide enhanced assurance and reduce the data protection-related risks where Code Members undertake Code Services. **The Code does not cover all of a Code Member's obligations under Data Protection Law. For example, it does not address the data protection responsibilities of Code Members in carrying out General Business Administration. For details of the key data protection compliance issues covered by the Code, please see paragraph 4.1.**

3.4 The Code does not address Code Members' responsibilities under any relevant sectoral legislation. The Code Member must make a declaration of compliance with such other legislation as part of its application for Code Member status.

Key requirement		
Code Requirement		*Supporting Evidence*
Legislative Compliance	*A legislation declaration confirming the Code Member's compliance with the applicable legislation.*	*Code Members must review all relevant aspects of applicable legislation before making the legislation declaration.* *The declaration wording will be provided by the MB.*

3.5 The Code cannot be relied upon by Code Members for the purposes of Article 46(2)(e) of the UK GDPR as an appropriate safeguard in respect of the transfer of Personal Data outside of the UK .

4. Code objectives

4.1 The purpose of the Code is to provide sector-specific guidance to assist Code Members with Data Protection Law compliance. The Code also provides for the monitoring of the compliance of Code Members against the Code Member Criteria. As stated in Part A paragraph 3.3 above, the Code does not cover all aspects of Data Protection Law and focuses on the key issues that are specific to the Investigative & Litigation Support Services sector in which Code Members operate. The Code covers the following "Key Issues" in relation to Code Services:

- The roles and responsibilities of Code Members when acting as Controllers, Joint Controllers, or Processors in respect of their obligations under Data Protection Law when processing Personal Data. A Code Member must determine its role when processing Personal Data and should take reasonable steps to ensure that any third party it is dealing with agrees to comply with its obligations under Data Protection Law.
- The requirement under Article 35 of the UK GDPR to conduct an assessment of the impact of the envisaged processing operations (a data protection impact assessment or "DPIA") on the protection of Personal Data where the processing of Personal Data is likely to result in a high risk to the rights and freedoms of Individuals. Code Members must determine when a DPIA is required, complete it, and take its conclusions into account

prior to commencing processing, with such processing contingent on the conclusions of the DPIA.

- Identification of the lawful basis for the processing of Personal Data. Code Members must establish and appropriately document a lawful basis for data processing under Article 6 (and, where processing Special Category Data or Criminal Offence Data respectively, satisfy the relevant conditions under Article 9 or Article 10) of the UK GDPR, while ensuring that the Personal Data is processed lawfully, fairly and in a transparent manner in accordance with Article 5.
- The carrying out of an assessment (a legitimate interests assessment or "LIA") to determine whether the Code Member can rely on its legitimate interests or those of a third party under Article 6(1)(f) of the UK GDPR as the lawful basis for any processing. See further information at Part B paragraph 32 below.
- Consent to share Personal Data in trace/locate case example. See further information at Part B paragraph 33 below.

4.2 The Code provides examples of the application of the Key Issues set out in Part A paragraph 4.1 above, and a template DPIA (at Appendix II).

5. Background

5.1 Investigators in the private sector & Litigation Support Services providers whose activities frequently require the processing of Personal Data have faced challenges when meeting the requirements of Data Protection Law. Investigators have also historically been subject to enforcement action by the ICO for non-compliance with Data Protection Law. The following examples explain some of these challenges. Further examples are found in Part B:

- A Code Member may find it challenging to manage Client expectations while still meeting the applicable Data Protection Law requirements in respect of both their own and their Client's roles and responsibilities. An instructing Client may not understand a Code Member's role in relation to certain processing activities. The Code Member must ensure that it

complies with its obligations as a Controller, Joint Controller or Processor, as applicable. Where necessary, the Code Member may also need to explain its role and its Data Protection Law obligations to its Client. It should also explain any consequences of complying with these obligations, for example the impact on the timescales or costs of delivering the Code Services in accordance with the Client's instructions.

- Investigators in the private sector & Litigation Support Services providers are regularly instructed by lawyers to assist in contentious matters involving court proceedings such as civil or criminal litigation or other Code Services. This may involve processing Personal Data that is subject to legal professional or litigation privilege, or that is otherwise held subject to a duty of confidence by a legal adviser. Certain exemptions apply to such Personal Data, in particular exemptions from the Individual's right to be informed and right of access, and from the Data Protection Principles insofar as they relate to these Individual rights. As, in these circumstances, Code Members are likely to be processing Personal Data in respect of which Individuals' rights could be limited, it is particularly important for them to be able to demonstrate that they are doing so in a way that is compliant with Data Protection Law [4]. Code Members should be aware that whether these exemptions apply is context specific and outside the scope of the Code. See Part B paragraph 27 below (Invisible Processing) for further guidance.
- Code Members must make their Clients aware that the processing of Personal Data in the carrying out of Code Services must be compliant with Data Protection Law, despite the challenges such as those set out above. **They must decline instructions which they are unable to carry out compliantly and in accordance with Data Protection Law.**

6. Benefits

6.1 Some of the key benefits of Code Membership are:

- familiarity with the Key Issues within the scope of this Code and clarity on how to address them within a Code Services context;

- demonstration by the Code Member of having received training on compliance with specific areas of Data Protection Law within the scope of the Code Services;
- a clearer understanding of the Data Protection Principles and how they apply to Code Members;
- credibility in the eyes of potential Clients who are looking at the Code Member's credentials in relation to Code Services;
- for some, the advantage of being an early adopter of the Code as more service providers in the Investigative & Litigation Support Services sector apply for Code Member status;
- instilling confidence in Individuals that their rights will be respected in the processing of their Personal Data for Code Services purposes; and
- the fact that the ICO will take into account: (i) Code Member status; and (ii) any action taken by the MB in respect of a breach of Data Protection Law, if it is considering enforcement action against the Code Member for any breach of Data Protection Law [5].

6.2 The ABI considers that these factors will also contribute to greater awareness of the need for general compliance with Data Protection Law (as well as the specific compliance with the Code) within the Investigative & Litigation Support Services sector.

7. Added value

7.1 The processing of Personal Data in the delivery of many Code Services carries a degree of risk of harm to Individuals [6]. The related risks can have wide-ranging impact including financial and emotional harm and may have a lasting impact on the lives of the Individuals affected. Code Membership is intended to increase the accountability of Code Members to such Individuals by demonstrating their compliance with key requirements of Data Protection Law when carrying out Code Services.

7.2 The Code increases the accountability of Code Members to the public by requiring them to apply codified guidance and good practice in relation to the

key data protection issues affecting the sector, as set out in the Code. It also provides a framework for independent monitoring and annual compliance audits by the MB.

7.3 Public awareness of the Code may result in Code Members receiving a higher volume of instructions from lawyers, insurers, financial services organisations, commerce, private Clients and third parties in other sectors on the basis that they operate in accordance with a code of conduct which has been approved by the ICO. As mentioned in Part A paragraph 6.1, the ICO will take into account Code Membership status, and compliance with the Code, as an aggravating or mitigating factor (as applicable) when considering enforcement action against a Code Member[7].

PART B – CODE OF CONDUCT CORE REQUIREMENTS

8. Introduction

8.1 Part B of the Code explains the key requirements as they apply to Code Members. It provides guidance and examples on the Key Issues of Data Protection Law outlined in Part A paragraph 4.1. These are:

- Roles and responsibilities (see Part B paragraphs 9 – 19 below).
- DPIAs (see Part B paragraphs 20 – 24 below).
- Lawful basis (see Part B paragraphs 25 – 30 below).
- LIAs (see Part B paragraphs 31 – 32 below)
- Consent to share Personal Data in trace/locate case example (see Part B paragraph 33 below).

8.2 To achieve Code Member status, an applicant Code Member must be able to demonstrate its compliance in the key areas covered by the Code, by fulfilling the Code Member Criteria and requirements set out in Appendix I to the ongoing satisfaction of the MB.

9. Roles & responsibilities

Key requirement		
Code Requirement		*Supporting Evidence*
Roles and Responsibilities	The Code Member understands its role and responsibilities and documents and communicates them to its Clients accordingly. Code Members must understand the roles and responsibilities in respect of the data processing which they undertake. In accordance with Data Protection Law, and using the guidance in the Code, a Code Member must be able to establish if it is acting as a Processor, Controller, or a Joint Controller in relation to specific data processing.	Evidence (at the discretion of the MB) that the Code Member has documented and communicated to its Client the roles and responsibilities in respect of the data processing undertaken in the delivery of Code Services. This could be evidenced for example by providing a copy of the Client engagement letter and/or contract.

9.1 The Code Member must, prior to taking on a new instruction, consider the Personal Data likely to be processed in carrying out the Code Services and establish the Code Member's role in processing Personal Data as a Controller, Joint Controller or Processor. This is fundamental to understanding its responsibilities under Data Protection Law and is a question of fact requiring careful consideration of the relevant processing. A Code Member or its Clients cannot choose their respective role and responsibilities – they will be determined by the facts of the processing. The Code Member must explain its role and responsibilities to the Client in communications, for example in its engagement letter or proposal for Code Services, before accepting a Code Services assignment or instructions.

9.2 A Code Member must take care when acting as a Controller and Processor for the same Personal Data to ensure it is clear which processing activities it is a Controller for and those for which it is a Processor. This will allow the Code Member to comply with the relevant obligations, both under Data Protection Law and its Client agreements.

9.3 If the Code Member fails to properly understand its role and responsibilities in the context of the processing it will be very difficult for the Code Member to comply with Data Protection Law or give Clients confidence in its Personal Data processing abilities and compliance [8].

10. Controller and Joint Controller

10.1 Data Protection Law defines a "Controller" as a natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines both the purposes and means of the processing of Personal Data. A Controller can be a company or other legal entity (such as an incorporated partnership, incorporated association, or public authority), or an Individual operating in a commercial capacity such as a sole trader, partner in an unincorporated partnership, or self-employed professional, e.g. a barrister [9].

10.2 Controllers make decisions about Personal Data processing activities. They exercise overall control of the Personal Data being processed and are also

ultimately in charge of and responsible for the processing. Controllers can determine the purposes and means of processing alone, or jointly with others (a "Joint Controller"). The purpose is the 'why' and the means is 'how' Personal Data is processed.

10.3 A Client instructing the Code Member to perform Code Services for purely personal or household activity may not be subject to UK GDPR and is unlikely to have data protection responsibilities. In these circumstances, the Code Member is likely to be the Controller, rather than the Processor or Joint Controller for this processing. It is good practice for the Code Member to verify the identity of the Client and its case scenario and purpose.

10.4 Where a Code Member is engaged to provide its services (other than in the circumstances above), the Code Member may be a Joint Controller for the purposes of Data Protection Law. This is because the Client has influenced why and how the Code Member collects and uses Personal Data by selecting the Code Member and requesting its services, and the nature of Code Services is such that the Code Member will be making the operational decisions as to what Personal Data is required to be processed and how it will be processed.

10.5 Code Members often need to process Personal Data in a manner not envisaged in their original instructions and a situation may change at such a pace that the Code Member cannot reasonably revert to the Client for detailed processing instructions. The ABI has found that in such situations, a Code Member is frequently required to make decisions about the processing of Personal Data that could place it into the role of a Controller, either solely or jointly with the instructing Client.

10.6 In particular, if the Code Member makes any of the following decisions, it is likely that it is a Controller or Joint Controller because it will be determining both the purpose and the means of the processing:

- whether to collect Personal Data in the first place;
- the lawful basis for doing so;
- the purpose/s the Personal Data is to be used for;

- which types of data will be collected and processed;

  Example: A Code Member may use details of an Individual provided by a Client to search a database, such as the Individual's name, date of birth and/or address. The Code Member is likely to be acting as a Processor in relation to this Personal Data if it is following the Client's detailed instructions. The processing of this Personal Data must be covered by a data processing agreement between the Code Member and its Client incorporating the mandatory clauses required under Article 28(3) of the UK GDPR. If, as part of the same search, the Code Member identifies other Personal Data not covered by the Client's original instructions and Article 28(3) agreement such as the Individual's email address, phone number, previous address and social media profile, and decides how and why to process that additional information in the delivery of Code Services to the Client, the Code Member may be acting as Controller rather than Processor of that additional Personal Data.
- which Individuals to collect data about;

  Example: When searching for an Individual, the Code Member may identify other Individuals' (cohabitees, previous occupants, other occupants, business associates) Personal Data. If the Code Member exercises its professional skill and judgement in deciding whether those other Individuals' Personal Data is processed to provide the relevant Code Services, this may establish the Code Member as a Controller when processing that Personal Data.
- what to tell Individuals about the processing;
- whether the data should be disclosed and to whom;

  Example: When searching for the beneficiary of an estate, a Code Member may need to decide whether to disclose the instructing Client's Personal Data as part of the search. The Code Member is likely to be acting as Controller of that Personal Data if the disclosure was not covered by the Client's initial instructions and Article 28(3) agreement.
- whether and for how long the data will be stored or whether to make non-routine amendments to the data. If the Code Member makes these

decisions, it is likely to be a Controller. If the Code Member acts in accordance with a Controller's (the Client's) instructions on retention and deletion and the making of amendments, it is likely to be a Processor. However, the circumstances of some Code Services may mean that these decisions are left to the Code Member.

Example: Almost all Personal Data processed by a Code Member for the purposes of Client engagements may later be admissible as evidence in litigation. The Code Member may therefore decide that a specific, longer retention period than the period covered by the Client's instructions is appropriate to meet any potential evidential responsibilities and legal obligations that might arise if a claim is reasonably in prospect. In making this decision the Code Member would be likely to be acting as a Controller.

- how to respond to requests made in line with Individuals' rights.

  Example: Where the Code Member makes decisions in relation to dealing with a subject access request from an Individual it is likely to be acting as a Controller.

10.7 A Code Member and its Client will be Joint Controllers where they jointly determine the purpose and the means of processing. This would normally be the case either because the Client has influenced the processing by selecting the Code Member and agreeing the specific services or tasks, so that it is involved in the decisions about the purpose and means of processing. Or, because the Client has worked with the Code Member to decide what Personal Data will need to be within scope, what it will be used for and how it will be processed.

10.8 Where Code Members are Joint Controllers with their Clients, they must have clear communication with their Clients as to the roles and responsibilities of each party. This must include who will carry out which Controller obligation, including how they will comply with Individuals' rights, Individual access

requests and transparency obligations. This should be set out in the engagement letter between the Client and the Code Member.

10.9 Joint Controllership by the Code Member and its Client may arise where the Code Member has a significant level of discretion about what and how to investigate in the conduct of Code Services.

10.10 An example of processing activities where a Code Member is likely to be a Joint Controller alongside the Client is set out at **Part B** paragraph 18 below.

10.11 If a Code Member is a company with employees, the company will be the Controller rather than its employees.

11. Processor

11.1 Data Protection Law defines a "Processor" as a legal person or entity which processes Personal Data on behalf of the Controller. A Processor must only process Personal Data in line with a Controller's instructions (unless otherwise required by law). If the Code Member is to act as a Processor rather than Controller for one or more processing activities, it must establish that it is not determining the purposes and means of those processing activities and is only processing Personal Data on behalf of and as instructed by the Controller. If the Code Member acts outside of its Client's instructions and/or processes Personal Data for its own purposes, it will step outside of its role as a Processor and become a Controller in respect of that processing.

11.2 A Code Member may be a Processor and still have a certain degree of discretion and make operational day-to-day decisions as to how the processing is accomplished, provided the instructions and/or service description contain enough detail so that the Client is able to verify and be responsible for the Code Member's compliance with Data Protection Law. For example, the Code Member, acting as a Processor, may decide what systems will be used when processing Personal Data, or which specific sources to use to obtain Personal Data for the purposes of the processing if these are within the instructions, and those instructions have enough detail so that the Client can verify and evidence

compliance with Data Protection Law. A Processor may also be limited in the discretion it may exercise through specific restrictions in its agreement with the Controller. For example, the agreement may require a level of information security that prohibits printing of Personal Data. A Code Member must ensure that its processing of Personal Data as a Processor reflects its obligations under the Article 28(3) processing agreement it is a party to.

11.3 Code Members typically act as Controllers in respect of at least some elements of Code Services where at some stage of delivery of the Code Services, or in carrying out certain activities, they determine why and how Personal Data is processed. At other times the Code Member will act on instructions from its Client as to the purpose and the means of the processing, and so will be a Processor. Examples relevant to Code Members are set out at **Part B** paragraph 16 below.

11.4 In some situations, a Code Member may be Controller and Processor of the same Personal Data in the delivery of Code Services, where it is carrying out certain activities in relation to that data as Controller and other processing activities in relation to the same data as Processor. For example, the Code Member may retain Personal Data that it has processed for its Client as set out in the examples in **Part B** paragraph 16 below in advance of an annual quality assessment as part of a BS102000 and / or Code Membership audit. The Code Member would be acting as Controller in relation to the processing of the data for these purposes. A further example is set out at **Part B** paragraph 17 below.

11.5 If a Code Member is a company with employees working on an assignment in which the company's role is that of a Processor, the company will be acting as a Processor, rather than its employees.

12. Controller responsibilities

12.1 The obligations of Controllers (including Joint Controllers) are set out in Data Protection Law.

12.2 When the Code Member is acting as a Controller, it is the Code Member's responsibility to ensure that its processing, as well as any processing undertaken on the Code Member's behalf by a Processor, complies with Data Protection Law.

12.3 The Code Member as the Controller is responsible for the following under Data Protection Law:

- **Adherence to the Data Protection Principles.**
- **Rights of Individuals:** The Code Member must make sure that people can exercise their rights in respect of their Personal Data, including the rights of access, rectification, erasure, restriction, data portability, objection, and those relating to automated decision-making.
- **Security:** The Code Member must adopt the necessary technical and organisational security measures to ensure the security of Personal Data.
- **Selecting an acceptable Processor:** The Code Member must only work with a Processor who provides sufficient guarantees that it will implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Data Protection Law and ensure the protection of the rights of Individuals. It is the Code Member's responsibility to determine if its Processor is competent to process the Personal Data in accordance with Data Protection Law. In doing so the Code Member must consider the type of processing being carried out and the related risks to Individuals.
- **Processor agreement under Article 28(3):** The Code Member must enter into a legally binding agreement or other legal document with each of its Processors which includes the mandatory clauses listed in Article 28(3) of the UK GDPR.

- **Notification of Personal Data breaches:** The Code Member is responsible for notifying Personal Data breaches to the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of Individuals. The Code Member is also responsible for notifying affected Individuals if the breach is likely to result in a high risk to their rights and freedoms.
- **Accountability obligations:** The Code Member must comply with Data Protection Law accountability obligations, such as maintaining records, carrying out DPIAs (see Part B paragraph 20 below) and, when required, appointing a Data Protection Officer.
- **Co-operation with the ICO:** The Code Member as Controller is also obliged to cooperate with the ICO to help it perform its duties. The Code Member will also be subject to the relevant investigative and corrective powers of the ICO and may be subject to administrative fines or other penalties.
- **Data protection fee:** The Code Member must pay the ICO a data protection fee unless it is exempt.

12.4 The Controller is ultimately accountable for its own compliance and the compliance of its Processors [10].

13. Processor responsibilities

13.1 The responsibilities of a Processor are prescribed both under Data Protection Law and in the instructions from, and contracts with, the Controller.

13.2 A Code Member, who is a Processor, will have less autonomy and independence over the Personal Data it processes than the Controller of that Personal Data, as it must follow the Controller's instructions in relation to the Personal Data and its processing. However, the Processor has several direct legal obligations under Data Protection Law, and it will be subject to regulation by the ICO [11].

13.3 If the Code Member is a Processor, it has the following obligations:

- **Controller's instructions:** The Code Member can only process the Personal Data in accordance with instructions from a Controller (unless otherwise required by law).

- **Processor contract under Article 28(3) of the UK GDPR:** The Code Member must enter into a binding contract with the Controller. This must contain the compulsory provisions which are set out in Article 28(3) of the UK GDPR, including Processor obligations which the Code Member must comply with.
- **Sub-Processors:** The Code Member must not engage another Processor (i.e. a Sub-Processor/sub-contractor/agent) without the Controller's prior specific or general written authorisation.
- **Security:** The Code Member as Processor must implement appropriate technical and organisational measures to ensure the security of Personal Data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure, or access.
- **Notification of Personal Data breaches:** If the Code Member becomes aware of a Personal Data breach, it must notify the Controller without undue delay. Most Controllers will expect to be notified immediately, and may contractually require this, as the Controller will only have a limited time within which to notify the ICO and affected Individuals. The Code Member must also assist the Controller in complying with its obligations in relation to Personal Data breaches.
- **Notification of potential data protection infringements:** The Code Member must notify the Controller immediately if any of its instructions would lead to a breach of Data Protection Law.
- **Accountability obligations:** The Code Member must comply with certain Data Protection Law accountability obligations, such as maintaining records and, when required, appointing a Data Protection Officer.
- **Co-operation with the ICO:** The Code Member as Processor is also obliged to cooperate with the ICO to help it perform its duties. The Code Member will also be subject to the relevant investigative and corrective powers of the ICO and may be subject to administrative fines or other penalties.
- **Additional contractual obligations:** As well as the terms prescribed under Article 28 (3) of the UK GDPR, a Code Member who is a Processor may also be subject to additional obligations under its contract with the relevant

Controller. For example, the Controller may instruct the Code Member to apply specific security measures commensurate with ISO27001 for certain processing.

13.4 If the Code Member wishes to use a Sub-Processor, it must obtain the Controller's written authorisation [12]. The authorisation can be specific or general. Specific authorisation means the Controller must approve the particular Sub-Processor for the particular processing operation in question. General authorisation means:

- the Controller pre-approves a list of potential Sub-Processors; or
- the Controller approves a list of criteria that the Code Member can use to select and appoint a Sub-Processor, for example that the Sub-Processor is also a Code Member and/or verified member of the ABI.

13.5 If the Code Member has general authorisation, it must inform the Controller if it wishes to make any changes to the list of possible Sub-Processors or criteria for choosing a Sub-Processor and give the Controller the opportunity to object.

13.6 The Code Member must send the Controller details of any proposed changes in writing, setting out the date by which the Controller should raise any objections. If it has any objections, the Controller must also respond in writing and explain its reasons.

13.7 If the Code Member has written authorisation, it may appoint the Sub-Processor but must put in place a contract with the Sub-Processor. The terms of the contract with the Sub-Processor that are required under Article 28(3) must offer an equivalent level of protection of the relevant Personal Data as those in the Article 28(3) Agreement between the Code Member and the Controller.

13.8 Overall control of the processing will remain with the Controller, but the Code Member Processor will be liable to the Controller for the Sub-Processor's compliance.

13.9 A Processor must assist the Controller with:

- its obligations to respond to requests from Individuals exercising their rights under Data Protection Law;
- compliance with its obligations concerning security;
- notification to the ICO and to affected Individuals of Personal Data breaches where required; and
- the carrying out of a Data Protection Impact Assessment, where required, and if relevant consultation with the ICO when the DPIA outcome reveals a high risk that cannot be sufficiently mitigated so that there remains a residual high risk.

13.10 When the processing ends, a Processor must delete or return all Personal Data to the Controller in accordance with the Controller's instructions unless further retention is legally required.

13.11 A Processor may be contractually liable to the Controller if it fails to meet the terms of its contract with the Controller.

14. Joint Controller responsibilities

14.1 **Obligations:** Where the Code Member is acting as a Joint Controller, it must set out in writing, for example in a contract or engagement letter, which of them will carry out which Controller obligations under Data Protection Law. Joint Controllership does not necessarily mean equal responsibility for the processing. To decide an appropriate allocation of responsibilities, Joint Controllers should take into account factors such as who is competent and, in a position, to effectively ensure Individuals' rights, and to comply with the applicable obligations under the UK GDPR. However, regardless of any such arrangements, the data subject may exercise his or her rights under Data Protection Law in respect of and against each of the Controllers.

14.2 **Transparent arrangement**: Joint Controllers are not required to have a contract, but the Code Member must have a transparent written arrangement that sets out the agreed roles and responsibilities under Data Protection Law.

The main points of this arrangement must be made available to Individuals at the time when their Personal Data is obtained from the Individual or a third party. The Code Member should include this information in its privacy notice [13].

14.3 **Individuals' rights**: In particular, the Code Member must decide (and be transparent about) how it will comply with transparency obligations and Individuals' rights. The Code Member may choose to specify a central point of contact for Individuals. However, Individuals will remain able to exercise their rights against each Joint Controller. An Individual may claim compensation against any Joint Controller in respect of a breach of Controller obligations, unless that Joint Controller can prove it was not in any way responsible for the breach.

14.4 **Accountability to the ICO:** In addition, Joint Controllers are each fully accountable to the ICO for failure to comply with their responsibilities [14].

15. Controller examples

15.1 A Client requires the Code Member to identify and locate Individuals who are potential witnesses in relation to an ongoing dispute and provides detailed instructions as to how the Code Member must carry out its services. The Code Member is likely to be a Processor. If the Code Member subsequently contacts these witnesses to see if they are interested in the Code Member's services, it would be determining the purpose of this new processing, which in this case is business development. In this further business development example, the Code Member is acting as a Controller and must comply with the Controller obligations under Data Protection Law.

15.2 In a debtor locate case, the Client instructs the Code Member to identify a particular Individual by means of contact at the last known address. On speaking to the occupant, the Code Member becomes alert to the likelihood that the debt scenario is not as instructed (or envisaged in the Article 28(3) processor agreement with the Client) and the Code Member has detected possible fraud. To maintain momentum with the lead, the Code Member

pursues a different line of enquiry, following the "hot lead" without discussion with the Client. This involves the processing of the Personal Data of a previously unknown Individual for a purpose not envisaged in the instructions and in a manner not previously foreseen. The processing activities involved in following the hot lead may include pursuing enquiries at the address, potentially taking structured notes, running searches on the electoral roll and other related processing. Due to the Code Member's extensive discretion over the purpose and means of these processing activities, the Code Member is likely to be acting as Controller or Joint Controller. In this scenario care must be taken that the Code Member does not breach any agreement with the Client, particularly the terms required to be in place between a Controller and Processor under in Article 28(3) UK GDPR.

Where the Code Member is a Controller, rather than its employees:

15.3 An investigator is employed by a Code Member company. The investigator is part of a small team with specific responsibilities for data protection. The employee is asked by their line manager to obtain personal information from the open electoral register that is to be used to search for information relating to Client services. The Code Member is the Controller because it has bought the information to use as part of its business, so it determines the purposes and the means of the processing. Although the Code Member company gives the employee specific responsibilities as part of their role, neither the line manager, employee nor their team are Controllers of the personal information. Employees generally act on behalf of their employers under their direct authority.

16. Processor examples

16.1 A creditor Client instructs the Code Member to distribute several statutory demands. The Client provides addresses and names for the recipients. The Code Member has instructions to attend the address, verify the identity of the Individual who is the debtor, and to serve the statutory demand. The Code Member is not deciding on either the purposes or means of the processing of the Personal Data based on these facts. The only Personal Data it is processing

is the information provided in the Client's instructions and the processing is only for the purposes of delivering statutory demands. The instructions or service description must also cover how the Personal Data is to be processed by the Code Member (with enough detail so the Client can verify and evidence compliance with Data Protection Law). The Code Member and Client will need to ensure they have a written agreement in place between them pursuant to Article 28(3) of the UK GDPR that covers the Processor obligations set out in Part B paragraph 13.3 above.

16.2 A Client instructs the Code Member to verify address details provided to the Client. The Client would like the Code Member to search the electoral roll and confirm whether the addresses match and, where they do not, to note that the addresses do not match. The Client does not want the Code Member to perform further searches on the roll to locate the Individuals, or carry out its own Investigations, for example by searching other databases. The Code Member is likely to be a Processor for this activity. The instructions or service description must also cover how the Personal Data is to be processed by the Code Member, such as the IT software applications it uses to process Personal Data (with enough detail so the Client can verify and evidence compliance with Data Protection Law). The Code Member and Client will need to ensure they have a written agreement in place between them in accordance with Article 28 (3) of the UK GDPR that covers the Processor obligations set out in Part B paragraph 13.3 above.

Where a Code Member is a Processor while making some operational decisions:

16.3 A Client instructs the Code Member to verify a list of addresses provided to it as part of its business. The Client asks the Code Member to search the open electoral register and confirm whether the addresses match. The Client is the Controller because it is determining the purposes of the processing, which is to verify the list of addresses provided to its business. It is also determining the means, which is to search the electoral register to check whether the addresses match. The Code Member has a contract with its Client in accordance with the

requirements of Article 28(3) of the UK GDPR. However, within the terms of its contract, the Code Member uses IT software selected to help it search the details in the electoral register. The Code Member also decides how to store and send the results securely to the Client. It has a process for ensuring personal information is deleted or returned in line with its Client instructions. For the Code Member to be a Processor, the instructions or service description must cover this operational processing, including the IT software and storage applications it uses, with enough detail so the Client can verify and evidence compliance with Data Protection Law.

17. Controller and Processor of the same Personal Data example

17.1 The Code Member accepts instructions from a Client to locate the whereabouts of a debtor. The Code Member exercises discretion as to the scope and extent of its search, exercising overall control of the Personal Data and deciding what to process and why. The Code Member is therefore likely to be acting as a (Joint) Controller. Before the task is complete the Client transfers the debt to a debt purchaser, who takes over its responsibility for the processing. The debt purchaser writes to the Code Member with detailed instructions to undertake trace activities. The debt purchaser outlines what systems should be used and the specific Personal Data that should be obtained. It is likely that the Code Member will become a Processor for the processing activities involved in fulfilling the new instructions. The debt purchaser and the Code Member will need to enter into a written agreement pursuant to Article 28 (3) of the UK GDPR that covers the Processor obligations set out in Part B paragraph 13.3 above.

18. Joint Controller examples

18.1 A law firm acting for a road traffic accident victim Client requests the Code Member to interview the law firm's client to extract full details of the accident and parties involved, undertake initial investigative assessment and report on a recommended way forward on a potential compensation claim. The Code Member and law firm discuss what information to obtain, how to obtain it and what to use it for, and so are deciding the purpose and means of processing

jointly with the law firm.

18.2 A Client instructs a Code Member to provide Investigative Services, and provides broad details as to what the Client is to investigate. The engagement letter sets out the type of services which the Code Member provides. The Code Member decides how to approach the Investigation, the research to carry out, who to speak to, and the IT systems and software to use. The Client and the Code Member are likely to be Joint Controllers. The Code Member is making the detailed decisions about what Personal Data it collects, the specific purposes it uses it for, and how it carries out that processing. The Client has sufficiently influenced this processing by choosing the Code Member, given the information it has about the Code Services, and then issuing its albeit broad instructions. The engagement letter or contract should set out how the Controller responsibilities are allocated between the Client and Code Member.

19. Liabilities

19.1 An Individual can bring a claim directly against the Code Member. The Code Member can be held liable under Article 82 of the UK GDPR to pay compensation for any damage caused by its processing (including non-material damage such as damage caused by distress).

19.2 The ICO has enforcement powers in relation to both Controllers and Processors who fail to comply with their respective obligations under Data Protection Law.

19.3 **Controller liabilities:**

The Controller will be liable for any damage (and any associated claim for compensation payable to an Individual) if its processing activities infringe Data Protection Law where it is unable to prove that it was not in any way responsible for the event giving rise to the damage.

19.4 **Joint Controller liabilities:**

- If parties are acting as Joint Controllers, Individuals may exercise their rights against each Joint Controller.

- An Individual can bring a claim for compensation against any Joint Controller involved in processing in breach of Data Protection Law. The Joint Controller will be liable to that Individual for the entire damage unless it can prove it was not in any way responsible for the event giving rise to the damage. Any arrangement made between Controllers such as one apportioning liability is irrelevant for these purposes.
- Under Data Protection Law, if the Code Member is liable as a Joint Controller to pay compensation to an Individual but was not wholly responsible for the damage, it may be able to claim back from another relevant Controller or Processor the share of the compensation corresponding to the other's share of the damage. Alternatively, the Joint Controller contracts may set out how such compensation should be apportioned. The Code Member should seek independent legal advice on this.

19.5 **Processor/Sub-Processor liabilities**:

- The Code Member acting as Processor may also be contractually liable to the Controller for any failure to meet the terms of the Processor contract with its Client. This will of course depend on the exact terms of that contract.
- The Code Member will only be liable to Individuals for damage caused by processing in breach of Data Protection Law, if:
  - it has failed to comply with Data Protection Law as it applies specifically to Processors; or
  - it has acted outside of or against the Controller's instructions (and so is acting as a Controller).
- The Code Member will not be liable to an Individual if it can prove that it is not in any way responsible for the event giving rise to the damage.
- If the Code Member is required to pay compensation to an Individual but is not wholly responsible for the damage, under Article 82(5), it may be able to claim back from the Controller the share of the compensation for which the Controller was liable. Alternatively, the Processor contract may set out

how such compensation should be apportioned. The Code Member should each seek independent legal advice on this.

- If the Code Member is a Processor and uses a Sub-Processor to carry out processing on its behalf, it will be fully liable to the Controller for the Sub-Processor's compliance. This means that, under Article 82(5), if a Sub-Processor is at fault, the Controller may claim back compensation paid to an Individual, from the Code Member for the failings of its Sub-Processor (or even from the Sub-Processor directly). The Code Member may then claim compensation back from the Sub-Processor. Alternatively, the Sub-Processor contract may set out how such compensation should be apportioned. The Code Member should seek independent legal advice on this.
- If the Code Member is a Sub-Processor, it will be liable to Individuals for any damage caused by its processing only if it has not complied with Data Protection Law obligations imposed on Processors or acted contrary to the Controller's lawful instructions, relayed by the Processor, regarding the processing.
- A Sub-Processor may also be contractually liable to the Processor for any failure to meet the terms of their agreed contract. This will of course depend on the exact terms of that contract.
- Processors and Sub-Processors should seek their own legal advice on issues of liability and on the terms of the contracts made between Controllers and Processors and Processors and Sub-Processors.

20. Data Protection Impact Assessments

Key requirement		
Code Requirement		*Supporting Evidence*
Case Extracts - DPIAs	*Code Members must be able to determine when a DPIA is required and understand how to carry out the assessment.*	*A sample of up to three DPIAs which reflect the Code Member's range of services, redacted and anonymised, from live cases conducted by the Code Member during the previous 12 months. Or the review of a pre-existing DPIA, as required by the MB. The DPIAs provided should be fully up to date and compliant with the requirements of Article 35 of the UK GDPR.* *The MB will take into consideration that the business may not regularly carry out DPIAs.*

20.1 Code services frequently involve the processing of Personal Data in high-risk circumstances, not least because of the potential harm that might be introduced by the Code Member's activities and findings. This risk increases with certain investigative methods such as surveillance, which is potentially intrusive and likely to result in a high level of risk to Individuals whose Personal Data is being processed.

20.2 A DPIA is essentially a risk assessment. DPIAs are an important tool in identifying and mitigating risk and ensuring compliance with Data Protection Law. They are an "early warning system", which will help the Code Member identify and, through the appropriate action, prevent potential problems before they occur.

20.3 A DPIA may cover a single processing operation or a group of similar processing operations.

20.4 Where a Code Member is a Controller and the DPIA identifies a high risk that cannot be fully mitigated, the Code Member must consult with the ICO before the processing takes place.

21. When is a DPIA required?

21.1 As a matter of good practice, prior to any processing taking place, a Code Member should consider whether a DPIA is needed.

21.2 A DPIA must be carried out before the processing of any Personal Data in any case likely to result in a high risk to the rights and freedoms of Individuals under Data Protection Law. A single DPIA may be sufficient to cover high risk processing in a number of similar cases or cases involving similar processing.

21.3 It is the Controller's responsibility to undertake the DPIA, so the Code Member's duties will vary depending on its role. If it is acting as a Processor of Personal Data in relation to Code Services, it will have a duty to assist the Controller with the DPIA, but not to undertake a DPIA itself.

21.4 Code Member activities involve several types of processing that may carry sufficient risk to require a DPIA and may also be considered particularly intrusive.

21.5 A DPIA will be required in any event where the Code Member, as Controller, intends to process Special Category Data (under Article 9(1)), or Criminal Offence Data (under Article 10(1)) or where children's Personal Data is involved.

21.6 A DPIA will consider the level of risk. Under Data Protection Law it is clear that in order to assess whether something represents a "high risk" to the rights and freedoms of Individuals, the Code Member needs to consider both the likelihood and severity of any potential harm. "Risk" implies a more than remote chance of some harm. "High risk" implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two. Assessing the likelihood of risk in that sense is part of the job of a DPIA. Some examples of activities in respect of which Code Members must consider the likelihood of harm occurring are:

- denial of a service (product, opportunity, or benefit) as a result of automated decision making – for example, due diligence services that

could result in the Individual being declined employment or other benefit;

- combining, comparing, or matching Personal Data – where obtained from multiple sources, which could for example be used by the Code Member in almost any case including fraud prevention or detection;
- Invisible Processing – where the Code Member processes Personal Data that has not been obtained directly from the Individual and, where the information was collected without providing any privacy information required by Article 14 of the UK GDPR. Processing in this way could mean that an affected Individual is prevented from exercising their rights. It is only permitted where the Controller considers compliance with Article 14 would prove impossible, involve a disproportionate effort or make the achievement of the objectives of the processing impossible (or seriously impair them). Tracking or any form of surveillance used as part of the Code Member's methodology is Invisible Processing; and
- physical harm – for example where the Code Member's processing of Personal Data may put the Individual at risk of harm, such as in a whistle-blower scenario.

21.7 In addition to the considerations set out in **Part B** paragraphs 21.1 to 21.5 above, a Code Member will need to look at whether the processing involves any of the activities described in **Part B** paragraph 21.6 above, in determining whether a DPIA is required.

21.8 Code Members should consider whether a single DPIA could be used for multiple elements of a Client's instructions. For example, when investigating a claim which involves the large-scale processing of Special Category Data, a single DPIA may be used to address a set of similar processing operations that present similar high risks.

22. What does a DPIA involve and what are the challenges of completing it?

22.1 A DPIA should be completed by a Controller, if necessary, with help from its Processors. Therefore, Code Members will only be responsible for completing DPIAs in respect of those Code Services for which they are

Controllers. Where Code Members are acting as Processors, they may need to assist their Clients with completing their own DPIAs.

22.2 A DPIA is a process to help identify and minimise the data protection risks of a project or class of processing and, in completing it (as in the template DPIA contained in Appendix II), a Code Member must:

- identify the need for the DPIA, explaining the project, case or activity relating to the processing;
- describe the nature, scope, context, and purposes of the processing;
- consider a consultation process with relevant stakeholders about the processing;
- assess the necessity and proportionality of the processing and explain the lawful basis for the processing;
- identify and assess the risks of harm to Individuals;
- identify any measures to mitigate those risks;
- consider whether there is still a high risk and, if so, consult the ICO before proceeding with the processing;
- sign off and record outcomes; and
- keep under review and reassess if anything changes.

22.3 Code Members' instructions from Clients tend to provide one side of a scenario and it is easy for the Code Member to assume that the information from its Client is complete. Such an assumption may cause the Code Member to fail to consider fully the rights of the Individuals it is instructed to investigate, or the risk of harm the processing may cause to Individuals. It is important that the Code Member objectively considers the harm that may be caused by the prospective processing. A DPIA will greatly assist the Code Member to assess the risks in an open and fair manner.

23. Importance of the DPIA

23.1 Conducting a DPIA does not have to be complex or time consuming, but it must be carried out rigorously, and in a manner which is proportionate to the data protection risks that may arise from the processing.

23.2 Completing a DPIA also helps the Controller completing it to ensure its compliance with the Data Protection Principles. It may flush out and help to rectify the following common issues with Personal Data processing for carrying out Code Services:

- the Personal Data processed is excessive or irrelevant - there is great temptation for a Code Member to "pad out" a report with Personal Data not strictly relevant to the purpose, merely to provide the Client with a sense of value for money;
- Personal Data is kept for too long - Code Members must not hoard case files and the Personal Data that is contained within them, on a "just in case" basis;
- Personal Data is used in ways that are unacceptable to or outside of the reasonable expectations of the Individuals concerned;
- the related Individuals' rights are not respected - for example, there is insufficient access to or transparency in relation to the processing;
- the Personal Data is inaccurate, insufficient, or out of date;
- the Personal Data is disclosed to recipients explicitly contrary to the Individual's wishes; or
- the Personal Data is not kept securely.

24. What happens after completing a DPIA?

24.1 After completing a DPIA, the outcomes must be incorporated into how the Code Member carries out the processing. For example, any risk mitigations identified in the DPIA must be put in place prior to the processing.

24.2 A Code Member may wish to consider publishing its DPIA to improve trust in its processing activities. This may be more appropriate for the services offered by a Code Member that are within an Individual's reasonable

expectations and do not have a covert element. Code Members can redact any commercially sensitive information if they do publish a DPIA.

24.3 If the DPIA confirms that a high risk remains despite any risk mitigations, then Data Protection Law requires the Code Member to consult with the ICO before the processing is carried out. The Code Member must send a copy of the DPIA to the ICO and can expect a response within ten working days, with the ICO's written advice usually following within eight weeks (unless the DPIA is deemed complex or further information is required).

24.4 If it is consulted on a DPIA, the ICO may decide that the risks have been sufficiently mitigated and the processing can continue, and may provide further suggestions for risk mitigations in written advice. The ICO may issue a warning, setting out the steps that must be taken to avoid breaching Data Protection Law; the ICO's decision may be appealed (via judicial review). In circumstances where the processing has started and where ICO has significant concerns, it may impose an enforcement notice which limits or bans the processing; the ICO's decision may be appealed (via the First Tier Tribunal). In all cases a Code Member must reflect carefully upon the ICO's written advice and any warnings enforcement notices it imposes.

25. Lawful basis

Key requirement		
Code Requirement		*Supporting Evidence*
Case Extracts – Lawful Basis	*Code Members, where necessary, must establish and appropriately document a lawful basis for data processing under Article 6 (and, where necessary, a condition under Article 9 or 10) of the UK GDPR, having considered the obligation under Article 5 of the UK GDPR for the Personal Data to be processed lawfully, fairly and in a transparent manner.*	*Case extracts, with an outline of the lawful basis relied on for the processing under Article 6, 9 and / or 10 of the UK GDPR and which demonstrates that the Code Member has considered its obligations under Article 5.* *Code Members must include evidence confirming that:* *(i) the purposes of processing activities have been reviewed and the most appropriate lawful basis has been chosen;* *(ii) the processing is necessary for the relevant purpose, and they are satisfied that there is no other reasonable and less-intrusive way to achieve that purpose; and* *(iii) where Special Category Data / Criminal Offence Data is processed, the conditions for processing such data are identified.*

25.1 This section of the Code deals with aspects of Data Protection Law that the Code Member must consider where it is acting as Controller rather than Processor. To establish whether it is acting as a Processor or Controller, a Code Member should refer to Part B paragraph 9 above.

25.2 The Code Member must identify the lawful basis for processing any Personal Data, and should establish a structured way of doing so before it takes on

instructions. The ICO has produced an interactive guidance tool which can be used to consider the appropriate lawful basis for processing [15].

25.3 Under the first Data Protection Principle, Code Members must be able to demonstrate that their processing is fair, lawful, and transparent. A key element of this requirement is that there is a valid lawful basis for the processing. The available lawful bases are set out in Article 6(1) of the UK GDPR. In addition:

- where a Code Member is processing Special Category Data, the processing must be covered by a condition under Article 9(2) of the UK GDPR and in certain circumstances one of the further specific conditions under Parts 1 or 2 of Schedule 1 of the DPA must also apply; and
- if the Code Member is processing Criminal Offence Data then it must also meet a condition under Parts 1, 2 or 3 of Schedule 1 to the DPA, as required by Article 10 UK GDPR.

25.4 The Code Member must pay special attention to the need to protect children's interests. Any harm to children which will or may arise from processing may mean that Personal Data cannot be collected or used at all.

Key requirement		
Code Requirement		*Supporting Evidence*
Protection of children's interests	*Demonstrates that particular attention is given to processing the Personal Data of children.*	*Evidence may include extracts from portfolios, LIAs or DPIAs or completing the ICO's self-assessment risk tool as found here for any pieces of work relating to children.*

25.5 Code Members must not, to the extent possible, switch the lawful basis for processing Personal Data part-way through their processing. This would be likely to have a negative impact on the fairness and transparency of the processing and could lead to breaches of accountability and transparency requirements under Data Protection Law. However, it is possible that some circumstances may require a change to the lawful basis, for example a legal obligation arising. Where there is good reason to review the lawful basis and

make a change, the Code Member must inform the Individual and document the change. For more information see **Part B** paragraph 30 below 'Processing for new purposes'.

26. **Article 6 of the UK GDPR – Lawful Bases**	
LAWFUL BASIS	DESCRIPTION
LEGITIMATE INTERESTS	Processing is permitted if it is necessary for the purposes of legitimate interests pursued by the Code Member or the Client (or by a third party), except where the interests are overridden by the interests, fundamental rights, or freedoms of the affected Individuals. The legitimate interests lawful basis is commonly relied on by Code Members and is dealt with in greater detail in Part B paragraph 31 below.
CONSENT	Personal Data may be processed on the basis that the Individual has consented to the processing. Consent [16] must be freely given, specific, informed, and unambiguous. It is important to make it known to the Individual that their consent may be withdrawn at any time and how that can be done. The process of obtaining the consent must make it easy for people to withdraw consent. Data Protection Law sets a high standard for consent. Consent is often not appropriate for Code Member activities such as investigating fraud, torts, domestic issues such as infidelity or divorce finances. If consent is inappropriate, the Code Member will have to look for a different lawful basis under Article 6 of the UK GDPR (and also ensure its processing is fair and transparent). Consent means offering Individuals real choice and control. Genuine consent should put Individuals in charge, build trust and engagement. Consent requires a positive opt-in and must not be a pre-ticked box or any other method of default consent. It must be obvious that the Individual has consented and to what.

	Explicit consent requires a very clear and specific statement of consent. Vague or blanket consent is not enough. It must be clear and concise. Any third-party Controller who will rely on the consent must be named. An evidential record of any consent must be kept, including who consented to what, when and how consent was granted. In general, consent is unlikely to be available to a Code Member when it is providing Code Services. However, it may be the relevant lawful basis for processing a Client's Personal Data or new processing/new Personal Data which is not covered by the original instruction or purpose. For example, if the Code Member needs to process new Personal Data once it has located an Individual (such as new information provided by the Individual about the matter), the Code Member will need to consider whether in all the circumstances consent can be relied upon to process this additional Personal Data and share it with the instructing Client, or whether an alternative lawful basis would apply.
CONTRACTUAL NECESSITY	Processing is permitted if it is necessary for the entry into, or performance of, a contract to which the Individual is party. The processing must be more than just useful, and must be truly necessary in order for the contract to be performed. This lawful basis is unlikely to be available to a Code Member when it is providing Code Services. However, it may be a relevant lawful basis in relation to processing necessary for the performance of a contract between the Code Member and its Client, which is an activity outside of the scope of this Code.
LEGAL OBLIGATIONS	The Code Member can rely on this lawful basis if it is necessary to process the Personal Data to comply with a common law or statutory obligation. Legal obligations in this context does not include contractual obligations which may be covered by the contractual necessity lawful basis explained above.

	The Code Member must be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out the obligation. The legal obligation will not necessarily specifically require the processing activity. The point is that the overall purpose must be to comply with a legal obligation that has a sufficiently clear basis in either common law or statute. This principle is subject to two important clarifications: • The legal obligation must be binding in nature. For example, the "compliance with legal obligations" lawful basis does not apply where a public authority requests access to Personal Data, but the Code Member's compliance with that request is not legally mandatory (for example, there is no court order). Of course, in this situation there may be other lawful bases available to the Code Member, depending on the facts. • A legal obligation in this context means a legal obligation for the Code Member arising under UK law. A legal obligation to process Personal Data arising under the laws of a non-UK jurisdiction (e.g. an obligation arising under US law) is not legal obligation for the purpose of this lawful basis. The legal obligation lawful basis may frequently arise in relation to Code Member activities when there is a requirement to report suspicious activity under the Proceeds of Crime Act 2002 or where the Code Member must comply with an order of the court under any circumstances. It is unlikely that this lawful basis would be available at the outset of an instruction. It would be most likely to arise during the course of the engagement, as and when a legal obligation to report or share Personal Data arose.
VITAL INTERESTS	Personal Data may be processed on the basis that it is necessary to protect the vital interests of the Individual or of another natural person.

	Vital interests covers the situation when someone's life, or their physical or mental health or wellbeing is at urgent and serious risk. This includes an urgent need for life-sustaining food, water, clothing or shelter. It is not a lawful basis that is likely to arise often, if at all, in Code Services.
PUBLIC TASK	Personal Data may be processed by a public authority on the basis that such processing is necessary for the performance of its tasks or functions in the public interest, or in exercising official authority vested in it. Personal Data may also be processed by a private organisation carrying out a specific task set out in law which is in the public interest. It is not a lawful basis that is likely to arise often, if at all, in Code Services.

Lawful basis – additional important considerations	
27. **INVISIBLE PROCESSING**	Invisible Processing is the processing of Personal Data that occurs without the Individual's knowledge. This can happen, for example, when a Code Member obtains Personal Data from an internet browser following an on-line search, or obtains Personal Data indirectly through third party sources. Invisible Processing can pose a high risk to Individuals because they will not be able to exercise their data protection rights or control over the Code Member's use of their Personal Data if they are unaware that it is being processed. If the Code Member handles Personal Data in ways that the Individual does not reasonably expect and does not provide the Individual with privacy information, the Code Member may breach Data Protection Law. **Example 1 – Covert surveillance:** Code Members, where necessary, justified, proportionate and subject to the outcome of a DPIA, may in exceptional circumstances conduct surveillance on Individuals for limited reasons, such as to gather evidence for legal proceedings or to investigate potentially fraudulent activity. The surveillance is usually conducted without the knowledge of the Individual being monitored. Invisible Processing of this type is likely to be unlawful unless there are clear and unequivocal compelling reasons to justify the processing. This type of processing will always require a DPIA (see DPIA template in Appendix II (1.xvii and 1.xviii)). **Example 2 – Background checks:** Code Members may be instructed to conduct background checks on Individuals to gather information about their personal and professional history. This might involve gathering information from public records or online sources which would be invisible to the Individual being investigated. If the Individual is unaware of such processing and would not reasonably expect it, then Invisible Processing cannot be justified. In such cases, the Code Member should

	contact the Individual to provide privacy information and obtain their consent to the processing at the outset. Where an Individual might reasonably expect the processing to be taking place, for example where they are actively looking for a job having posted their cv on recruitment websites or where they are selling a business, the Code Member can rely on legitimate interest as the lawful basis for the processing and, subject to the outcome of the LIA (see Part B paragraphs 31-32 below), the background checks may be conducted without the Individual's knowledge. A DPIA must be carried out in these circumstances (see DPIA template in Appendix II (1.xvii)). **Example 3 – Tracking devices:** To support an Investigation or to avoid possible compromise, Code Members may, subject to the outcome of a DPIA, need to consider the use of tracking devices to monitor the movements of Individuals. The processing will be invisible if the tracking is done without the Individual's knowledge or consent. This is likely to be considered unlawful unless there are clear and unequivocal compelling reasons to justify the processing. The monitoring will always require a DPIA, as shown in the DPIA template in Appendix II (1.xvii and xviii). **Example 4 – Social media monitoring:** Code Members may monitor social media accounts to gather information about Individuals. If the monitoring is done without the Individual's knowledge or consent and/or in breach of the terms and conditions of the social media platform, it will be considered Invisible Processing and will always require a DPIA (see DPIA template in Appendix II (1.xvii)). **Privacy Information exceptions** In some circumstances, an exemption may apply from the right to be informed (under the DPA, Schedule 2, Part 1). For example, where the purpose of the processing is the prevention or detection of crime and providing privacy information would prejudice that purpose. Or, where informing the affected Individual would impede the performance of tasks carried out for the purposes of legal proceedings, including obtaining legal advice, establishing a legal claim and for bringing or

	defending a legal claim. This exemption recognises that disclosing certain privacy information to Individuals during ongoing or contemplated legal proceedings may hinder the legitimate interests pursued by the Controller, such as defending its position or providing evidence. The Code Member should consider the impact of Invisible Processing on its lawful basis for processing. It may be difficult for the Code Member to rely on legitimate interests if it processes Personal Data in ways that the Individual does not reasonably expect and does not provide privacy information. It must be confident that it has a compelling reason to justify the unexpected nature of the processing and can mitigate the impact on Individual rights. Even where the processing has a detrimental impact on the Individual, the Individual's interests will not always take precedence over the Code Member's (or Client's or other third party's) legitimate interests. This is determined by the gravity of the impact and if it is justified in light of the Code Member's purpose. The interests of the Code Member do not necessarily have to coincide with those of the Individual, and if the Code Member (or Client or other third party) has a more compelling interest, this may justify the impact on the relevant Individuals. The requirement to provide privacy information may not apply in circumstances where Personal Data has not been obtained directly from the relevant Individual if providing privacy information to the Individual would be impossible, involve disproportionate effort or make the achievement of the objectives of the processing impossible or seriously impair them (under Article 14(5)(b) of the UK GDPR) [17]. If the Code Member intends to rely on one of these exceptions, it must still publish general privacy information, for example, in a privacy notice on its website, and conduct a DPIA. When a Code Member does not provide privacy information to the Individual and relies on the exceptions under Article 14(5)(b), there may be a high risk to the Individual. A DPIA will assess and demonstrate

	whether the Code Member is taking a proportionate approach. It will help the Code Member consider how best to mitigate the impact on Individuals' ability to exercise their rights and it will also help demonstrate how the Code Member complies with the Data Protection Principles. For further information about DPIAs, please refer to Part B paragraph 20 to 24 above. **Example 1 – Providing privacy information would be impossible:** A Code Member is asked by a Client to trace a particular person, for whom they have no current contact details. The UK GDPR requires the Code Member to provide privacy information to the person being traced within a reasonable period and no later than one month. Despite the Code Member's efforts, it proves to be difficult to trace the person concerned and it takes longer than one month. The Code Member relies on the exception that it is impossible to provide privacy information directly to the person concerned. This remains the case until the Code Member locates the person at which point the Code Member must provide appropriate privacy information to the person. **Example 2 – Providing privacy information would be disproportionate:** A Code Member is conducting an Investigation for its Client that involves looking through local, publicly available historical records at the Registry Office, but the search does not produce any records which are relevant to the Investigation. The Code Member must provide privacy information directly to people even when using data from publicly accessible sources. However, the Code Member relies on the exception for disproportionate effort because the processing has no impact on the Individuals concerned and any contact with them would not be proportionate in the circumstances. **Example 3 – Providing privacy information would render impossible or seriously impair the achievement of the objective:** A Code Member is asked by an employer to investigate potential gross misconduct by an employee using covert monitoring. The Code Member considers that telling the employee about the collection of the Personal Data would

	render the objective of the processing impossible or else seriously impair it because the Individual would behave differently if they knew about the monitoring. In all of these examples, the Code Member must carry out a DPIA to assess the risk of the processing, and justify its reliance on the exception. It is also important for Code Members to ensure that they are complying with Data Protection Law generally and that they are transparent about their data processing activities.

28. PROCESSING CRIMINAL OFFENCE DATA (ARTICLE 10 OF THE UK GDPR)	Additional conditions apply to the processing of Criminal Offence Data because of the potentially significant impact that the processing of such data can have upon the Individual. The additional conditions (there are, at the time of the first edition of the Code, 28) as set out in Schedule 1 of the DPA. However, Criminal Offence Data is treated differently to other Special Category Data, on the basis that there is a public interest in protecting the public from criminal activity. This is supported by the ICO in its guide to the UK GDPR [18]. Information about suspicions of criminal activity or investigations into potential criminal offences must be treated in the same way as Personal Data relating to actual criminal offences and convictions. Most of the conditions for processing Criminal Offence Data depend on the Controller being able to demonstrate that the processing is necessary for the purpose that the Code Member has identified, and it must be satisfied that there is no less intrusive way to achieve this purpose. In addition to meeting one of the conditions for processing Criminal Offence Data set out in Schedule 1 of the DPA, for many of those conditions, a Controller must have an appropriate policy document ("APD") in place relating to its processing of such data. The Code Member must also ensure that specific information about processing of Criminal Offence Data is provided in privacy information given to Individuals. The ICO has produced a template for this purpose [19]. For any permitted Criminal Offence Data processing, the Code Member should consider conducting a DPIA as a matter of good practice. The Client's instruction for the Code Member to process Criminal Offence Data is often included in a request for the Code Member to carry out due diligence background investigations. A Code Member is not permitted to maintain a comprehensive register of criminal convictions in any circumstances.

Key requirement		
Code requirement		*Supporting Evidence*
Criminal convictions	*Code Members must not maintain a comprehensive register of criminal convictions.*	*An annual written declaration confirming on-going compliance or alternative evidence which is accepted by the MB in its discretion.*

Explanation: The processing of Criminal Offence Data is governed by a complex legislative framework. Criminal Offence Data may only be processed:

- under the control of an official authority, or
- as permitted under Data Protection Law.

Where Code Members are not processing Criminal Offence Data in an official capacity, any such processing that they carry out must:

- have a valid lawful basis under Article 6 of the UK GDPR;
- comply with an additional condition for the processing of this type of Personal Data under Schedule 1 of the DPA. Examples of the applicable conditions of processing are in order to assess people's suitability for employment, to prevent or detect unlawfu acts, to prevent fraud, or for the purposes of legal claims or insurance; and
- have an APD in place when relying on any of the conditions in Schedule 1 of the DPA.

The Code Member must also ensure that it complies with all other requirements of Data Protection Law when processing Criminal Offence Data. This means, for example, that the processing must be carried out in a manner that is fair, transparent, necessary, proportionate, and generally lawful (not just under Data Protection Law).

A Code Member may be instructed by a Client to process Criminal Offence Data. If the Code Member does not have official authority for the processing, it must be permitted under UK Data Protection Law and to demonstrate this must comply with the appropriate conditions set out in Schedule 1 of the DPA.

Even if Criminal Offence Data is publicly available, its processing is still subject to the above restrictions. For example, certain websites provide criminal case court listings, sentencing, types of offences and the parties' details. For the Code Member to process such data as Controller it would need to meet the lawful basis requirement under Article 6 of the UK GDPR and the conditions of Article 10 UK GDPR / Schedule 1 DPA.

Criminal Offence Data Processing example:

An insurance company Client has been alerted to multiple road traffic accident claims on various policies, which appear to be interconnected and fraudulent. The insurer requires the Code Member's assistance in processing the Personal Data of the insured parties and the third parties involved in each suspect claim to explore the suspicion of criminality, including researching any Criminal Offence Data relating to past similar and relevant activity that may support or eliminate the suspicion.

In the event that the Code Member is acting as a Controller, the Code Member must identify an appropriate lawful basis to process the Personal Data of the people involved. Depending on the circumstances, it may be able to rely on legitimate interests (its own and those of the insurance company). However, the processing of Criminal Offence Data means that the Code Member will also need to meet one of the conditions as set out in Schedule 1 DPA and may also need to have an APD in place. For example, the condition for "preventing or detecting unlawful acts" set out in paragraph 10(1) of Schedule 1 may apply.

29. PROCESSING SPECIAL CATEGORY (SENSITIVE) PERSONAL DATA (ARTICLE 9 OF THE UK GDPR)	"Special Category Data" means Personal 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**. In addition to establishing the Article 6 lawful basis for processing Special Category Data, the Code Member must also meet one of the ten conditions set out in Article 9 of the UK GDPR. Five of the ten Article 9 conditions also require the Code Member to meet additional requirements under Schedule 1 to the DPA. These are summarised in the explanation box below. The Code Member must in normal circumstances examine the processing and establish the applicable conditions of processing before the processing is carried out, in order to assess and mitigate any associated risks. This is because processing Special Category Data is likely to pose a higher risk to Individuals. For further information about DPIAs, please refer to Part B paragraph 20 to 24 above. The processing of Special Category Data in reliance on certain of the conditions in Article 9 may also require an APD, setting out and explaining the procedures for securing compliance and policies regarding the retention and erasure of such Personal Data. The ICO's APD template referred to above in relation to Criminal Offence Data will also be relevant for the processing of Special Category Data too [20]. For any processing of Special Category Data, the processing must be necessary for the purpose the Code Member has identified, and it must be satisfied that there is no other reasonable and less intrusive way to achieve this purpose.

Explanation: The processing of Special Category Data is prohibited, unless:

- The Individual has given explicit consent.
- The processing is necessary in the context of employment law, or laws relating to social security and social protection. This condition will also require the Code Member to meet the conditions set out in condition 1 of Part 1 of Schedule 1 of the DPA.
- The processing is necessary to protect vital interests of the Individual (or another person) where the Individual is incapable of giving consent.
- The processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes. However, this condition is unlikely to be relevant to Code Services.
- The processing relates to Personal Data that have been manifestly made public by the Individual.
- The processing is necessary for the establishment, exercise, or defence of legal claims, or for courts acting in their judicial capacity [21].
- The processing is necessary for reasons of substantial public interest, which is on the basis of UK law which is proportionate to the aim pursued, protects the rights of Individuals and meets one of the 23 specific public interest conditions set out in Schedule 1 Part 2 of the DPA.
- The processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services.

This condition will also require the Code Member to meet the condition set out in condition 2 of Part 1 of Schedule 1 of the DPA.

- The processing is necessary for reasons of public interest in the area of public health (e.g. ensuring the safety of medicinal products).

  This condition will also require the Code Member to meet the conditions set out in condition 3 of Part 1 of Schedule 1 of the DPA. However, this condition is unlikely to be relevant to Code Services.

- The processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.

  This condition will also require the Code Member to meet the conditions set out in condition 4 of Part 1 of Schedule 1 of the DPA. However, this condition is unlikely to be relevant to Code Services.

Special Category Data processing example:

The Code Member's Client is being sued by one of its employees following an accident at work. The Client wants to pass the details of the accident to the Code Member to investigate the injuries sustained by the claimant (the Individual), ahead of instructing solicitors to obtain legal advice on its position and potentially to defend the claim. The Personal Data relates to the Individual's injuries and concerns the Individual's health. For the purposes of Data Protection Law this activity constitutes Special Category Data processing. If the Code Member is the Controller, in order to process the Personal Data provided by the Client, the Code Member, in addition to its other obligations, would need both an Article 6 lawful basis and additional Article 9 condition for processing. The Code Member may be able to rely on the Article 9(2)(f) condition that the processing is necessary for the establishment, exercise, or defence of

	legal claims. The Code Member must ensure that the processing is only carried out to the extent necessary to defend the claim.
30. PROCESSING FOR NEW PURPOSES	Save in exceptional circumstances, the Code Member should not use data for secondary purposes. As a general rule, if the new purpose is very different from the original purpose, would not be reasonably expected by or would have an unjustified impact on the Individual, it is unlikely to be compatible with the Code Member's original purpose for collecting the data. **Explanation**: Where Personal Data is to be processed for a new purpose, the Code Member must consider whether the new purpose is "compatible" with the original purpose, taking into account the following: • Any clear link between the original purpose and the new purpose. • The context in which the data has been collected, including the Code Member or Client's relationship with the affected Individuals, considering in particular what the Individuals would reasonably expect. • The nature of the Personal Data and whether Criminal Offence Data and / or Special Category Data is involved. • The possible consequences of the new purpose processing for the affected Individuals. • The existence of appropriate safeguards (e.g. encryption or pseudonymisation). .

31. Legitimate interests

Key requirement		
Code Requirement		*Supporting Evidence*
Case Extracts – Legitimate Interests	*The LIAs must determine the lawful basis for processing in accordance with Article 6(1)(f) of the UK GDPR. The three-part test from the ICO's guidance here should be correctly applied. The MB will take into consideration that the business may not regularly carry out LIAs.*	*A sample of up to three LIAs from live cases conducted by the Code Member which reflect the Code Member's range of services during the previous 12 months, as required by the MB.*

31.1 Legitimate interests under Article 6 of the UK GDPR is a relatively flexible lawful basis for processing, but a Code Member cannot assume it will always be the most appropriate lawful basis. In this section the Code will explain how legitimate interests works in the context of Code Services and what a Code Member can do to demonstrate that it has met its responsibilities under Data Protection Law. For more information, please refer to the ICO's guidance here.

31.2 This part of the Code is only relevant for when the Code Member is acting as a Controller and so requires a lawful basis for its processing. Code Members who are acting as Processors are referred to Part B paragraphs 11, 13, and 16 above generally. In addition, the Code Member must be aware that for Special Category Data or Criminal Offence Data, there are a range of additional requirements in respect of the processing, as explained in the explanatory box in Part B paragraphs 29 and 28 above.

31.3 Reliance on legitimate interests as the lawful basis for processing comes with significant responsibility for the Code Member, as it involves balancing the rights and freedoms of the Individual against the legitimate interests being pursued. The processing in question may evolve as the relevant instructions develop, so the Code Member must carry out regular reviews as necessary to ensure that its reliance on legitimate interests continues to be appropriate.

31.4 The Code Member (as Controller) must complete a legitimate interests assessment ("LIA") prior to commencing the processing. The LIA should include a three-part "balancing test" to show how the Code Member determines that it's, or a third party's, legitimate interests override those of any affected Individuals (see further in **Part B** paragraph 32 below). The LIA should also assess the following:

- Not using people's data in intrusive ways or in ways which could cause harm, unless there is a very good reason.
- Protecting the interests of vulnerable groups such as people with learning disabilities or children.
- Whether the Code Member could introduce safeguards to reduce any potentially negative impact.
- Whether the Code Member can offer an opt-out.
- Whether the Code Member is required to carry out a DPIA.

31.5 There are a number of factors that might indicate that legitimate interests is unlikely to be an appropriate lawful basis for the Code Member's processing (as Controller). For example, the Code Member may wish to avoid relying on the legitimate interests basis if:

- The processing does not comply with broader legal, ethical or industry standards.
- The Code Member does not have a clear purpose and is keeping the data "just in case" (in this case the processing is unlikely to be compliant on any basis).
- The Code Member could achieve the end result without using Personal Data.
- The Code Member intends to use the Personal Data in ways people are not aware of and would not expect (unless the Code Member has a very compelling reason that could justify the unexpected nature of the processing).

- There is a risk of significant harm arising from the processing (unless the Code Member has a more compelling reason that could justify the impact).
- The Code Member is not confident about the outcome of the balancing test.
- The Code Member or the Client would be embarrassed by any negative publicity about how the Code Member intends to use the data.
- Another lawful basis more obviously applies in respect of a particular processing activity. Although in theory more than one lawful basis may apply to the processing, in practice legitimate interests is unlikely to be appropriate for any processing purpose where another basis more obviously applies.

31.6 While any purpose could potentially be relevant, that purpose must be "legitimate". Anything unethical or unlawful is not a legitimate interest. If the Code Member is not satisfied with the outcome of the balancing test, it may be safer to look for another lawful basis under Article 6 of the UK GDPR, or decline the case instructions.

31.7 There are three elements for the Code Member to consider when it is relying on the legitimate interests lawful basis. It helps to think of this as a three-part test, which allows Code Members to use Personal Data while still balancing the needs of the Individual with the interests of the Controller or relevant third party. Part B paragraph 32 below provides further detail on how the test should be approached.

32. The Legitimate Interests 3-part test

1. IDENTIFY A LEGITIMATE INTEREST
2. SHOW THAT THE PROCESSING IS NECESSARY TO ACHIEVE IT
3. BALANCE IT AGAINST THE INDIVIDUAL'S INTERESTS, RIGHTS AND FREEDOMS

IDENTIFY A LEGITIMATE INTEREST PURSUED BY THE CONTROLLER OR A THIRD PARTY	Consider the following questions: • Why does the Code Member need to process the data? • What is the Code Member trying to achieve? • Who benefits from the processing and in what way? • What would the impact be if the processing couldn't go ahead? • Would the use of the data be unethical or unlawful in any way? • Would the Code Member be complying with other relevant laws and industry guidelines? **Explanation**: There are circumstances in which the purpose will clearly justify the legitimate interest. Data Protection Law makes it clear that (to the extent necessary) fraud prevention and network / information security are deemed to be legitimate interests. Similarly, disclosures to give warning of criminal acts or public security may be legitimate interests (although they may be overridden by a binding obligation of secrecy). The Code Member needs to avoid reliance on vague or generic "business interests". A wide range of interests may be considered as "legitimate". They can be the Code Member's own interests or the interests of a third party, and commercial interests as well as wider societal benefits. They may be compelling or trivial but ultimately, they must be legitimate. Interests that are less than compelling may be overridden in the balancing test. The Code Member must think about specifically what interests it is furthering with the particular processing operation.
SHOW THAT THE PROCESSING IS NECESSARY TO ACHIEVE IT	Consider: • Does this processing help to further that interest? • Is it a reasonable way to go about it?

	• Is there another less intrusive way to achieve the same result? **Explanation**: Invariably an Investigation starts with considering the legitimate interests pursued by the Code Member (or that of the Client or a third party) as the lawful basis under Article 6 of the UK GDPR. The Code Member needs to identify the purpose and decide whether it constitutes a legitimate interest. The Code Member needs to be as specific as possible, as this will help when it comes to the necessity and balancing tests. Necessary, in this section, means that the processing must be a targeted and proportionate way of achieving the purpose of the processing.
BALANCE IT AGAINST THE INDIVIDUAL'S INTERESTS, RIGHTS AND FREEDOMS	Consider: • What is the nature of the Code Member's (or the Client's) relationship with the Individual? • Is any of the data particularly sensitive or private or contain Criminal Offence Data? • Would people reasonably expect the Code Member to use their data in this way? • Is the Code Member happy to explain it to them? • Are some people likely to object or find it intrusive? • What is the possible impact on the Individual? • How big an impact might it have on them? • Will the Code Member be processing children's data? • Are any of the Individuals vulnerable in any other way? • Can the Code Member adopt any safeguards to minimise the impact? • Can an opt-out be offered? **Explanation**: The Code Member must consider whether the legitimate interest can be overridden by the rights and interests of the Individual. Under Data Protection Law when carrying out Code Services the Code Member must ensure that the Individual's rights are respected, and privacy is protected.

32.1 Following the LIA, the Code Member needs to weigh up the relevant considerations at the third stage of the test. The Code Member must reach a conclusion as to whether the processing is necessary (part 2 of the test) for the purposes of the legitimate interests (part 1 of the test) pursued by the Code Member or a third party. If so, the Code Member must consider whether the interests in part 1 of the test are overridden by the interests or fundamental rights and freedoms of the Individual (part 3 of the test).

32.2 Completion of an LIA and application of its conclusions must demonstrate that the Code Member has appropriately considered whether legitimate interests is the correct lawful basis for processing the Personal Data.

32.3 The Code Member must clearly document the decision and assessment keeping a record of the LIA. Whilst there is no standard format for this, the Code Member may wish to adopt the ICO template [22].

32.4 Code Members must consider carrying out an LIA before commencing processing for which it relies on legitimate interests as a lawful basis. Code Members must carry out an LIA unless they have an existing LIA which is identical. The LIA will demonstrate the thought process used in reaching a decision and to justify the outcome on the specific facts of the case. As a type of case develops, the LIA may need to be reviewed and refreshed as necessary when there is a significant change in the purpose, nature, or context of the processing. If, after weighing all the factors, the processing will cause undue interference with the interests, rights, or freedoms of the affected Individuals, the Code Member cannot rely on the legitimate interest lawful basis. The Code Member must be confident that the benefits of the processing justify any identified risks (the higher the risks the more compelling the justification must be). It may be safer to look for another lawful basis if the Code Member is unsure.

Example:

1. A Client seeks the Code Member's assistance in a suspected fraud. The Code Member conducts an LIA to ensure that it is relying on the

legitimate interest basis appropriately. In the LIA, the Code Member documents that it considers it has a legitimate interest in processing the Personal Data for the purposes of fraud prevention. The Code Member considers that the processing is necessary in order to achieve that purpose and documents this, together with the fact that there are no less intrusive methods of reasonably achieving the same result. The Code Member must also consider proportionality and the risk of excessive processing. Finally, the Code Member weighs the rights and freedoms of the affected Individual against the relevant interests of the Code Member or third party. The Code Member, in particular, reflects on whether it would be reasonable for a fraudster to expect a victim of suspected fraudulent activity to process the suspected fraudster's Personal Data in contemplation of the victim taking remedial action. The fact that, in a Code Member's case, the processing may be covert and potentially intrusive would present another factor to consider in the balancing of the rights and freedoms of the affected Individual against the legitimate interest of the Code Member. This may be weighed against the fact that the Client's and the public interest in investigating the fraud is a compelling one. The Code Member must ensure that the LIA is conducted thoroughly, and the documentation retained for review in the future.

33. Consent to share in trace / locate case example

Key requirement		
Code Requirement		*Supporting Evidence*
Lawful basis (legitimate interests – trace or locate)	*The Code Member has considered and recorded the lawful basis appropriately in respect of Personal Data processing with reference to trace or locate instructions. Code Members are required to determine the appropriate lawful basis for processing and, where relying on legitimate interests as the lawful basis, keep a record of the LIA completed. In completing the LIA, the Code Member applies the three-part test.*	*There is no standard form for documenting the legal bases for processing Personal Data, however Code Members must ensure that they can demonstrate that a lawful basis applies. This should explain, where relevant, any difference between the processing undertaken prior to locating an Individual and after locating an Individual. The Code provides guidance on this (see Part B paragraphs 33.1-33.9 below) and the Code Member should use that guidance to support the evidence of the thought process in reaching a decision and justification of the outcome.* *Evidence may be required of any LIA undertaken, which includes the thought process in reaching a decision and justification of the outcome.* *Code Members must include evidence confirming that:* *(i) the purposes of processing activities have been reviewed and the most appropriate lawful basis has been chosen;* *(ii) the processing is necessary for the relevant purpose, and they are satisfied that there is no other reasonable and less-intrusive way to achieve that purpose; and* *(iii) where Special Category Data / Criminal Offence Data is processed, the conditions for processing such data are identified.*

33.1 Code Members may find that building in appropriate safeguards can weigh as a factor in the legitimate interests balancing test. Safeguards may help support a conclusion that the Individual's interests no longer override the Code Member's interests. However, the Code Member must be aware that safeguards cannot always tip the scales and justify the processing.

33.2 A worked example of this is in relation to trace and locate instructions, which are relevant to the legitimate interests lawful basis. A Code Member may be instructed to trace a beneficiary of an estate who has not come forward to claim an entitlement under a will. The Client has made it clear that it would like the Code Member to share the facts of the instruction with the Individual for the purpose of carrying out their executor duties. The Code Member has the name and last known address of the Individual provided by the Client, but it will be exercising its discretion and using its own leads to track down the Individual.

Pre-trace processing

33.3 In the above example, the Code Member must establish its role and responsibilities in respect of the data processing. As in this case the Code Member will be determining the purpose and means of the processing, it is likely that the Code Member will be a Controller and so must establish a lawful basis for processing the Personal Data. The Code Member may consider that legitimate interests is the most appropriate lawful basis for the processing activities of tracing the Individual and contacting them on the Client's behalf. The Code Member must therefore complete an LIA to verify and demonstrate that the legitimate interests lawful basis does apply in the particular circumstances of that processing.

33.4 When completing the LIA, the Code Member considers whether the rights and freedoms of the Individual outweigh the legitimate interests of the Code Member's Client (as a third party) in tracing the Individual.

Post-trace processing

33.5 Following identification of the beneficiary in the above example, the Code Member must assess the appropriate lawful basis for processing the new

Personal Data which is the contact information for the identified Individual in accordance with the Client's instructions (the "post-trace" processing). Legitimate interests is unlikely to be an appropriate lawful basis for post trace processing and that the Individual's consent to the processing is likely to be required. Where the Individual's consent is not provided, the Code Member must not carry out further processing of the Individual's Personal Data by sharing it with the Client.

33.6 The Code Member should make its Client aware that the Code Member will be unable to share its findings with the Client without the Individual's consent.

33.7 If the Code Member is presented with a complete change in circumstances or an unanticipated type of processing is needed, then the lawful basis for the new processing must be considered. In the example in **Part B** paragraph 33.2 above, if the beneficiary, upon being traced, would like to meet the rest of the family of the deceased, this may represent unanticipated processing that would require a review of the lawful basis. For this new processing it may be that the consent of the Individuals in the family is the appropriate lawful basis to rely upon, but this should be considered on a case-by-case basis.

Example:

The Code Member is instructed by a Client to locate their adult child with whom they have been estranged and out of touch for many years. The Client wishes to resume contact with the Individual. The Code Member recognises its role as Controller and must carry out an LIA where it considers legitimate interest as the lawful basis for the processing. The Code Member concludes that the lawful basis of legitimate interest will only cover locating the Individual, being the first stage of the processing. In relation to the sharing of the Individual's Personal Data (their contact details), which is the next stage of the processing, the Code Member concludes that the Individual's rights and freedoms outweigh the Client's interest and so the Code Member accepts the assignment on the condition that it will, after locating the Individual, seek their consent for their details to be shared with the Client. If the Individual does not provide consent

the Code Member will not be able to process the Personal Data further by sharing it with its Client.

33.8 Example communication seeking Individual's consent:

Dear sir or madam,

We have been instructed by ..... (client) to locate you. Our client's purpose is to (e.g. re-establish contact, discuss the estate of the late ...).

We write to seek your consent for us to share your details with our client.

We have not at this stage shared your details and should you decline to consent we shall of course respect your wishes and advise our client accordingly. In which event it will be an end of our involvement, and your details deleted from our records.

Details we currently hold and wish to share are:

Name: ...Date of birth: ...Address: ...Email: ...Contact number: ...

Please refer to our privacy information on our website, click here.

Should you agree to our sharing your details with our client please reply by signing the below "I consent to the sharing of my data as above".

Yours truly,

Code Member

I consent to the sharing of my data as above.

Signed ..... (Individual)

33.9 Some typical example case scenarios where the legitimate interest lawful basis may or may not be applied with safeguards and 'consent to share' examples are set out in Appendix III.

PART C – CODE OF CONDUCT MANAGEMENT & INFRINGEMENTS

34. Management

34.1 The Code Member Criteria set out in Appendix I form the basis of the assessment by the MB on any application for Code Member status. The MB will also carry out subsequent annual desktop assessments to confirm that the Code Member continues to meet the Code Member Criteria including, where applicable, ongoing membership of the ABI (where membership means that the Code Member is exempt from demonstrating compliance with the full set of criteria set out in paragraph 1 of Appendix 1).

34.2 The Code Member is accountable for its own compliance with the Code. The Code Member must always be prepared to justify its decisions and actions. The MB's role includes considering allegations of infringements of the Code by Code Members. Whilst they fall outside the scope of the Code, Code Members must also be aware of and comply with their wider regulatory and legal obligations, including compliance with wider Data Protection Law.

34.3 A breach or failure to comply with the Code Member Criteria and Code requirements may be serious either in isolation or because it represents a persistent or concerning pattern of neglect. The MB will take this into account in its assessments.

35. Monitoring Body

35.1 As of the date of publication of this Code, SSAIB is the only MB, pending its approval by the ICO. SSAIB is a certification body accredited by UKAS (UK Accreditation Service [23]), with expertise in auditing against the recommendations of BS102000 code of practice for the provision of investigative services. It is a company limited by guarantee, operating on a not-for-profit basis.

35.2 The role of the MB is three-fold. First, the MB will implement procedures that provide for the effective audit and monitoring of Code Members' compliance

with the Code. Secondly, the MB will provide efficient mechanisms for the recording and investigation of complaints about infringements of the Code, including dispute resolution, sanctions, and remedies. Thirdly, the MB will assist the ABI with its annual review of the Code to ensure that it is up to date and reflects changes in practice / legislation.

35.3 A MB has to demonstrate an ability to meet the following specific requirements:

- independence in relation to four main areas: (i) legal and decision-making procedures, (ii) financial, (iii) organisational, and (iv) accountability;
- dealing with conflicts of interest to ensure the Monitoring Body can deliver its monitoring activities in an impartial manner;
- expertise in relation to the subject matter of the Code, with its personnel having the required knowledge and experience in relation to the sector, processing activity, Data Protection Law and auditing, to carry out compliance monitoring in an effective manner;
- established rules and procedures that enable it to assess the eligibility of Controllers and Processors to apply the Code, to monitor Code Members' compliance and to periodically review its operation;
- established procedures and structures to handle complaints about infringements of the Code or the manner in which the Code has been, or is being, implemented by a Controller or Processor, and to make those procedures and structures transparent to the public;
- a documented process to receive, evaluate and make decisions on complaints made about its monitoring responsibilities and activities, including any appeals;
- a clear framework to communicate information to the ICO;
- established procedures and mechanisms to contribute to reviews of the Code; and
- appropriate legal status.

36. Monitoring arrangements

36.1 Compliance with the Code will be assessed by the MB, on application to Code Member status and thereafter on an annual basis. The assessment will be conducted as a remote desktop exercise and require the Code Member to successfully demonstrate competence by providing evidence of compliance with the requirements at Appendix I.

36.2 The MB will maintain a record of all complaints in relation to the Code and the resultant actions, which the ICO can access at any time. The decisions of the MB will be made publicly available in line with its complaints handling procedure.

36.3 The MB will contribute to reviews of the Code as required by the ABI, to ensure that it remains relevant and up to date. It will also provide the ABI, and any other establishment or institution referred to in the Code with an annual report on the operation of the Code, which will include a list of current Code Members; any new members admitted over the previous twelve months; information concerning Code Member breaches of the Code; details of any Code Members suspended or excluded in the last 12 months; and outcomes of any Code Review.

36.4 The MB will apply Code updates and implement amendments and extensions to the Code as instructed by the ABI, following the approval of those Code updates by the ICO.

36.5 In undertaking its role, the MB has nominated a monitoring officer, who will act as the main point of contact with the ABI and be responsible for the activities of the MB.

36.6 The MB will ensure that only auditors with relevant expertise undertake assessments against the Code. That expertise will be evidenced by the MB against the following criteria:

- IRCA certification as a QMS ISO 9001 lead auditor;

- confirmed competency to undertake product conformity audits in relation to BS102000:2018;
- attendance at the ABI-provided UK GDPR training workshop; and
- successful completion of relevant and accredited continuous professional development training.

36.7 Any changes to Code monitoring arrangements will only be implemented in consultation with the ICO. If the ICO revokes the accreditation of the MB, the ABI will identify a replacement MB at the earliest possible opportunity. The replacement MB will then apply to ICO for accreditation within six months of the date of revocation and the application must include all relevant supporting evidence of compliance with the ICO's requirements. Failure to apply within this period will result in the withdrawal of Code approval by the ICO and existing Code Membership will become void. The ABI will not accept any new applications for Code Membership until a new MB is accredited.

37. Complaints

Key requirement		
Code Requirement		*Supporting Evidence*
Complaints	*Code Members must respond to Individuals' complaints received in accordance with the Code and guidance from the ICO. The MB may also investigate alleged breaches of the Code, and the Code Member must communicate with the MB in accordance with the Code and the cooperation criteria.*	*Evidence of any complaints received by the Code Member from Individuals in relation to data protection and the steps the Code Member took to respond to the complaint. Also, where relevant, evidence that in relation to MB investigations of alleged breaches of the Code, the Code Member has communicated with the MB in accordance with the Code and the cooperation criteria in this Code ("Cooperates with the MB" in Appendix I).*

37.1 The MB will be responsible for the recording, acknowledgement, and investigation of complaints of infringements of the Code, by Code Members.

A copy of the MB's complaints and appeals procedure will be published on its website and include guidance in relation to qualifying complaints.

37.2 Details of the complaint will be confirmed in writing, using a complaint form, and recorded in a complaints and disputes file maintained by the MB. The complaint will be acknowledged by the MB within 15 working days of its receipt of the completed form along with any questions the MB requires a response to. Relevant and permitted aspects of the complaint may be provided to the Code Member at the MB's discretion, within 15 working days of the MB having received the completed form; to obtain any information it requires from the Code Member. The timing or details of any complaint made under the Code does not impact the other obligations to which the Code Member is subject under Data Protection Law.

37.3 Code Members must provide the MB with a written response to the complaint within 30 working days of receiving their copy of the complaint, unless extended by the MB. That response must include an outline of the lawful basis for the processing of the Personal Data, subject to the complaint and, where appropriate a copy of the related DPIA, together with any other documentation deemed necessary by the MB.

37.4 The MB will consider any action necessary in line with Part C paragraph 38 below and notify the Code Member accordingly. The complainant will be informed by the MB of its findings and any action taken within ten working days of the Code Member being notified. The complainant will have a right of appeal against the findings of the MB and any action taken by them. Any appeal would be to the MB but reviewed by a panel of three MB auditors whose majority decision will be final. This does not affect any right of the complainant to refer a complaint to the ICO.

37.5 The MB will include a trend analysis of recorded complaints within the annual report referred to above.

Key requirement		
Code Requirement		*Supporting Evidence*
Cooperates with the MB	*Evidence that the applicant Code Member has responded, or is able to respond, to any correspondence from the MB in full and address/remedy all issues raised within the required timeframe.*	*Code Members must provide a written response and enclose any relevant evidence to show that they are able to comply with the MB's requests which may include providing evidence of operational email accounts.* *Where the MB has communicated with the Code Member, the Code Member must provide evidence to show that it has corresponded appropriately with and cooperated with the MB, including in relation to any investigations of alleged non-compliance with the Code.*

38. Infringements

38.1 Any infringement of the Code will, in the first instance, be addressed by the MB issuing a non-conformity report ("NCR"). The Code Member must address the NCR within a reasonable period. The Code Member must address the NCR with suitable measures to identify the root cause and prevent any future re-occurrence.

38.2 The MB will consider the need for any corrective advice or sanctions, which may include a training requirement, formal warning, report to the ABI or formal notice requiring suspension or exclusion as a Code Member.

38.3 In considering the issuing of corrective advice or sanctions the MB will take account of the causation factors and whether these comprised human error, a failure of process or deliberate act. It will also take account of any previous instances in which corrective advice or sanctions have been issued to the Code Member or where any pattern of repeated infringements can be

reasonably inferred. An infringement matrix is shown at section 39 below for illustrative purposes.

38.4 Suspension or exclusion of Code Members will only apply in the most serious of circumstances. Normally, Code Members will first have the opportunity to take suitable corrective measures where appropriate, as agreed with the MB. The Code Member will have a right of appeal in the event of a decision by the MB to either suspend or exclude them as a Code Member. Any such appeal must be made to the MB, in writing, within 21 days of notification of the findings of the Monitoring Body having been sent to the Code Member, setting out clearly the basis for the appeal. Any appeal would be to the MB but reviewed by a panel of three MB auditors whose majority decision will be final.

38.5 Where the Code Member is also a member of the ABI and the MB considers that an infringement warrants further action, it may make a referral to the ABI disciplinary process in accordance with the ABI byelaws, to consider a possible breach of the ABI code of ethics & professional standards. The ABI disciplinary procedure is explained by the flow chart available on the ABI website [24].

38.6 In other circumstances, where the Code Member is not a member of the ABI but of some other representative body, the MB may make a referral to that body under the relevant disciplinary process.

38.7 In the event of the suspension or exclusion of a Code Member, the MB will without delay notify the ICO with details of the infringement, actions taken and the reasons for taking them.

38.8 Code Membership does not affect the enforcement powers of the ICO as the regulator of Data Protection Law.

Key requirement		
Code Requirement		*Supporting Evidence*
Address non-conformity report(s) (NCRs).	*Full and adequate response to an NCR addressing and remedying all issues raised within the required timeframe.*	*Code Members must respond to an NCR issued by the MB by setting out in detail how they seek to address an NCR. Required actions may include updating DPIAs and LIAs to ensure compliance with Data Protection Law and providing further evidence of the lawful basis for processing Personal Data.*

39. Infringement matrix

Example infringement	Example MB action
Failure to record or accurately complete a DPIA when required. Failure to apply or accurately complete a legitimate interest assessment. Processing Personal Data without recording an appropriate lawful basis.	In isolated incidents, infringements such as these may merit corrective advice and a possible requirement for further training in the area relating to the infringement. Where infringements are repeated, are egregious or occur in in respect of Special Category Data, Criminal Offence Data or where children's Personal Data is processed, the MB may decide that more severe action is appropriate.
Failure to address a non-conformity report within the stipulated period.	A Code Member who fails to address non-conformity within the stipulated period has been given the opportunity to correct its processing activities but has failed to do so.
Repeated processing of Personal Data where no lawful basis recorded; repeated failure to record or accurately complete a DPIA when required; repeated failure to apply or accurately complete the legitimate interest assessment.	It may be that suspension escalating to expulsion is the appropriate action by the MB in such circumstances. In respect of failure to record a lawful basis, complete a DPIA when appropriate to do so, or to accurately complete the LIA, a written warning could be appropriate. However, repeated infringements, an egregious breach or a combination of different

		infringements, or breaches in respect of Special Category Data, may lead to more severe action being appropriate.
Repeated failure to respond to a non-conformity report within the stipulated period.		In these situations, the Code Member will have already been given the opportunity to correct its processing activities in advance of the infringement. It may be that suspension escalating to expulsion is the appropriate action by the MB in such circumstances.
Failure to record or accurately complete a DPIA after retraining.		
Failure to apply or accurately complete the LIA after retraining.		
Processing Personal Data where no lawful basis exists.		In these situations, it may be appropriate for the MB to expel the Code Member and/or refer the Code Member under the ABI's or other relevant disciplinary process. A number of factors, such as sensitivity, seriousness, repetition, and previous training, will be considered when making a decision to expel a Code Member.
Processing Personal Data where the LIA indicated that legitimate interests was not an appropriate lawful basis (and no other lawful basis applied).		

40. Consultation

40.1 First Consultation:

- The draft proposed Code was initially circulated to members of the ABI on 01 July 2020 with an initial closing date 31 July 2020. A copy was made available on the ABI website.
- The initial consultation sought ABI Members' input on the content of the draft proposed Code and a vote on the concept of developing a code of conduct and applying for ICO approval.
- As of 31 July 2020, only 10% of the response forms received from ABI Members expressed opposition or were unsure and the remaining 90% were in favour of the development of the Code of conduct and proposed application to the ICO for its approval.
- On 01 August 2020 the draft code of conduct on the ABI website was updated with the input from ABI Members and on that date, input was sought from the Investigative & Litigation Support Services sector by circulating notice to the known representative bodies and network groups.
- On 01 August 2020 notice of the consultation inviting input was also sent to representatives from various stakeholders, Individuals, and law enforcement.
- The first consultation closed on 14 August 2020. The relevant feedback was shared with the ICO.

40.2 Second Consultation:

- On 16 August 2022 a revised draft code of conduct was made available on the ABI website with a 'Press Release' circulated to ABI Members, other sector representative bodies, and representatives from various stakeholders, Individuals, law enforcement and the media.
- The 'Press Release' pointed to the draft code of conduct, a dedicated consultation feedback web page and invited interested parties to attend a live consultation event in London on 07 September 2022.

- The second consultation closed on 16 September 2022. The relevant feedback was shared with the ICO, and the draft code of conduct updated.

41. Review

41.1 The ABI will review the Code on an annual basis in consultation with the MB (the "Code Review"). A formal Code Review Framework has been agreed between the ABI and the MB, which includes horizon scanning. Any updates or changes to legislation and guidance that are identified through this Code Review Framework shall be considered in a timely fashion for inclusion as an amendment or extension to the Code by the ABI. Any amendments or extensions to the Code may be made by the ABI, but only following approval by the ICO.

41.2 The ABI will submit an annual report to the ICO following the annual review, which shall be endorsed by the MB, and shall include:

- any proposed amendments for approval by the ICO - including those that result from any review of compliance, as a result of complaints or other significant changes – to ensure that the Code remains relevant to members, continues to meet application of Data Protection Law, and adapts to any changes in legislation;
- progress with the Code, such as how many Code Members and any issues encountered;
- a list of current Code Members; any new members admitted over the previous twelve months;
- information concerning Code Member breaches of Code requirements;
- details of any members suspended or excluded in the last 12 months; and
- outcomes of the Code Review.

Appendix I - Code Member Criteria & Requirements

The Code Member Criteria and requirements are set at a standard readily achievable by any business providing Code Services and represent the minimum requirement to achieve membership of the ABI and satisfy most Clients' expectations for their chosen provider of Code Services. However, Code Membership is available to any sector agency that meets the Code Member Criteria and requirements, whether a member of, or affiliated to, the ABI or not.

Code Member Criteria & requirements in detail		
All Code Members must satisfy requirements 1 to 14 set out below to the satisfaction of the Monitoring Body as detailed in paragraph 3.1 of the Code. **ABI Members will satisfy requirement 1 (i. to viii.) by virtue of their ABI membership.**		
Code Requirement		Supporting Evidence
1. At least one Principal of the Code Member's business must meet the criteria and provide the supporting evidence set out in this requirement.		An organogram or visual layout of the business structure showing persons in control, supported where relevant by up-to-date Companies House filings.
	i. Proof of identity and residential address.	Two certified forms of identity such as passport and driving licence and two proof of address documents such as a utility bill dated within the last three months.
	ii. Current professional indemnity insurance for the business with a minimum cover set at least £500,000.	A letter from the insurer confirming the required professional indemnity insurance cover is in place for the current period; OR any relevant certification of insurance.
	iii. ICO registration.	An up-to-date ICO registration certificate or a link to the ICO register with the correct contact and address details provided.

Code Member Criteria & requirements in detail		
	iv. A criminal conviction certificate (basic DBS disclosure) no older than 12 months for the first submission and no older than 3 years for each annual assessment.	A DBS application may be completed here https://www.gov.uk/request-copy-criminal-record.
	v. Two satisfactory professional or character references.	References to include work ethic, skills, strengths, and achievements and must include an endorsement of the applicant Code Member's honesty and suitability for Code Membership.
	vi. A comprehensive CV.	The CV must cover all qualifications, education and relevant work experience.
	vii. A personal and corporate financial probity check that is free of monetary judgments or insolvency. Any unsatisfied monetary judgments, undischarged insolvency, including debt relief order will disqualify from Code Membership.	A financial probity check can be completed through a variety of providers.
	viii. Work samples in the area of Code Services.	Two reports of work in the area of Code Services from the last two years with all Personal Data redacted. The cases reported must demonstrate the applicant Code Member's ability to communicate the outcomes of Code Services undertaken clearly and in a logical and orderly format.
2.Training	Adequate training and competence in Code Services and sector specific Data Protection Law requirements.	Satisfactory completion of data protection training to the level comparable to the ABI UK GDPR compliance workshop, or training to an equivalent standard on the areas covered by the Code, undertaken up to 12 months prior to application, and thereafter, every 3 years.

Code Member Criteria & requirements in detail		
		The MB may in its discretion consider other relevant and suitable qualifications.
	Maintenance of an adequate record of training completion and performance.	An up-to-date log of training completed, and scores achieved on any assessments undertaken. Evidence of course attendance or qualification certificate.
	Analysis of training needs to ensure that training provided is fit for purpose.	Evidence of usage of ABI comparable training modules to ensure that training covers the key areas of the Code.
	Training on roles and responsibilities.	Evidence of training addressing the differences between the roles of Controller, Joint Controller and Processor. A training requirement must be the Code Member assessing and explaining which role is undertaken in relation to hypothetical activities, and of the nature of the hypothetical processing under consideration.
	Training on DPIAs.	Evidence of training covering the requirements of Article 35 of the UK GDPR including: (i) carrying out a DPIA prior to processing commencing; and (ii) ensuring that a DPIA contains a description of processing, the necessity and proportionality of processing, an assessment of the risks to the rights and freedoms of Individuals and measures envisaged to address risks.
	Training on the lawful bases under Article 6 of the UK GDPR.	Evidence of training covering each of the lawful bases, when processing is necessary, why lawful bases for processing are important, how to decide which lawful basis applies, how to document the lawful basis and

Code Member Criteria & requirements in detail		
		what information needs to be provided to Individuals.
	Training on LIAs	Evidence of training covering completion of an LIA, when an LIA is required, assessment of the processing to decide on the outcome of an LIA, next steps after completion of the LIA and how LIAs overlap with DPIAs.
	Training on the seven Data Protection Principles.	Evidence of training outlining the seven Data Protection Principles under the UK GDPR and why the principles are important in the context of Code Services.
3. Legislative compliance	A legislation declaration confirming the Code Member's compliance with applicable legislation.	Code Members must review all relevant aspects of applicable legislation before making the legislation declaration. The declaration wording will be provided by the MB.
4.Roles and Responsibilities	The Code Member understands its role and responsibilities and documents and communicates them to its Clients accordingly. Code Members must understand the roles and responsibilities in respect of the data processing which they undertake. In accordance with Data Protection Law, and using the guidance in the Code, a Code Member must be able to establish if it is acting as a Processor, Controller, or a Joint Controller in relation to specific data processing.	Evidence (at the discretion of the MB) that the Code Member has documented and communicated to its Client the roles and responsibilities in respect of the data processing undertaken in the delivery of Code Services. This could be evidenced for example by providing a copy of the Client engagement letter and/or contract.
5. Case Extracts - DPIAs	Code Members must be able to determine when a DPIA is required and understand how to carry out the assessment.	A sample of up to three DPIAs which reflect the Code Member's range of services, redacted and anonymised, from live cases conducted by the Code Member during the previous 12 months. Or the review of a pre-existing DPIA, as required by the MB. The

Code Member Criteria & requirements in detail		
		DPIAs provided must be fully up to date and compliant with the requirements of Article 35 of the UK GDPR. The MB will take into consideration that the business may not regularly carry out DPIAs.
6. Case Extracts – Lawful Basis	Code Members, where necessary, must establish and appropriately document a lawful basis for data processing under Article 6 (and, where necessary, a condition under Article 9 or 10) of the UK GDPR, having considered the obligation under Article 5 of the UK GDPR for the Personal Data to be processed lawfully, fairly and in a transparent manner.	Case extracts, with an outline of the lawful basis relied on for the processing under Article 6, 9 and / or 10 of the UK GDPR and which demonstrates that the Code Member has considered its obligations under Article 5. Code Members must include evidence confirming that: (i) the purposes of processing activities have been reviewed and the most appropriate lawful basis has been chosen; (ii) the processing is necessary for the relevant purpose, and they are satisfied that there is no other reasonable and less-intrusive way to achieve that purpose; and (iii) where Special Category Data / Criminal Offence Data is processed, the conditions for processing such data are identified.

Code Member Criteria & requirements in detail		
7. Protection of children's interests	The Code Member pays particular attention to processing the Personal Data of children.	Evidence may include extracts from portfolios, LIAs or DPIAs or completing the ICO's self-assessment risk tool as found here for any pieces of work relating to children.
8. Criminal convictions register	Code Members must not maintain a comprehensive register of criminal convictions.	An annual written declaration confirming on-going compliance or alternative evidence which is accepted by the MB in its discretion.
9. Case Extracts – Legitimate Interests	The LIAs must determine the lawful basis for processing in accordance with Article 6(1)(f) of the UK GDPR. The three part test from the ICO's guidance here should be correctly applied.	A sample of up to three LIAs from live cases conducted by the Code Member which reflect the Code Member's range of services during the previous 12 months, as required by the MB. The MB will take into consideration that the business may not regularly carry out LIAs.
10. Lawful basis (legitimate interests – trace or locate)	The Code Member has considered and recorded the lawful basis appropriately in respect of Personal Data processing with reference to trace or locate instructions. Code Members are required to determine the appropriate lawful basis for processing and, where relying on legitimate interests as the lawful basis, keep a record of the LIA completed. In completing the LIA, the Code Member applies the three-part test.	There is no standard form for documenting the lawful bases for processing Personal Data, however Code Members must ensure that they can demonstrate that a lawful basis applies. This should explain, where relevant, any difference between the processing undertaken prior to locating an Individual and after locating an Individual. The Code provides guidance on this (see Part B paragraph 33 above) and the Code Member should use that guidance to support the evidence of the thought process in reaching a decision and justification of the outcome. Evidence may be required of any LIA undertaken, which includes the thought process in

Code Member Criteria & requirements in detail		
		reaching a decision and justification of the outcome. Code Members must include evidence confirming that: (i) the purposes of processing activities have been reviewed and the most appropriate lawful basis has been chosen; (ii) the processing is necessary for the relevant purpose, and they are satisfied that there is no other reasonable and less-intrusive way to achieve that purpose; and (iii) where Special Category Data / Criminal Offence Data is processed, the conditions for processing such data are identified.
11. Complaints	Code members must respond to Individuals' complaints received in accordance with the Code and guidance from the ICO. The MB may also investigate alleged breaches of the Code, and the Code Member must communicate with the MB in accordance with the Code and the cooperation criteria.	Evidence of any complaints received by the Code Member from Individuals in relation to data protection and the steps the Code Member took to respond to the complaint and where relevant, evidence that in relation to MB investigations of alleged breaches of the Code, the Code Member has communicated with the MB in accordance with the Code and the cooperation criteria in this Code ("Cooperates with the MB").

Code Member Criteria & requirements in detail		
12.Co-operates with the MB	Evidence that the Code Member has responded, or is able to respond, to any correspondence from the MB in full and address/remedy all issues raised within the required timeframe.	Code Members must provide a written response and enclose any relevant evidence to show that they are able to comply with the MB's requests which may include providing evidence of operational email accounts. Where the MB has communicated with the Code Member, the Code Member must provide evidence to show that it has corresponded appropriately with and cooperated with the MB, including in relation to any investigations of alleged non-compliance with the Code.
13. Address non-conformity report(s) (NCRs).	Full and adequate response to an NCR addressing and remedying all issues raised within the required timeframe.	Code Members must respond to an NCR issued by the MB by setting out in detail how they seek to address an NCR. Required actions may include updating DPIAs and LIAs to ensure compliance with Data Protection Law and providing further evidence of the lawful basis for processing Personal Data.
14. Knowledge	The Code Member has sufficient working knowledge of Data Protection Law.	Code Members are expected to be sufficiently knowledgeable in areas of Data Protection Law and procedure relating to Code Services, as covered in the Code. Applicants and Code Members may be asked specific questions on past work and should be able to demonstrate they are sufficiently knowledgeable about relevant Data Protection Law, as covered in the Code.

Appendix II - Data Protection Impact Assessment – Template (optional example)

Name of Controller Name of Controller contact Contact details	*Code Member*
DATA PROTECTION IMPACT ASSESSMENT **PROJECT NO: .....**	
1: The need for the DPIA: Explain broadly what the project aims to achieve and what type of processing it involves. Summarise the need for a DPIA. We consider whether to do a DPIA if we plan to carry out any: i. evaluation or scoring; ii. automated decision-making with significant effects; iii. systematic monitoring; iv. processing of sensitive data or data of a highly personal nature; v. processing on a large scale; vi. processing of data concerning vulnerable Individuals; vii. innovative technological or organisational solutions; viii. processing that involves preventing Individuals from exercising a right or using a service or contract. We always carry out a DPIA if we plan to: ix. use systematic and extensive profiling or automated decision-making to make significant decisions about people; x. process Special Category Data or Criminal Offence Data on a large scale; xi. systematically monitor a publicly accessible place on a large scale; xii. use innovative technology; xiii. use profiling, automated decision-making or Special Category Data to help make decisions on someone's access to a service, opportunity, or benefit; xiv. carry out profiling on a large scale; xv. process biometric or genetic data; xvi. combine, compare, or match data from multiple sources; xvii. process Personal Data without providing a privacy notice directly to the Individual; xviii. process Personal Data in a way that involves tracking Individuals' online or offline location or behaviour; xix. process children's or other vulnerable individuals' Personal Data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them; xx. process Personal Data that could result in a risk of physical harm in the event of a security breach; xxi. process Personal Data that could result in a risk of the denial of service (product, opportunity, or service). [Note: The Code Member may be able to justify a decision not to carry out a DPIA if it is confident that the processing is despite any of the above criteria unlikely to result in a high risk, but the reasons for this decision must be documented. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of Personal Data. In some cases, a DPIA may be needed if only one of the above factors is present	**Code Member's answers / conclusions**

2: Describe the processing:

a. NATURE: describe the nature of the processing:

	Code Member's answers / conclusions
i. How data is -	
a. Collected and sourced.	
b. Stored.	
c. Used and deleted.	
ii. Who has access to the data?	
iii. With whom is the data shared, e.g. Client, sub-contractor?	
iv. What are the retention periods?	
v. What are the security measures?	
vi. Are any new technologies being used?	
vii. Whether any novel types of processing are to be used?	
viii. What types of processing identified as likely high risk are involved?	

b. SCOPE: what the processing covers:

i. The nature of the Personal Data.	
ii. The volume and variety of the Personal Data.	
iii. The sensitivity, including whether it includes Special Category Data and / or Criminal Offence Data.	
iv. The extent and frequency of the processing.	
v. The duration of the processing.	
vi. The number of Individuals involved.	
vii. The geographical area covered.	

c. CONTEXT: the wider picture, including internal and external factors which might affect expectations or impact:

i. The source of the data.	
ii. The nature of your relationship with the Individuals.	
iii. How far Individuals have control over their data.	
iv. How far Individuals are likely to expect the processing.	

v. Whether these Individuals include children or other vulnerable people.	
vi. Compliance with relevant code of practice, guides, policies.	
vii. Any previous experience of this type of processing.	
viii. Any relevant advances in technology or security.	
ix. Any current issues of public concern.	
x. ABI UK GDPR code of conduct membership link to register entry.	
d. PURPOSE: it is important to establish the purpose, for example ask yourself what you want to achieve?	
i. Your or your Client's legitimate interests, where relevant.	
ii. The intended outcome for Individuals.	
iii. The expected benefits for the Code Member or its Client	

3: **Consultation process:**	**Code Member's answers / conclusions**
Consider how and when to consult with relevant stakeholders, for example: i. Sub-contractors or industry experts. ii. Data protection consultant or professional body, if necessary. iii. Anyone else in the Code Member's organisation. iv. Individual, such as in the trace / locate (consent to share) scenarios. Where appropriate, consult relevant stakeholders in some form. However, if you decide this is not appropriate, you must record this decision here, with a clear explanation. For example, you may be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.	
Assess necessity and proportionality: Consider: i. Will the processing achieve the purpose? ii. Is there any other reasonable way to achieve the same result? Explain: iii. The lawful basis for the processing.	

iv. How processing for incompatible or different purposes to those for which the data was obtained by the Code Member will be prevented. v. Measures in place to ensure – a. Data quality. b. Data minimisation. c. The provision of privacy information to Individuals. d. That Individual's rights are supported. e. Sub-contractors' compliance.	

5: Identify and assess risk:

Consider the potential impact on Individuals and any harm or damage the processing may cause – whether physical, emotional, or material. In particular, look at whether the processing could contribute to any of the items listed below:

To assess whether the risk is a high risk, the Code Member needs to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm may still count as high risk.

An example of a high risk is an illegitimate access to data leading to a threat on the life of the Individuals, a layoff and / or a financial jeopardy.

The purpose of the scoring system below is to encourage careful consideration of and reflection on relevant risks. If the check reveals an "overall score" of 3+ in any particular sub-category, this may indicate high risk processing.

		Code Member's answers / conclusions		
		Remote (1), possible (2), or probable (3)	***Minimal (1), significant (2), or severe (3)***	***Total score***
i.	Inability to exercise rights (including but not limited to privacy rights).	Likelihood of harm	Severity of harm	Overall risk
ii.	Inability to access services or opportunities.	Likelihood of harm	Severity of harm	Overall risk
iii.	Loss of control over the use of Personal Data.	Likelihood of harm	Severity of harm	Overall risk
iv.	Discrimination.	Likelihood of harm	Severity of harm	Overall risk
v.	Identity theft or fraud.	Likelihood of harm	Severity of harm	Overall risk
vi.	Financial loss.	Likelihood of harm	Severity of harm	Overall risk
vii.	Reputational damage.	Likelihood of harm	Severity of harm	Overall risk
viii.	Physical harm.	Likelihood of harm	Severity of harm	Overall risk
ix.	Loss of confidentiality.	Likelihood of harm	Severity of harm	Overall risk
x.	Re-identification of data.	Likelihood of harm	Severity of harm	Overall risk

xi.	Any other significant economic or social disadvantage.	Likelihood of harm	Severity of harm	Overall risk
xii.	Security risks (including sources of risk and the potential impact of each type of breach). You should consider illegitimate access to, modification of or loss of Personal Data.	Likelihood of harm	Severity of harm	Overall risk
xiii.	Any other risks not previously anticipated.	Likelihood of harm	Severity of harm	Overall risk

6: Identify measures to reduce risk:

Identify additional measures that could be taken to reduce or eliminate risks identified as medium or high risk in step 5.
You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing.
Against each risk identified, record its source.
Consider options for reducing that risk. For example:

Options to reduce / eliminate risk:		**Code Member's answers / conclusions**			
		Risks reduced from section 5	***Eliminated (E), Reduced (R), or Accepted (A)***	***Low (L), Medium (M), or High (H)***	**Measure approved**
i.	Deciding not to collect certain types of data.	Which risks	Effect on risk	Residual risk	Y/N
ii.	Reducing the scope of the processing.	Which risks	Effect on risk	Residual risk	Y/N
iii.	Reducing retention periods.	Which risks	Effect on risk	Residual risk	Y/N
iv.	Taking additional technological security measures.	Which risks	Effect on risk	Residual risk	Y/N
v.	Training staff to ensure risks are anticipated and managed.	Which risks	Effect on risk	Residual risk	Y/N
vi.	Anonymising data where possible.	Which risks	Effect on risk	Residual risk	Y/N

vii.	Writing internal guidance or processes to avoid risks.	Which risks	Effect on risk	Residual risk	Y/N
viii.	Using a different technology.	Which risks	Effect on risk	Residual risk	Y/N
ix.	Making changes to privacy notices.	Which risks	Effect on risk	Residual risk	Y/N
x.	Offering Individuals, the chance to opt out where appropriate.	Which risks	Effect on risk	Residual risk	Y/N
xi.	Implementing new systems to help Individuals to exercise their rights.	Which risks	Effect on risk	Residual risk	Y/N
xii.	Other.	Which risks	Effect on risk	Residual risk	Y/N
xiii.	Other.	Which risks	Effect on risk	Residual risk	Y/N

7: Sign off and record outcomes:	**Code Member's conclusions**
Finally, you should record: i. what additional measures you plan to take; ii. whether each risk has been eliminated, reduced, or accepted; iii. the overall level of 'residual high risk' after taking additional measures; iv. whether you need to consult the ICO; and v. advice from DPO on whether processing can proceed.	

Item	Name / position / date	**Code Member's notes**
Measures approved by:		
Residual risks approved by:		
This DPIA will be kept under review by:		

Appendix III - Legitimate interests or consent examples

The following are brief examples of where the Code Member (when processing Personal Data as Controller) may consider legitimate interests or consent as the appropriate lawful basis. It is important for the Code Member to carry out its own LIA in each case to ensure all parts of the LIA three-part test are met prior to any processing. Reference is made to Part B paragraph 31 above, which discusses legitimate interests.

CLIENT'S INSTRUCTIONS	PURPOSE	CODE MEMBER'S ACTION	SAFEGUARDS
Trace the whereabouts of a member of the Client's family.	Re-establish contact.	The Code Member might accept the Client's instructions on the condition that if the Individual is located, the Code Member will have to undertake new processing to contact the Individual to explain the instructions. This post trace processing would require an appropriate lawful basis which will be fact sensitive. Specifically, if the Code Member relies on the lawful basis of consent, but is unable to obtain consent from the Individual, then it will not be able to process the Personal Data further. If the Code Member relies upon legitimate interests, then it must consider whether it has met the requirements of the 3-part LIA without the consent of the Individual. This will be a fact-sensitive and case-by-case assessment and further guidance is referred to in Part B paragraph 32 above.	If the Code Member's legitimate interests override the rights of the affected Individual in the Code Member's LIA 3-part test, the Code Member may proceed with pre-trace processing. Thereafter the Code Member will need to carry out a further LIA for any additional processing if it proposes to rely on the lawful basis of legitimate interests. Alternatively, the Code Member may rely on consent if the Individual consents to the further processing.
Trace the whereabouts of a friend.	To join a social network group.		
Trace the whereabouts of a former acquaintance.	To inform of some event, e.g., death of mutual friend.		
Trace the whereabouts of a work colleague.	To collaborate on potential case against employer.		
Trace the whereabouts of a beneficiary (probate estate).	To advise of inheritance.		
Trace the whereabouts of an Individual who is indebted to the Client and / or against whom the Client has a legal claim; for example, under a contract or a tort, ahead of, or in support of a legal action.	To enable the Client to commence a lawful debt recovery process and / or legal proceedings.	The Code Member, if satisfied as to authenticity of the Client's instructions, may accept the instructions and proceed to process and report the relevant Personal Data, on the basis that the Client has a legitimate interest that outweighs the interests and fundamental rights of the Individual. The Individual, in any event, is unlikely to consent to the processing of their Personal Data for the Client's purpose.	Subject to the legitimate interests of the Code Member or Client overriding the rights of the affected Individual in the Code Member's LIA three-part test, no further safeguards such as the Individual's consent would be required or likely to be forthcoming and seeking consent might compromise the Client's purpose.

DOMESTIC SCENARIOS			
CLIENT'S INSTRUCTIONS	PURPOSE	CODE MEMBER'S ACTION	SAFEGUARDS
Trace the whereabouts of a former spouse / partner / cohabitee.	Client's curiosity.	The Code Member's LIA three-part test is likely to conclude that the Client's purpose does not give rise to a legitimate interest. However, if a compelling reason exists the Code Member may consider processing limited to locating the Individual so that it can seek the Individual's consent prior to any further processing, in particular the sharing of the Individual's contact information. In the event consent is declined, the Code Member must cease further processing including the deletion of the Personal Data.	Curiosity is unlikely to be a legitimate interest overriding the rights of the affected Individual in the Code Member's LIA 3-part test.
The Client requires observation of their cohabiting partner.	The Client has reasonable cause to suspect their partner's financial mismanagement.	The purpose is potentially contentious, and the Client has a legitimate interest that outweighs the interests and fundamental rights of the Individual. If the Client's suspicion is found to be true, the Individual may expose the Client to some financial risk or other harm.	Subject to the legitimate interests of the Code Member or Client overriding the rights of the affected Individual in the Code Member's LIA three-part test, the Code Member may proceed with the processing. Where Special Category Data or Criminal Offence Data may be required to be processed, the Code Member must meet a relevant Article 9 (Special Category Data) or Article 10 (Criminal Offence Data) condition as well as establishing the lawful basis for the processing under Article 6 .

DUE DILIGENCE / BACKGROUND CHECKS			
CLIENT'S INSTRUCTIONS	PURPOSE	CODE MEMBER'S ACTION	SAFEGUARDS
To investigate the background and / or financial reliability of the Individual.	In anticipation of the Client's commitment to investing in the Individual's business following an approach by the Individual.	The Client requires due diligence to be carried out on the Individual to mitigate the risks to the Client's financial exposure and / or reputation. The Individual would reasonably expect the Client to undertake	Subject to the legitimate interests of the Code Member or Client overriding the rights of the affected Individual in the Code Member's LIA three-part test the Code Member may proceed. However, where no

		such an investigation prior to making the investment.	approach has been made by the Individual and the Client's interest is exploratory, the processing would be Invisible Processing and not be justified. The Code Member might consider obtaining the Individual's consent prior to any processing.

End notes:

[1] https://ico.org.uk/for-organisations/guide-to-dp/guide-to-the-uk-gdpr/code-of-conduct-detailed-guidance/ico-register-of-uk-gdpr-code-of-conduct/.
[2] https://www.theabi.org.uk/files/applications-for-membership/membership-criteria-full-provisional.pdf
[3] A list of Code Members can be found on the ABI website https://www.theabi.org.uk/abi-uk-gdpr-code-member-register.
[4] See ICO guide on exemptions at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/.
[5] Please refer to the ICO's Regulatory Action Policy available at: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
[6] Harm, in this context, can include physical, material, or non-material damage as set out in Recital 75 of the UK GDPR which may impact the rights and freedoms of natural persons as a result of Personal Data processing.
[7] *Refer to* endnote 5.
[8] The ICO's website provides detailed information and guidance on the roles of Controllers and Processors https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/Controllers-and-Processors/.
[9] (ICO Website ico.org.uk/, and licensed under the Open Government Licence).
[10] *Refer to* endnote 9.
[11] *Refer to* endnote 9.
[12] *Refer to* endnote 9.
[13] See ICO guide and template: https://ico.org.uk/for-organisations/sme-web-hub/make-your-own-privacy-notice/.
[14] *Refer to* endnote 9.
[15] Available at: https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/.
[16] Consent is defined in UK GDPR Article 4(11) as: "*Any freely given, specific, informed and unambiguous indication of the Individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her*".
[17] See ICO guide: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/are-there-any-exceptions/
[18] What is Criminal Offence Data? | ICO.
[19] appropriate-policy-document.docx (live.com).
[20] Refer to endnote 19.
[21] The Code Member must be able to justify why processing of this specific data is necessary to establish, exercise or defend the legal claim. The use of this data must be relevant and proportionate, and the Code Member must not process more data than is needed.
[22] Available at: legitimate interests assessment (LIA) template
[23] For further information, please consult https://www.ukas.com/.
[24] https://www.theabi.org.uk/files/policies-and-guidance/discipline/disciplinary-flow-chart.pdf