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

   Accredited as a MB by the ICO on [•].

[APPROVED BY:

The Information Commissioner's Office (ICO) on [•]. **[Note: the current draft is not ICO approved]]**

[VERSION INFORMATION:

This is Version 1 of the Code and is dated [•]]

PUBLISHING AND COPYRIGHT INFORMATION:

Published by ABI **/**/2022

Table of Contents

1. Introduction

1.1 The EU General Data Protection Regulation 2016/679 as it forms part of the domestic law of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act 2018 ("**DPA**", together with the UK GDPR, applicable case law and mandatory code of practice, the "**Data Protection Law**") introduced significant new requirements in relation to how British private investigators should handle personal data. It is important that business and the public have confidence in the data handling practices of the sector. The Association of British Investigators ("**ABI**") has worked in consultation with members of the ABI ("**ABI Members**"), the Credit Services Association, the Chartered Institute of Credit Management, the Law Society of England & Wales jointly with the Solicitors Regulation Authority, law enforcement bodies and members of the public to produce this voluntary Data Protection Code of Conduct for Investigative & Litigation Support Services (the "**Code**").

1.2 The purpose of the Code is to demonstrate the knowledge of and compliance with specific areas of Data Protection Law particularly engaged by Investigation and Litigation Support Services. Certified adherence to the Code is intended to give confidence to users of investigative and Litigation Support Services that Code Members (as defined below) have demonstrated compliance with key aspects of Data Protection Law and a high standard of protection and accountability to the satisfaction of an independent monitoring body ("**MB**").

1.3 The Code builds on the existing standards and criteria required for ABI membership. Code Members are not required to be ABI Members. Code Members will be required to meet certain of the same criteria, as for membership of the ABI, along with additional criteria. These, together, form the Criteria (as defined below) set out in Appendix V of the Code.

1.4 The ABI has worked with the Information Commissioner's Office ("**ICO**") to ensure the Code meets the requirements of Data Protection Law. [This version of the Code was approved by the ICO on [●]]. Nothing in the Code removes the powers of the ICO in respect of the enforcement of Data Protection Law. For more information about Codes of Conduct, please see the ICO's guidance and register of UK GDPR Codes of Conduct[1].

1.5 The Code is issued under Article 40 of the UK GDPR. Monitoring compliance with the Code is carried out by an impartial 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 publication of the first edition of the Code, there is one MB for the Code, which is the Security Systems and Alarms Inspection Board ("**SSAIB**").

[1] https://ico.org.uk/for-organisations/guide-to-dp/guide-to-the-uk-gdpr/codes-of-conduct-detailed-guidance/ico-register-of-uk-gdpr-codes-of-conduct/

1.6 The Code is in three parts, plus Appendices. Part A explains the scope, objectives, context, and benefits of the Code. Part B delivers guidance on the Key Issues on which the Code will focus: roles and responsibilities; lawful basis; legitimate interest assessment; and Data Protection Impact Assessment ("**DPIAs**") (as defined below). Part C explains how the Code is managed and how infringements are dealt with. The appendices provide template documents, specific guidance on other aspects of Data Protection Law as relevant to Code Members, Criteria for Code Members, and the main activities within the scope of the Code Appendix I (Activities).

1.7 The Association of British Investigators Limited (ABI) is a voluntary individual members' professional body with membership criteria available on its website[2].

2 https://www.theabi.org.uk/become-a-member

2. Definitions

ABI Member	Full or provisional member of the ABI.
Activities	The activities frequently undertaken in private investigator's provision of Investigations and Litigation Support Services, detailed in Appendix I (Activities).
APD	Appropriate policy document relating to a Code Member's processing of Criminal Offence Data to satisfy the requirements of Data Protection Law.
BYOD	Allowing staff to use their own devices in the workplace.
Client	The legal person requesting the Code Services.
Code Member	As defined in Part A paragraph 3.1 below and shall include prospective Code Members as the context requires and permits.
Code Owner	The Association of British Investigators Limited (by guarantee) registered in England & Wales number 00998568 with its registered office situate at Brentano Suite, Catalyst House, Centennial Park, Centennial Avenue, Elstree WD6 3SY.
Code Review	The review of the Code by the ABI and MB in accordance with Part C paragraph 37.1 of the Code.
Code Review Framework	A framework for the review of the Code agreed between the ABI and MB.
Code Services	Services and activities (including the Activities) related to Investigations or Litigation Support Services performed by the Code Member.
Controller	The natural or legal person, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Please refer to Part B of the Code for detailed discussion about the role of Controllers.
CPD	Continuous Professional Development.
Criminal Offence Data	Personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. It may include related measures, including topics such

	as bail, bail conditions and community orders and their terms.
Criteria	The specific measurable controls which the MB will assess compliance with in the review and monitoring process set out in Appendix V.
Data Subject	Any living individual who can be identified, directly or indirectly, via an identifier such as a name, an identity number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.
DPIA	Data Protection Impact Assessment is a risk assessment used when processing is likely to result in a high risk to the rights and freedoms of natural persons under Data Protection Law as defined in Part A paragraph 4.1.2.
General Business Administration	Internal business processing, such as Client onboarding, Client AML verification, payroll and other administrative processes.
Investigations	As defined in the Private Security Industry Act 2001: "surveillance, enquiries or investigative activities that are carried out for the purposes of obtaining information about; a particular legal person or about the activities, status, or whereabouts of a particular legal person, or the circumstances in which, or means by which, property has been lost, stolen, damaged or altered, or any other activities ancillary to current or anticipated legal proceedings, conducted under instruction of a Client".
Joint Controller	Two or more Controllers which, jointly, decide the means and purposes of the processing.
Key Issues	The key issues which the Code will consider as defined in Part A paragraph 4.1 below.
LIA	Legitimate Interest Assessment as set out in Part A paragraph 4.1.4 below.
Litigation Support Services	Services, including Investigations, rendered by an investigation agency to legal professionals in contentious scenarios in contemplation of, or during, legal proceedings.
MB	The monitoring body 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. Please refer to Part C of the Code for further information about the MB.
Personal Data	Information relating to an identified or identifiable Data Subject; an identifiable Data Subject is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that Data Subject.
Processor	a natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Controller.
Special Category Data or Special Categories of Data	Has the meaning given in Article 9 UK GDPR.
SSAIB	The Security Systems and Alarms Inspection Board www.ssaib.co.uk. It was 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*).

PART A – EXPLANATORY STATEMENT

3. Scope

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

3.1.1 is an ABI Member or a non-member that (as determined by the MB) meets the Criteria;

3.1.2 has demonstrated, to the satisfaction of the MB, competence, good practice and compliance with Data Protection Law, within the scope of this Code; and

3.1.3 has been granted "Code Member" status by the MB and added to the register of Code Members,

(each a "**Code Member**"). A list of Code Members can be found on the ABI website[3] or by contacting the ABI by email secretariat@theabi.org.uk.

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, including each of the Activities in Appendix I below. This may include the processing of Personal Data of enquiry subjects, witnesses, informants, or their affiliates. The Code does not cover Code Members' responsibilities under Data Protection Law relating to General Business Administration.

3.3 The Code does not cover all a Code Member's obligations under Data Protection Law. The Code is designed to provide enhanced assurance and reduce the data protection-related risks of instructing Code Members to undertake Code Services[4].

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

3.5 This Code applies to Code Members which are subject to Data Protection Law. It applies to Code Members' Code Services but does not apply to transfers of Personal Data to outside of the UK by Code Members, for the purposes of Article 46(2)(e) of the UK GDPR.

4. Code Objectives

4.1 The purpose of the Code is to provide sector-specific guidance to assist with Data Protection Law compliance and to assess Code Members against the Criteria. As referred to at Part A paragraph

[3] https://www.theabi.org.uk/code-register

3.3 above, the Code does not cover all aspects of Data Protection Law and will focus on issues that are specific to the sector in which Code Members operate. The ABI has identified as particularly problematic for private investigators. The Code covers how the following key issues (the "**Key Issues**") apply to the Code Services:

4.1.1 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 interacting with Personal Data. A Code Member should determine its role when processing Personal Data and take reasonable steps to ensure that any third party it is dealing with agrees to comply with its obligations under Data Protection Law, to the extent necessary under the Code.

4.1.2 The requirement under Article 35 of the UK GDPR to conduct an assessment of the impact of the envisaged processing operations on the protection of Personal Data, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons (a data protection impact assessment or "**DPIA**"). Code Members should 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.

4.1.3 Identification of the correct lawful basis for the processing of Personal Data. Code Members, where necessary, should establish and appropriately document a lawful basis for data processing under Article 6 (and, where necessary, a condition under Article 9 or 10) 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.

4.1.4 To the extent that the lawful basis for any processing is the legitimate interests of the data Controller or a third party under Article 6(1)(f) of the UK GDPR, the assessment of whether those interests are overridden by the interests or fundamental rights and freedoms of the Data Subject. Code Members should have completed an assessment of the legitimate interests involved in the processing (a legitimate interests assessment or "**LIA**"), whether the processing is necessary for those interests and the balancing test of those interests set against Data Subjects' rights, including completion of the three-part test that the ICO has set out[5].

4.2 In addition to the Key Issues at Part A 4.1.1 to 4.1.4, the Code will provide Code Members with specific guidance on the data protection principles (at Appendix II), examples of the application of the Key Issues at Part A paragraph 4.1 above, and a template DPIA (at Appendix IV) to the extent

[5] Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests

relevant to the Code Services. The Code does not extend to data protection responsibilities for the purposes of General Business Administration and does not represent all of a Code Member's responsibilities under Data Protection Law.

5. Background

5.1 The ICO, in guidance on disclosing information to private investigators[6] (issued under the Data Protection Act 1998), explained that private investigators undertake a wide variety of work including tracing debtors, acting on behalf of individuals in disputes, and tracing beneficiaries (Appendix I (Activities) contains further information about the activities of private investigators). These Activities frequently require the processing of Personal Data.

5.2 Private investigators have had action taken against them by the ICO for breaches of Data Protection Law, including under previous data protection legislation[7]. Beyond the risk of prosecution, private investigators have challenges when meeting the requirements of Data Protection Law that this Code addresses. The following examples explain some of the sectoral challenges facing private investigators. Further examples are found in Part B.

5.2.1 A Code Member may find it challenging to manage Client expectations while still meeting the applicable Data Protection Law requirements in respect of roles and responsibilities. An instructing Client may not understand a Code Member's role for certain processing activities and the Code Member has a responsibility to ensure that, as applicable, it complies with its obligations as a Controller or Processor. Where necessary, the Code Member may also need to explain its role and Data Protection Law obligations to its Client and any consequences (such as timescales or costs to accommodate the applicable requirements) that the role may have on the instructions given to the Code Member.

5.2.2 Private investigators are regularly instructed by lawyers to assist in contentious matters involving court proceedings such as civil litigation or, where relevant, other Code Services. This may involve processing Personal Data that is subject to legal professional 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 right to be informed, the right of access and from the principles of Data Protection Law, insofar as they relate to these rights. As Code Members are likely to be processing Personal Data in respect of which Data Subjects'

[6] Available at https://ico.org.uk/media/1556/disclosures_to_private_investigators.pdf

[7] See, for example, the widely-reported convictions of Woodgate and Clark Ltd [https://www.theabi.org.uk/news/instruct-unregulated-pis-at-your-peril]or ICU Investigations Ltd [https://www.bbc.co.uk/news/uk-england-27162574] under Section 55 of the Data Protection Act 1998.

rights are limited, it will be particularly important for them to be able to demonstrate that they are doing so in a compliant manner.

5.2.3 Code Members should make their Clients aware that the processing of Personal Data must be carried out in compliance with Data Protection Law, despite the challenges such as those in Part A paragraphs 5.2.1 and 5.2.2 above. Code Members should consider declining or clarifying instructions that do not comply with Data Protection Law, including the data protection principles set out in Appendix II below.

6. Benefits

6.1 Data Protection Law aims to ensure that Data Subjects can trust Controllers and Processors to use their data fairly and responsibly. Data Protection Law requires Controllers and Processors to think about and justify how and why they use Personal Data. Some of the key benefits of the Code for Code Members are:

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

6.1.2 the fact that they have received training on systems that safeguard Personal Data within the scope of the Code Services;

6.1.3 a clearer understanding of the data protection principles and how they apply to Code Members;

6.1.4 credibility in the eyes of potential Clients considering the Code Member's credentials in relation to Code Services;

6.1.5 for some, the advantage of being an early adopter of the Code as more private investigators apply for Code Member status;

6.1.6 confidence from Data Subjects that their rights will be respected, for Code Services purposes; and

6.1.7 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 regarding the breach of Data Protection Law in (ii)[8].

[8] 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

6.2 The ABI considers that the points at Part A paragraphs 6.1.1 to 6.1.7 above will also engender a greater awareness of the need for general compliance with Data Protection Law (as well as the specific compliance with the Code) within the Investigations and Litigation Support Service sector.

7. Added value

7.1 In most Investigations the processing of Personal Data has a degree of risk of harm to Data Subjects[9]. This risk can be wide-ranging, including financial and emotional harm as well as harm which will have lasting impacts on the lives of those affected. Code Membership status is intended to increase the accountability of operators in the sector by assessing compliance with the Key Issues.

7.2 The Code increases accountability of the sector to the public by codifying guidance and good practice in relation to the Key Issues for the sector, giving a framework for independent monitoring and a framework for annual compliance audits by a MB.

7.3 The Code Member applies the guidance on Data Protection Law compliance within the scope of the Code, overseen by an independent, ICO- accredited MB.

7.4 Awareness of the Code may affect the instructions provided to Code Members from lawyers, insurers, financial services, commerce, private Clients, and other sectors, including documenting the data protection roles and responsibilities of the parties. As mentioned in Part A paragraph 6.1.7, the ICO shall take into account Code Membership status, and compliance with the Code, as an aggravating or mitigating factor (as relevant) when considering enforcement action against a Code Member[10].

[9] harm, in this context, can include physical, material or non-material damage as set out in Recital 75 of the UK GDPR which may be done to the rights and freedoms of natural persons as a result of Personal Data processing.

[10] *Ibid* footnote 8 p.11-12

PART B – CODE OF CONDUCT CORE REQUIREMENTS

8. Introduction

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

8.1.1 Roles and responsibilities;

8.1.2 DPIAs;

8.1.3 Lawful basis; and

8.1.4 LIAs.

8.2 To achieve Code Member status, a candidate for Code Member must be able to demonstrate its compliance in relation to these Key Issues, by fulfilling the Criteria in Appendix V to the satisfaction of the MB.

9. Roles & responsibilities

9.1 Determining a Code Member's role in processing Personal Data as a Controller or Processor is fundamental to understanding their responsibilities under Data Protection Law. Determination of the role is a question of fact and requires careful consideration of the relevant processing. A Code Member or its Clients cannot choose their role and responsibilities – they will be determined by the facts of the processing.

9.2 Failing to properly understand their role and responsibilities will make it very difficult for the Code Member to comply with Data Protection Law or give Clients confidence in its Personal Data processing abilities[11].

10. Controller

10.1 Data Protection Law defines a "Controller" as a legal person or entity that, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

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

[11] 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/

10.3 When a Client is instructing a Code Member to perform Code Services for domestic or household purposes, the Code Member will be a Controller, rather than a Processor or Joint Controller, for this processing. This is because the Client will not have data protection responsibilities of its own.

11. Processor

11.1 Data Protection Law defines a "Processor" as a legal person or entity that processes Personal Data on behalf of the Controller and under their authority. Although a Processor may make its own day-to-day operational decisions, it should only process Personal Data in line with a Controller's instructions, unless it is required otherwise by law.

11.2 Code Members more typically act as Controllers in respect of their Code Services. This is based on the fact that Code Members often receive instructions that require them, at some stage of the instructions, to determine how and why Personal Data is processed.

11.3 However, there may be certain Activities for which the Code Member acts on instructions as to the purpose and the essential means of the processing, in these cases, it will be a Processor. Examples relevant to Code Members are set out at Part B paragraph 16 below.

11.4 There may be some situations in which a Code Member is both a Controller and Processor of the same Personal Data, where it is carrying out certain Activities on that data as Controller and other processing activities on the same data as Processor. An example is at paragraph 17 below.

12. Controller responsibilities

12.1 Data Protection Law sets out prescriptive responsibilities for Controllers (including Joint Controllers), because they are making decisions about the means and purposes of the processing of Personal Data. The responsibilities of a Controller are set out in Data Protection Law, and specific guidance, where relevant, is included within the Code.

12.2 Individuals affected by the processing of their Personal Data can bring direct claims against a Controller if that processing breaches Data Protection Law. The ABI has seen cases where the processing has infringed Data Protection Law and caused harm, which has led to enforcement action and claims by Data Subjects or Clients against private investigators. If parties are acting as Joint Controllers, then they are jointly and severally liable for the processing that they're carrying out jointly. Private investigators may sometimes act as Joint Controller with their Client (as explained at Part B paragraph 17 below), which would mean that a claim may be made against either of them in respect of their joint processing.

12.3 Even when receiving instructions on specific tasks, the Code Member may be a Controller for the purposes of Data Protection Law. Due to the nature of the work, a private investigator will often determine what Personal Data is necessary and how it should be processed, in order to provide its

services. A Code Member may determine certain non-essential means of its processing and still be a Processor. However, if the Code Member is exercising significant discretion and determining any of the essential means of processing, or any of the purposes, then they are likely to be acting as a Controller.

12.4 In order to determine whether it is acting as a Controller, the Code Member must establish whether it is determining the purposes and essential means of that particular processing. In particular, the Code Member should reflect on whether it has discretion over any of the following:

12.4.1 **the purpose/s for the processing.** The ABI has found that frequently, ABI Members receive instructions that require them to follow new leads. These new leads could, in turn, lead to business development opportunities with the data beyond the initial scope of the instructions. In that circumstance, a Code Member would be deciding whether purpose of the new processing (i.e. using that data for business development purposes) and would therefore be likely to be acting as a Controller for that new processing;

12.4.2 **which types of data will be collected and processed.** When searching a database using the Data Subject's details provided by the Client (such as name, and/or date of birth, and/or address) the Code Member is likely to be acting as a Processor. However, if the Code Member identifies other Personal Data through that search (such as email, contact number, social media profile, previous or forwarding address) and decides whether that additional Personal Data is processed for the purpose of providing its services, then this is one of the factors that would establish the Code Member as a Controller when processing this additional Personal Data;

12.4.3 **which individuals to collect data about**. When searching for a Data Subject, the Code Member may identify other individuals' Personal Data such as cohabitees, previous occupants, current occupants, or business associates. To the extent that the Code Member exercised its professional skill and judgement in deciding whether those other individuals' Personal Data is processed to provide its services, this is one of the factors that would establish the Code Member as a Controller when processing Personal Data of these individuals;

12.4.4 **whether the data should be disclosed and to whom.** For example, when searching for the beneficiary of an estate, a Code Member may have to consider whether to disclose the instructing Client's Personal Data as part of the search. The Code Member would be likely to be acting as a Controller to the extent that the disclosure was not part of the initial instructions;

12.4.5 **whether and for how long the data will be stored.** If the Code Member determines this, it is likely to be Controller. Processors must follow their Controller's instructions in relation to

retention and deletion and must generally return or delete Personal Data at the end of the engagement. However, the circumstances of the case may mean that the decision on retention is left to the Code Member. Almost all the Personal Data processed by a Code Member for the purposes of Client engagements has the potential of being treated as evidence in litigation. The Code Member may therefore decide that a retention period is appropriate to meet any potential evidential responsibilities and legal obligations that could arise if a claim is reasonably in prospect. The Code Member would be likely to be acting as a Controller if deciding the length of time for which Personal Data should be stored, or whether to store or delete it at all; and

12.4.6 **how to respond to requests made in line with individuals' rights.** For example, whether and how to deal with any subject access request from a Data Subject. If yes, then the Code Member is likely to be Controller.

13. Processor responsibilities

13.1 The responsibilities of a Processor are prescribed both under Data Protection Law, under Article 28 of the UK GDPR, and in the instructions and contracts with the Controller. Processors have less independence and authority over the processing of Personal Data they undertake on behalf of the Controller, as they must generally follow the Controller's instructions about the Personal Data. The responsibilities of a Processor are set out in Data Protection Law, and specific guidance, where relevant, is included within the Code.

13.2 Processors may also be subject to additional responsibilities under the contracts they are required to have in place with Controllers. For example, a Controller may instruct a Processor to apply specific security measures commensurate with ISO27001 for certain processing. Alternatively, a Controller may contractually oblige its Processor to notify the Controller of Personal Data breaches within a specific timescale, rather than the statutory requirement to do so, without undue delay.

14. Joint Controller responsibilities

14.1 Joint Controllers jointly determine the purposes and means of processing together and they have the same or shared purposes. Controllers will not be Joint Controllers if they are processing the same data for different purposes.

14.2 Joint Controllers need to decide which Controller will carry out which obligation under the UK GDPR and allocate these responsibilities in a written agreement. Regardless of those allocations, each Controller retains responsibility for complying with the obligations on Controllers under the UK GDPR.

14.3 Data subjects may exercise their rights against each Joint Controller and a Joint Controller can be liable for the entire damage to an individual caused by the joint processing, unless it can provide it

is not responsible for the event giving rise to the damage. The arrangement between Joint Controllers may allocate risk as between the Joint Controllers in relation to any liability caused by the processing.

14.4 Examples of processing activities for which a Code Member is likely to be a Joint Controller alongside the Client are set out at paragraph 18 below.

15. Controller examples

15.1 Code Members often need to process Personal Data in a manner not envisaged in the original instructions and a situation may change at such a pace that the Code Member cannot reasonably revert to the Client for 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 would place it into the role of a Controller, either solely or jointly with the instructing Client.

15.2 Set out below are some common examples.

Controller examples:

1. A Client requires the Code Member to identify and locate individuals who are potential witnesses relevant to an ongoing dispute. The Client has not provided a list of the potential witnesses or the processing of Personal Data that the Client would like to be carried out, beyond identifying the ongoing dispute. The Code Member must establish its data protection role and responsibilities to comply with the requirements of Data Protection Law. The Code Member may process this data for the purpose of fulfilling the Client's instructions. It may, however, not use all the potential witnesses for the Client's instructions and it may contact these witnesses for related enquiries to see if they are interested in the Code Member's services. In considering its role, the Code Member should consider the fact that it would be determining the purposes of the new processing, in this case; business development. In this example, the Code Member is acting as a Controller and must comply with the Controller obligations under Data Protection Law.

2. A Client company requires the Code Member to investigate an investment to establish whether they have been defrauded. The Client has left it up to the Code Member to proceed with the Investigation as the Code Member sees fit. As the Investigation continues, the Code Member needs to process Personal Data of individuals involved in the investment. The Code Member does not use the Personal Data for any other purpose, and it discusses the requirement to process Personal Data for the purpose of the instructions with the Client. The Code Member decides whose Personal Data is collected, what data is collected, who it will be shared with and therefore the key means of processing. However, it is likely that the purpose of the processing is still to fulfil the Client's instructions. Given there is discussion between the Code Member and

its Client about the processing of Personal Data, it is possible that the Code Member is acting as a Joint Controller in this example, however the Code Member is not deciding the purposes of the processing on its own.

3. In a debtor locate case, the Client instructs the Code Member to identify a particular individual and provides a last known address. The Code Member, on speaking to the occupant becomes alert to the likelihood that the debt scenario is not as instructed but 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 Data Subject 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 means and purpose of these processing activities, the Code Member is likely to be acting as Controller, for the processing it is deciding means and purposes of.

16. Processor examples

16.1 If it is to act as a Processor for one or more processing activities, the Code Member must establish that it is not determining the purposes and essential means of those processing activities and is only processing Personal Data on behalf of and as instructed by the Controller.

16.2 A Code Member may be a Processor and still have a certain degree of discretion as to how the processing is accomplished. 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. However, discretion over the essential means by which the Personal Data will be processed indicates that the Code Member will be a Controller, not a Processor. 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 processing agreement it is a party to.

16.3 A Processor must not process Personal Data outside of the instructions from a Controller, as to do so would be likely to breach the requirements of Articles 28 and 29 of the UK GDPR.

16.4 There are certain limited circumstances in which a Code Member can act as a Controller and Processor for its Client. This is normally where it is undertaking different processing activities in relation to the same Personal Data. This is discussed in Part B paragraph 17 below.

Processor examples:

1. A creditor Client instructs the Code Member to distribute several statutory demands. The Client provides addresses and names for the recipients of the statutory demands. The Code Member has instructions to attend the address, verify the identity of the Data Subject who is the debtor, and to serve the statutory demand. The Code Member is not deciding on the means or purposes of the processing of the Personal Data based on these facts. The only Personal Data it is processing is the information provided in the instructions from the Client and only for the purposes of delivering statutory demands. The Code Member and Client will need to ensure they have a written agreement in place between them that fulfils the requirements mentioned in Part B paragraph 13.1 above.

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. As the Code Member is determining neither the means nor the purposes of the processing, it is likely that it will be a Processor for this activity. The Code Member and Client will need to ensure they have a written agreement in place between them that fulfils the requirements mentioned in Part B paragraph 1.3.1 above.

17. Controller and Processor of the same data

17.1 In some cases, the Code Member could be a Controller and a Processor of the same Personal Data that it is processing in order to provide services to its Client. The Code Member may be a Controller for some processing activities and a Processor for other processing activities, if for certain activities it is determining the purposes and means of processing and for other activities its Client is making such determination.

17.2 For example, the Code Member may be processing in the manner described in the examples above but also retains that Personal Data in advance of annual quality assessment of its handling of instructions. For the retention of the data for its quality assessment purpose, the Code Member would be acting as a Controller.

Controller and Processor example:

1. The Code Member accepts instructions from a Client to locate the whereabouts of a debtor. The Code Member exercises its discretion as to the search scope it will use and the extent of the searching and is thus likely acting as a Controller. Before the task is complete the Client transfers the debt to a debt collection agency, which takes over the instructions and so becomes

a Controller. The debt collection agency writes to the Code Member and instructs the Code Member to undertake specific trace activities on specific systems for specific Personal Data. The debt collection agency determines how and why the Personal Data is being processed in light of the changed instructions. It is likely that the Code Member will become a Processor for the processing activities involved in fulfilling the new instructions. The debt collection agency Client and the Code Member should enter into the required terms between a Controller and Processor.

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

18. Joint Controller

18.1 A Code Member and its Client will be Joint Controllers where they jointly determine the purpose and the means of processing (as referred to in Part B paragraph 14.1 above). This would normally be the case where the Client and the Code Member work together to decide what Personal Data will need to be involved, what it will be used for and how it will be processed.

18.2 Where Code Members are Joint Controllers with their Clients, they should have clear discussions with instructing Clients as to the roles and responsibilities of each party. This should include who will carry out which Controller obligation, including how they will comply with individuals' rights, Data Subject access requests and transparency obligations. This may be set out in the engagement letter between the Client and the Code Member. The examples below explore Joint Controllership in more detail.

Joint Controller example:

1. A law firm acting for a road traffic accident victim Client requests the Code Member to interview the lay Client to extract full details of the accident and parties involved, undertake initial investigative assessment and report on recommended way forward on potential compensation claim. The Code Member discusses the means and purposes for that processing in consultation with the law firm on behalf of their mutual Client and concerning common Data Subjects. The Code Member is therefore not independently deciding what information to obtain, how to obtain it and what to use it for, but does so jointly with the law firm.

19. Data Protection Impact Assessments

19.1 Code Services frequently involve the processing of Personal Data in high-risk circumstances, not least the potential consequences of harm that could be introduced by the Code Member's Activities

and findings. This risk increases with certain investigative methods such as surveillance, which is potentially intrusive.

19.2 A DPIA is essentially a risk assessment. It is a data protection "early warning system", which helps the Code Member identify and, with the appropriate action, prevent potential problems before they occur. Given the risks of harm present in Code Members' work, a DPIA must be conducted prior to any Code Services processing (but not always for General Business Administration).

19.3 A DPIA may cover a single processing operation or a group of similar processing operations and they are an important tool in identifying and mitigating risk, and ensuring compliance with Data Protection Law.

19.4 It is important that where a high risk of harm is identified by the Code Member and the risk cannot be mitigated that the Code Member consults the ICO prior to any processing.

20. When is a DPIA required?

20.1 A DPIA is required for any processing likely to result in a high risk to the rights and freedoms of natural persons under Data Protection Law.

20.2 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 for the Code Services, it will have a duty to assist the Controller with its own DPIA, but not to undertake one itself.

20.3 Code Member Activities are likely to involve several types of processing that carry risk and warrant a DPIA (e.g. refusal, data matching, invisible processing, tracking, risk of physical harm), and may also be considered particularly intrusive. Refusal may occur, for example, following a Code Member's adverse findings in conducting due diligence background checks on an individual in relation to an employment. Another example is where the Code Member's lawful basis is legitimate interest, particularly in contentious scenarios, and the Code Member is performing "invisible processing", in other words not providing information to the Data Subject about their rights.

20.4 A DPIA will be required in any event where the Code Member will process Special Category Data for investigative or Litigation Support Services, or where children's data is involved. Processing Criminal Offence Data on a large scale, which is often a request in due diligence background Investigations, will also require a DPIA.

20.5 A DPIA will consider the level of risk. To assess whether something is "high risk", Data Protection Law is clear that the Code Member needs to consider both the likelihood and severity of any potential harm to individuals. "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 should consider the likelihood of harm occurring are:

20.5.1 refusal – for example, due diligence services that could result in the Data Subject being declined employment or other benefit;

20.5.2 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;

20.5.3 invisible processing – where the Code Member re-uses publicly available Personal Data, for example where information has been collected about an individual from another source without providing any privacy information. This could mean that an individual is prevented from exercising their rights;

20.5.4 tracking – for example any form of surveillance used as part of the Code Member's methodology; and

20.5.5 physical harm – for example where the Code Member's processing of Personal Data may put the Data Subject at risk of harm, such as in a whistle-blower scenario.

20.6 Beyond the specific factors at Part B paragraph 20.5.1 to 20.5.5 above, a Code Member will need to consider the risk of the processing in line with the guidance in Part B paragraph 20.3 and 20.4 as to whether the processing warrants a DPIA. A DPIA will not be required where the processing is not likely to present a high risk to the rights and freedoms of Data Subjects.

20.7 Code Members should consider whether a single DPIA could be used for a number of different parts of a Client's instructions. This will vary depending on the Code Member's role as a Controller or Processor of the Personal Data. For example, when investigating a claim with a particular relevance to Special Category Data and multiple Data Subjects, a single DPIA covering all the processing may be sufficient, provided that the processing, and the potential harm, is the same for each Data Subject.

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

21.1 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.

21.2 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, a Code Member must (as in the template DPIA contained in Appendix IV):

21.2.1 identify the need for the DPIA explaining the project relevant to the processing;

21.2.2 describe the nature, scope, context, and purposes of the processing;

21.2.3 consider a consultation process with relevant stakeholders about the processing;

21.2.4 assess the necessity and proportionality of the processing and explain the lawful basis for the processing;

21.2.5 identify and assess the risks of harm to individuals;

21.2.6 identify any measures to mitigate those risks;

21.2.7 consider whether there is still a high risk and, if so, consult the ICO before proceeding with the processing;

21.2.8 sign off and record outcomes; and

21.2.9 keep under review and reassess if anything changes.

21.3 Code Members' instructions 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 persons they are instructed to investigate, or the risk of harm the processing may cause. It is important that the Code Member is independent when considering the harm that may be caused by its potential processing. A DPIA will greatly assist the Code Member to assess the risks in an open and fair manner.

22. **Importance of the DPIA**

22.1 Conducting a DPIA does not have to be complex or time consuming, but it must be carried out rigorously, in proportion to the data protection risks that may arise from the processing.

22.2 Completing a DPIA also helps the Controller completing it to ensure its compliance with the principles of Data Protection Law. DPIAs may flush out and help to rectify the following common issues with Personal Data processed for investigative or litigation support purposes:

22.2.1 it 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;

22.2.2 it is kept for too long - Code Members have a tendency to hoard case files and the Personal Data that is contained within them, on a "just in case" basis;

22.2.3 it is used in ways that are unacceptable to or outside of the reasonable expectations of the Data Subjects;

22.2.4 Data Subjects' rights are not respected - for example, with insufficient access to or transparency over the processing;

22.2.5 it is inaccurate, insufficient, or out of date;

22.2.6 it is disclosed to recipients explicitly contrary to the Data Subject's wishes; or

22.2.7 it is not kept securely.

23. What happens after completing a DPIA

23.1 After completing a DPIA, the outcomes should be incorporated into how the processing is undertaken. For example, any risk mitigations identified in the DPIA should be put in place prior to the processing.

23.2 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 should redact any commercially sensitive information if they do publish a DPIA.

23.3 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 should send a copy of the DPIA to the ICO and can expect a response within ten working days, with the ICO's written advice following in due course.

23.4 If it is consulted on a DPIA, the ICO may decide that the risks have been sufficiently mitigated and the processing can continue, with its written advice giving further suggestions for risk mitigations. The ICO may issue a warning, setting out the steps that must be taken to avoid breaching Data Protection Law. In circumstances where the ICO has significant concerns, it may impose a limitation or ban on the processing. Although the ICO's decision may be appealed, a Code Member should reflect carefully upon the ICO's written advice and any ban it imposes.

24. Lawful basis

24.1 Please note that this section of the Code deals with aspects of Data Protection Law that the Code Member will not have to consider to the extent that it is acting as a Processor. To establish whether a Code Member is acting as a Processor or Controller, it should refer to Part B paragraph 9 above.

24.2 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 must be 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 categories of Personal Data it must identify a condition under Article 9(2) of the UK GDPR. If the Code Member is processing Personal Data relating to criminal convictions and offences or related security measures 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.

24.3 The Code Member must pay special attention to the need to protect children's interests. Any potential harm to children may mean that Personal Data cannot be collected or used at all.

24.4 Code Members must not, to the extent possible, switch their 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.

LAWFUL BASIS ARTICLE 6 OF THE UK GDPR	
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 Data Subjects. Legitimate interest tends to be commonly relied on by Code Members and is dealt with in greater detail below.
CONSENT	Personal data may be processed on the basis that the Data Subject has consented to the processing. Consent[12] must be freely given, specific, informed, and unambiguous. It is important to make it known to the Data Subject that the consent may be withdrawn at any time and how that can be done. 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 should 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 should not be a pre-ticked box or any other method of default consent. It should 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. The process of obtaining the consent must make it easy for people to withdraw consent. 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 within the parameters of providing investigative and support services. However, it may be a lawful basis in relation to the Client's Personal Data or it may be relevant to new processing and

[12] Consent is defined in UK GDPR Article 4(11) as:

"*Any freely given, specific, informed and unambiguous indication of the Data Subject'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*".

	Personal Data not within the original purpose. For example, if the Code Member needs to process new Personal Data on locating the Data Subject (for example, information given by the Data Subject about the matter), then the Code Member will need to consider whether in all of the circumstances consent should 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 Data Subject is party. The processing must be more than just useful, it must be truly necessary in order for the contract to be performed. This lawful basis is unlikely to be available to a Code Member within the parameters of investigative and Litigation Support Services. However, it may be a lawful basis in relation to a contract between the Code Member and their Client, an activity which is outside 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. Contractual obligations are not included in the relevant legal obligations. The Code Member should 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 does not mean that there must be an obligation specifically requiring 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) does not qualify as a legal obligation for the purpose of this lawful basis. The legal obligation lawful basis could often arise in Code Member activities when there is a requirement to report suspicious activity under the Proceeds of Crime Act 2002 or when compelled by an order of the court under any circumstances. It would be unlikely that this lawful basis could be relied upon at the outset of an instruction. It would instead be most likely to arise during the course of the engagement, as and when the 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 Data Subject or of another natural person. This essentially applies in "life-or-death" scenarios. It is not a lawful basis that is likely to arise often, if at all, in investigative or Litigation Support Services.
PUBLIC TASK	Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest, or in the exercise of official authority vested in the Controller. It is not a lawful basis that is likely to arise often, if at all, in investigative or Litigation Support Services.

LAWFUL BASIS – ADDITIONAL IMPORTANT CONSIDERATIONS	
DATA RELATING TO CRIMINAL OFFENCES ARTICLE 10 OF THE UK GDPR .	Additional conditions apply to the processing of Personal Data relating to criminal offences, because of the potentially significant impact that the processing of such data can have upon the Data Subject. The additional conditions (there are, at the time of the first edition of the Code, 28) are set out in Schedule 1 of the Data Protection Act 2018. However, Criminal Offence Data is treated differently to other Special Categories of Data, on the basis that there is a public interest from society to protect the public from criminal activity. This is supported by the ICO in its guide to the UK GDPR [13]. Information about suspicions of criminal activity or Investigations into potential criminal offences should be treated in the same way as Personal Data relating to actual criminal offences and convictions. The processing of Criminal Offence Data must be necessary for the purpose that the Code Member has identified and they 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, a Controller must have an APD in place relating to its processing of such data. The Code Member should 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[14] **Explanation:** The processing of Criminal Offence Data is governed by a complex legislative framework and may only be processed: • under the control of an official authority, or • as permitted under Data Protection Law. A Code Member must have: o a valid lawful basis under Article 6 of the UK GDPR; o an additional condition for processing this type of data, under schedule 1 of the Data Protection Act 2018. Examples of the available conditions are to assess people's suitability for employment, or preventing or detecting unlawful acts, preventing fraud, legal claims and insurance; and o An APD in place. • The Code Member must also ensure that the other requirements of Data Protection Law are complied with in its processing of Criminal Offence Data; for example that it does so in a manner that is fair, transparent, necessary, proportionate and generally lawful (not just under Data Protection Law).

What is Criminal Offence Data? | ICO

[14] appropriate-policy-document.docx (live.com)

	• A Code Member may encounter requests to process Criminal Offence Data in contracts. To do this, a Code Member will need an additional legal basis such as the Data Subject's explicit consent. The data may be provided by the Data Subject in a disclosure certificate from the Disclosure and Barring Service, for example. • 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 they 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 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 data of 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 insured party. Depending on the circumstances, that may be the legitimate interest basis. However, for insured parties and third parties, the Code Member will also need to meet one of the permissive conditions to process the Criminal Offence Data. In this example, possible relevant conditions in Schedule 1 of the DPA may include: paragraph 10 (preventing or detecting unlawful acts), paragraph 14 (preventing fraud), paragraph 33 (legal claims - if litigation is ongoing or contemplated), or paragraph 37 (insurance).
PROCESSING SPECIAL CATEGORY (SENSITIVE) PERSONAL DATA ARTICLE 9 OF THE UK GDPR	"Special categories of Personal 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 The processing of Special Category Data will require one of ten separate conditions to be met and may 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 referred to above in relation to Criminal Offence Data will be relevant for the

Special Categories of Data too [15].

In addition to the UK GDPR Article 6 lawful basis, the processing of Special Categories of Data requires one of the ten conditions under Article 9 of the UK GDPR to be fulfilled. Five of the ten Article 9 conditions also require the Code Member to meet additional requirements under Schedule 1 to the DPA. The explanation box below summarises these conditions and requirements.

The conditions should normally be determined and the processing examined in a DPIA prior to processing commencing, to assess and mitigate the risk. This is because processing Special Categories of Data is likely to pose a higher risk to Data Subjects. For further information about DPIAs, please refer to Part B paragraph 19 to 23 of the Code above.

For any processing of Special Categories of Data, the processing must be necessary for the purpose the Code Member has identified and they must be satisfied that there is no other reasonable and less intrusive way to achieve this purpose.

Explanation: the processing of Special Category Personal Data is prohibited, unless:

- The Data Subject has given explicit consent.
- The processing is necessary in the context of employment law, or laws relating to social security and social protection. See also schedule 1 part 1 of Data Protection Act 2018 for employment, health or social care, public health, research.
  - this condition will also require the Code Member to meet one of the conditions set out in Part 1 of Schedule 1 of the DPA 2018. Of most relevance to the Code Members may be: (10) preventing or detecting unlawful acts; (11) protecting the public against dishonesty; (14) preventing fraud; (15) suspicion of terrorist financing or money laundering; (20) insurance.
- The processing is necessary to protect vital interests of the Data Subject (or another person). Here the Data Subject 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.
- The processing relates to Personal Data that have been manifestly made public by the Data Subject.
- The processing is necessary for the establishment, exercise, or defence of legal

[15] Available at https://ico.org.uk/media/for-organisations/documents/2616286/appropriate-policy-document.docx

claims, or for courts acting in their judicial capacity [16].

- The processing is necessary for reasons of substantial public interest, occurs based on a law that is, inter alia, proportionate to the aim pursued, protects the rights of Data Subjects and meets one of the specific conditions set out in schedule 1 part 2 of the Data Protection Act 2018.
  - this condition will also require the Code Member to meet one of 23 specific public interest conditions as set out in Part 2 of Schedule 1 of the Data Protection Act 2018, of which the following may be most relevant to a Code Member: (1) preventing or detecting unlawful acts, (14) preventing fraud, and (20) insurance.

- 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 one of the conditions set out in Part 1 of Schedule 1 of the DPA 2018. Of most relevance to the Code Members may be: (10) preventing or detecting unlawful acts; (11) protecting the public against dishonesty; (14) preventing fraud; (15) suspicion of terrorist financing or money laundering; (20) insurance.

- 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 one of the conditions set out in Part 1 of Schedule 1 of the DPA 2018. Of most relevance to the Code Members may be: (10) preventing or detecting unlawful acts; (11) protecting the public against dishonesty; (14) preventing fraud; (15) suspicion of terrorist financing or money laundering; (20) insurance.

- 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 one of the conditions set out in Part 1 of Schedule 1 of the DPA 2018. Of most relevance to the Code Members may be: (10) preventing or detecting unlawful acts; (11) protecting the public against dishonesty; (14) preventing fraud; (15) suspicion of terrorist financing or money laundering; (20) insurance.

Special category processing example:
The Code Member's Client is being sued by one of its employees following an accident at work. The employer wants to pass the details of the accident to the Code Member to investigate the accident, ahead of instructing solicitors to obtain legal advice on its position and potentially to defend the claim. The

[16] 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.

		Client wants to provide some Personal Data about the individual's injuries, which constitute health data. For the purposes of Data Protection Law this would constitute Special Category processing. In the event that the Code Member is a Controller, in order to process the Personal Data provided by the Client to carry out the instructions, the Code Member, in addition to its other obligations, would need an Article 6 lawful basis as well as an additional Article 9 condition for processing. The Code Member might rely on the Article 9(2)(f) condition that the processing is necessary for the establishment, exercise or defence of legal claims. The processing would only be lawful, on that basis, to the extent necessary to defend the claim. The Code Member must work within those limits to perform the data processing for defence of the claim.
PROCESSING FOR NEW PURPOSES	Save in exceptional circumstances, as explained under the purpose limitation principle of Data Protection Law[17] 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 be unexpected, 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 are 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 factors: • Any clear link between the original purpose and the new purpose. • The context in which the data have been collected, including the Code Member or Client's relationship with the Data Subjects, considering in particular what the Data Subjects would reasonably expect. • The nature of the Personal Data and whether criminal and/or Special Category Personal Data is involved. • The possible consequences of the new purpose of processing for Data Subjects. • The existence of appropriate safeguards (e.g., encryption or pseudonymisation).

25. Legitimate interest:

25.1 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. In this section the Code will explain how the legitimate interest lawful basis works in a private

[17] See Appendix II below for more information on these principles.

investigations context and what a Code Member can do to demonstrate that it has considered its relevant responsibilities under Data Protection Law.

25.2 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. In addition, the Code Member should be aware that for Special Category or Criminal Offence Data, there are a range of additional requirements in respect of the processing, as explained in the explanatory box of Part B paragraph 25 above.

25.3 Reliance on the legitimate interests basis comes with significant responsibility for the Code Member, as it involves balancing the rights and freedoms of the Data Subject against the interests being pursued. The relevant data processing may change as the instructions develop, so the Code Member should ensure regular review as necessary to ensure that its reliance on the legitimate interests basis is appropriate.

25.4 There are three elements for the Code Member to consider when it is relying on the legitimate interest lawful basis. It helps to think of this as a three-part test and this section provides further detail on how that test should be approached.

LEGITIMATE INTEREST **3-PART TEST** 1. IDENTIFY A LEGITIMATE INTEREST 2. SHOW THAT THE PROCESSING IS NECESSARY TO ACHIEVE IT 3. BALANCE IT AGAINST THE DATA SUBJECT'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. The UK GDPR makes it clear that fraud prevention and network/information security can be legitimate interests. Similarly, disclosures to give warning of criminal acts or public security may be based on legitimate interest (although they may be overridden by a binding obligation of secrecy).

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 interest pursued by the Code Member (or that of 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 Data Subject? • Is any of the data particularly sensitive or private? • 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**: When should the Code Member avoid choosing legitimate interests? 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. For example, the Code Member may wish to avoid relying on the legitimate interests basis if: • The Client is a public authority and the processing is for the performance of tasks as a public authority. • 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's 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. 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.

25.5 Following application of 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 Data Subject (part 3 of the test). The ICO has produced an interactive guidance tool which can be used to consider the appropriate lawful basis for processing, including legitimate interests[18].

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

25.7 The Code Member should keep a record of the LIA and, whilst there is no standard format for this, the Code Member may wish to adopt the ICO template[19].

25.8 Code Members should consider carrying out an LIA for each case for which it relies on legitimate interests as a lawful basis. This would demonstrate the thought process used in reaching a decision and to justify the outcome on the specific facts of the case. As a case develops, the LIA may need to be reviewed and refreshed, at least as necessary when there is a significant change in the purpose, nature, or context of the processing.

25.9 If, after weighing all the factors, the processing will cause undue interference with the interests, rights, or freedoms of the affected Data Subjects, the Code Member should not rely on the legitimate interest lawful basis without there being a compelling reason, which it should document.

25.10 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

[18] Available at: https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/

[19] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

interests or the interests of third parties, 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 compelling may be overridden in the balancing test. The Code Member must think about specifically what interests they are furthering with the particular processing operation.

Example:

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 its LIA, the Code Member documents that it considers it has a legitimate interest in processing the Personal Data of the fraudster to establish the veracity of the allegations. The Code Member considers that the processing is necessary in order to achieve that purpose and documents this, together with how there are no less intrusive methods of reasonably achieving the same result. The Code Member should also consider proportionality and the risk of excessive processing. Finally, the Code Member weighs the rights and freedoms of the affected Data Subject 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 Code Member considers that it would be, on the basis that a fraudster would reasonably expect a victim to try and prevent the fraud or identify the culprit. 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 Data Subject 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 should ensure that the LIA is conducted thoroughly and the documentation retained for review in the future.

26. **Safeguards (Consent to share)**

26.1 Code Members may find, as explained in the explanatory box of Part B paragraph 25 above, 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 should be aware that safeguards cannot always tip the scales and justify the processing.

26.2 A worked example of this is in relation to trace and locate instructions, which are relevant to the legitimate interests lawful basis. In some cases, a Code Member may have been 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 Data Subject for the purpose of carrying out their executor duties. The Code Member has the name and last known address of the Data Subject provided by the Client but it will be exercising its discretion and using its own leads to track down the Data Subject.

Pre-trace processing

26.3 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 means and purpose of the processing, it is likely that it will be a Controller and so must establish a lawful basis for processing the Personal Data. Legitimate interests is likely to be the most appropriate lawful basis for the processing activities of tracing the individual and contacting them on the Client's behalf. The Code Member completes an LIA to verify and demonstrate that the legitimate interests lawful basis does apply in the particular circumstances of that processing.

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

Post-trace processing

26.5 Following identification of the Data Subject, the Code Member must assess again the appropriate basis for processing the new Personal Data which is the contact information for the identified Data Subject in accordance with the Clients instructions (the "**post-trace**" processing). The Code Member may consider consent or legitimate interests to be the most appropriate legal basis, but both have their challenges. If the Code Member relies on the consent of the Data Subject, if consent is not achieved then the Code Member must not process the Personal Data by sharing it with the Client. If the legitimate interests basis is relied upon, then the Code Member must consider whether it has given due regard to safeguarding the rights and freedoms of the Data

Subject. This is not a straightforward situation and consideration should be given on a case-by-case basis.

26.6 If the outcome of the LIA for the post-trace processing assessment is that the rights and freedoms of the individual outweigh the interests of the Client, then no further processing of the Data Subject's Personal Data may continue and no Personal Data may be shared with the Client. The Code Member may need to delete the Personal Data, unless they had a valid alternative basis on which to keep it. The Client would need to be made aware that the Code Member would have no obligation to share their findings with the Client, if doing so was not permissible under Data Protection Law.

26.7 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 should be considered. In the example 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 consent is the appropriate lawful basis to rely upon, but it should be considered on a case-by-case basis.

Example communication seeking Data Subject's consent:

Dear sir or madam,
We have been instructed by our 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: ...
Should you agree to our sharing your details with our Client please reply by signing the below "I consent to the above".
Yours truly,
Code Member
I consent to the sharing of my data as above.
Signed .....Data subject

26.8 Some typical example case scenarios showing when legitimate interests lawful bases may or may not be applied with safeguards, 'consent to share', are provided in Appendix III below.

PART C – CODE OF CONDUCT MANAGEMENT & INFRINGEMENTS

27. Management

27.1 The Criteria form the basis of the assessment by the MB on any application for Code Member status and during subsequent annual desktop assessments.

27.2 The Code Member is accountable for compliance with the Code and other regulatory requirements that apply (including wider Data Protection Law) and must always be prepared to justify their decisions and actions.

27.3 A failure in meeting the standards within the Code or a breach 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.

27.4 The ABI provides dedicated training workshops covering the issues as set out in the Code and other areas to assist Code Members in meeting their Data Protection Law obligations, specifically under the Criteria in Appendix V.

28. MB:

28.1 As at publication of the first edition of the Code, the SSAIB has agreed to undertake the role required of a MB for the Code, subject to its accreditation by the ICO. SSAIB is a certification body accredited by UKAS (UK Accreditation Service[20]), with expertise in auditing against the recommendations of BS102000 code of practice for investigative services. It is a company limited by guarantee, operating on a not-for-profit basis.

28.2 The role of the MB is two-fold. Firstly, 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.

28.3 In gaining accreditation by the ICO the MB has demonstrated an ability to meet specific requirements:

28.3.1 independence in relation to four main areas: (i) legal and decision-making procedures, (ii) financial, (iii) organisational and accountability, (iv) structured and managed to safeguard independence and impartiality;

[20] For further information, please consult https://www.ukas.com/wp-content/uploads/schedule_uploads/00011/04947/0131Management Systems.pdf

28.3.2 established rules and procedures that enable it to perform its monitoring tasks without influence from Code Members or the ABI;

28.3.3 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;

28.3.4 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; and

28.3.5 a documented process to receive, evaluate and make decisions on complaints made about its monitoring responsibilities and activities, including any appeals.

28.4 As a result, the MB shall not provide any services to Code Members that would adversely affect its independence and any decisions made by the MB related to its functions shall not be subject to approval by any other organisation, including the ABI.

29. Monitoring arrangements

29.1 Compliance with the Code will be assessed by the MB, on application to Code Member status and thereafter on an annual basis. The assessment shall be conducted as a remote desktop exercise and require the Code Member to successfully demonstrate competence by providing evidence of compliance with the Criteria at Appendix V. This shall include: the lawful basis for the processing of Personal Data under Article 6 of the UK GDPR; completing and/or reviewing the Code Member's DPIA for the type of processing they undertake; and reviewing the documented LIA showing the application of the legitimate interests test. These Criteria and other supporting evidence are set out in more detail in Appendix V below.

29.2 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 shall be made publicly available in line with its complaints handling procedure.

29.3 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 shall 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 shall 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.

29.4 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.

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

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

29.6.1 IRCA certification as a QMS ISO 9001 lead auditor;

29.6.2 confirmed competency to undertake product conformity audits in relation to BS102000:2018;

29.6.3 attendance at the ABI-provided UK GDPR training workshop; and

29.6.4 successful completion of relevant and accredited CPD training.

29.7 Any changes to Code monitoring arrangements shall only be implemented in consultation with the ICO. If the Commissioner revokes the accreditation of the MB, the Code Owner shall identify a replacement MB at the earliest possible opportunity. The replacement MB shall 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 Commissioner's requirements. Failure to apply within this period will result in the withdrawal of Code approval by the Commissioner and existing Code Membership will become void. The Code Owner will not accept any new applications for Code Membership until a new MB is accredited.

30. Complaints

30.1 The MB will be responsible for the recording, acknowledgement, and investigation of complaints over infringements of the Code by Code Members. A copy of the MB's complaints and appeals procedure shall be published on its website and include guidance in relation to qualifying complaints.

30.2 Details of the complaint shall be confirmed by the Data Subject in writing, using a complaints 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 their receipt of the completed form along with any questions the MB requires a response to. Relevant aspects of the complaint may be provided to the Code Member 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.

30.3 Code Members will be required to provide the MB with a written response to the complaint within 30 working days of receiving their copy of the complaint. That response shall include an outline of

the lawful basis for the processing of the Personal Data subject to the complaint and a copy of the related DPIA, together with any other documentation deemed necessary by the MB.

30.4 The MB will consider any action necessary in line with Part C paragraph 31 below and notify the Code Member accordingly. The complainant will be informed by the MB of their findings and any action taken within ten working days of the Code Member being notified. The complainant shall have a right of appeal against the findings of the MB and any action taken by them. This does not affect any right of the complainant to refer a complaint to the ICO as the complainant sees fit.

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

31. Infringements

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

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

31.3 In considering the issuing of corrective advice or sanctions the MB shall take account of the causation factors and whether these comprised human error, a failure of process or deliberate act. It shall 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 34 below for illustrative purposes.

31.4 Suspension or exclusion of Code Members will only apply in the most serious of circumstances. Normally, Code Members shall first have the opportunity to take suitable corrective measures where appropriate, as agreed with the MB. The Code Member shall 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 officer having been sent to the Code Member, setting out clearly the basis for the appeal.

31.5 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[21].

31.6 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.

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

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

[21] https://www.theabi.org.uk/code-register

32. Infringement matrix

Example infringement	Example MB action
Failure to record or accurately complete a DPIA when required, Failure to apply or accurately complete the legitimate interest assessment. Processing Personal Data where no lawful basis has been recorded.	In isolated incidents, infringements such as these could merit corrective advice and possible requirement for further training on the relevant infringement area. In repeat scenarios, egregious breaches of these or breaches in respect of Special Category Personal Data, more severe action may be appropriate.
Failure to address a Non-conformance report within the stipulated period. 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.	In isolated incidents, a written warning could be appropriate for these example infringements. Repeated infringement, an egregious breach or a combination of different infringements, or breaches in respect of Special Category Personal Data may lead to more severe action being appropriate.
Failure to respond to a Non-conformance report within the stipulated period. Failure to record or accurately complete a DPIA after retraining. Failure to apply or accurately complete the LIA after retraining.	In these situations, the Code Member will have already been given the opportunity to correct its processing activities in advance of this infringement. It may be that suspension escalating to expulsion is the appropriate action by the MB in such circumstances.
Processing Personal Data where no lawful basis could exist. Processing Personal Data where the LIA indicated insufficient or no legitimate basis.	In these situations, it may be appropriate for the MB to expel the Code Member and refer the Code Member under 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.

33. Consultation

33.1 First Consultation:

33.1.1 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.

33.1.2 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.

33.1.3 As at 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.

33.1.4 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 investigation and litigation support services sector by circulating notice to the known representative bodies and network groups.

33.1.5 On 01 August 2020 notice of the consultation inviting input was also sent to representatives from various stakeholders, Data Subjects, and law enforcement.

33.1.6 The first consultation closed on 14 August 2020. The relevant feedback was shared with the ICO.

33.2 Second Consultation:

33.2.1 On * 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, data subjects, law enforcement and the media.

33.2.2 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.

33.2.3 The second consultation closed on 16 September 2022. The relevant feedback was shared with the ICO.

34. Review:

34.1 The MB will review the Code on an annual basis in consultation with the Code Owner (the "**Code Review**"). A formal Code Review Framework has been agreed between the MB and the ABI, 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 Code Owner. Any amendments or extensions to the Code may be made by the Code Owner, but only following approval by the ICO.

34.2 The Code Owner will submit an annual report to the ICO following the annual review, which shall be endorsed by the MB shall include:

34.2.1 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 intended to ensure that the Code remains relevant to members, continues to meet application of Data Protection Law, and adapts to any changes in legislation;

34.2.2 progress with the Code, such as how many Code Members and any issues encountered; and

34.2.3 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- Activities

These are the non-exhaustive activities frequently undertaken in the provision of Investigations and Litigation Support Services by private investigators.

Activity	Sub-activity	Description	Examples of Personal Data processed
Accident Investigation	Road traffic	Producing accident and Locus reports, site visits, photograph and DVD logs, sketches, witness statements to gauge whether injuries are genuine, witness tracing.	Reports and notes, photographs, Special Category Data including medical records.
	Trip and slip	Assessment of slip resistance, site visits, photographs, assessment of accident, witness statements, logbooks.	Reports and notes, photographs, Special Category Data including medical data.
	Workplace	Discreet surveillance, background investigations, evidence collection e.g. interviewing work colleagues.	Reports and notes, photographs and interview notes.
Blackmail	Disclosure	Tracing of blackmail instigators, due diligence on instigators, paper trail tracking.	Reports and notes, photographs and interview notes.
	Product contamination	Product testing, site visits at manufacture premises, photographs.	-
Due Diligence	Employment recruitment	Screening applicants, gathering, analysing and reporting pertinent information in a highly confidential and discreet way to assist employer with decisions.	Reports and notes including potentially Special Category (racial/ethnic origin, medical records).
	Investments	Gathering financial information about potential company and business partners, details of accounts, asset tracing.	Reports and notes, identity details and data including potentially Special Category (racial/ethnic origin, medical records).
Employment Investigations	Absenteeism	Evidence collection (photographic/video) using technology and investigative methods, interviewing work colleagues and producing a report.	Reports, photographic and video evidence and notes including potentially Special Category (medical records).
	Disciplinary	Evidence collection (photographic/video) using	Reports, photographic and video evidence and notes

		technology and investigative methods, interviewing work colleagues and producing a report.	including potentially Special Category (medical records).
	Grievance including harassment, discrimination, and victimization	Evidence collection (photographic/video) using technology and investigative methods, interviewing work colleagues and producing a report.	Reports, photographic and video evidence and notes including potentially Special Category (medical records).
Family	Children	Evidence collection relating to custody e.g. ability to look after a child in a safe environment with adequate care, quality of care the parent delivers and any issues that may arise, such as safeguarding and child protection issues. Includes visits at residential addresses, photographs and videos.	Data relating to a child and child protection. Reports, photographic and video evidence and notes including potentially Special Category (medical records).
	Finances	Gathering financial information about an individual, details of accounts (including off-shore), asset tracing.	Personal data such as contact details, financial information.
	Genealogy or heir hunting	Locating beneficiaries to estate, contact potential beneficiaries, researching lineage.	Personal data such as contact details.
	Infidelity	Carrying out discreet surveillance, recovering deleted messages, GPS tracking, producing final report with photo and video evidence.	Reports, photographic and video evidence and notes. Potentially Special Category (sexual orientation).
Fraud & Theft	Bribery and corruption	Identification and surveillance of perpetrator, inform fraud squad once sufficient evidence gathered.	Personal data such as contact details and residential address.
	Forgery	Identification and surveillance of perpetrator, analysis of forged object/writing, background checks, GPS tracking.	Personal data such as contact details and residential address.
	Fraud by misrepresentation or omission	Identification and surveillance of perpetrator, recovering deleted messages, GPS tracking.	Personal data such as contact details and residential address.

General Investigations	Civil	Evidence gathering in anticipation of civil trial, checking financial documents, witness statements and other evidence collection depending on the nature of the trial.	Personal data depending on the nature of the potential civil case, and therefore may include Special Category.
	Criminal	Evidence gathering in anticipation of a criminal trial, witness statements, site visits, GPS tracking and other evidence collection depending on the nature of the trial.	Personal data depending on the nature of the potential civil case, and therefore may include Special Category.
Intellectual Property	Copyright and trademark infringements	Mystery shopping where investigator purchases goods as evidence of retail locations, site visits to storage and distribution points.	-
	Product counterfeiting	Mystery shopping, locating distribution channels, site visits to distribution points.	-
Litigation Support	Evidence gathering (witnesses)	Placing overt and covert cameras, vehicle tracing systems, physical surveillance, witness identification, witness statements, producing comprehensive report.	Personal data depending on the nature of the potential civil case, and therefore may include Special Category.
	Pre-suit reports	Gauging financial status, employment status, asset tracing prior to bringing legal action. Lifestyle information, criminal record, credit history.	Personal data such as contact details, home address, financial information.
	Process serving (delivery of legal documents)	Delivering legal documents to specified addresses, making contact with subject of legal documents.	Personal data such as contact details and home address.
Loss Investigations	Insured claims	Verifying soft fraud and hard fraud insurance claims to establish validity, background check on claimant history, evidence collection.	Personal data depending on the nature of the potential case, and therefore may include Special Category Data such as medical records.
	Third party insurance claims	Verifying soft fraud and hard fraud insurance claims to establish validity, background check on claimant history, evidence collection.	Personal data depending on the nature of the potential case, and therefore may include Special Category Data such as medical records.

Tracing	Debtors and their assets	Producing report on worth and value of debtor including details of accounts (including off-shore) and associated companies and using asset tracing software, surveillance Investigations and undercover operations.	Personal data such as contact details and financial information.
	Missing persons	Searching public records, interview family and friends, physical searches of last known address, contacting and arranging a meeting with the missing person.	Contact details, home address and other Personal Data.

Appendix II - Data Protection Principles

DATA PROTECTION PRINCIPLES	
PRINCIPLE	EXPLANATION
LAWFULNESS, FAIRNESS AND TRANSPARENCY	**Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.** • The Code Member must determine the lawful basis under Article 6 of the UK GDPR before starting to process Personal Data. It's important to get this right first time. If the Code Member finds at a later date that the chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to Data Subjects and lead to breaches of accountability and transparency requirements. • A Code Member must not process Personal Data in a way that is unduly detrimental, unexpected, or misleading to the Data Subjects concerned. In many cases the Code Member is likely to rely on legitimate interests in contentious circumstances, i.e. in relation to ongoing or contemplated criminal or civil legal proceedings. The Data Subjects' expectations may not necessarily be obvious but on careful analysis through the LIA and DPIA, it may be reasonable to conclude that the Data Subjects ought to reasonably expect the processing. One possible example is the Code Member's processing of Personal Data following the Client's concerns about fraud or some other harmful and contentious issue. • A Code Member must be clear, open, and honest with people from the start about who they are and how they will use the Personal Data. That is not to say that the Code Member must notify a Data Subject of the processing in every case, as this is something that would probably compromise the Investigation in a contentious matter, the very purpose for the processing[22].
PURPOSE LIMITATION	**Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.** • The Code Member must be clear about what the purposes for processing are from the start. • The purposes need to be recorded as part of the accountability obligations (including through the DPIA). • A Code Member can only use the Personal Data for a new purpose if either this is compatible with the original purpose, the Data Subject gives consent, or there exists a clear obligation or function requiring this set out in law.

[22] See Article 14(5)(b) of the UK GDPR: in some cases, transparency is not required, where it would render impossible or seriously impair the objectives of the processing.

	This requirement aims to ensure that the Code Member is clear and open about the reasons for obtaining Personal Data, and that what the Code Member does with the data is in line with the reasonable expectations of the individuals concerned. Specifying the purposes from the outset helps accountability for the processing and helps avoid Personal Data being used for purposes that are incompatible with, or different to, the purpose for which the data was originally obtained by the Code Member. This is especially important for the Code Member when undertaking invisible processing, as is likely in most of their case scenarios. In any event, the clarity in the reasons also helps individuals understand how the Code Member uses their data, makes decisions about whether they are happy to share their details, and assert their rights over data where appropriate. It is fundamental to building public and Client trust in how the Code Member uses Personal Data. There are clear links with other principles – in particular, the fairness, lawfulness, and transparency principle. Being clear about why a Code Member is processing Personal Data will help to ensure the processing is fair, lawful, and transparent. **Example:** A Client bank instructs the Code Member to investigate the financial status of the Data Subject to assist in assessing their ability to meet a debt due to the bank. The instructions require the bank to share relevant confidential data about the Data Subject that will assist the Code Member in the specific task (purpose). Coincidentally and shortly after the Code Member is instructed by a separate Client in a domestic dispute unrelated to the bank's purpose. The data processed in the bank's case has a specific purpose that would be incompatible to be processed in the domestic case.
DATA MINIMISATION	**Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.** The Code Member will not collect any more information than is necessary and required in order to perform the processing activity. The Code Member will need to carefully consider the extent of information passed to or requested from Clients and subcontractors. What is adequate and relevant will depend on the Code Member's specified purpose for collecting and using the Personal Data. It may also differ from one individual to another. So, to assess whether the Code Member is holding the right amount of Personal Data, they must first be clear about why they need it. For Special Category Data or Criminal Offence Data, it is particularly important to make sure the Code Member collects and retains only the minimum amount of information. This needs to be considered separately for each individual, or for each group of individuals sharing relevant characteristics. The Code Member should periodically review their processing to check that the Personal

	Data held is still relevant and adequate for the purposes and delete anything that is no longer needed. This is closely linked with the storage limitation principle. **Example**: In a debt related trace instruction, the Code Member is engaged to find a particular debtor. The Code Member collects information on several people with a similar name to the debtor. During the enquiry some of these people are discounted. The Code Member should delete most of their Personal Data, keeping only the minimum data needed to form a basic record of a person they have removed from their search. It is appropriate to keep this small amount of information so that these people are not contacted about debts which do not belong to them. If the Code Member needs to process particular information about certain individuals only, they should collect it just for those individuals – the information is likely to be excessive and irrelevant in relation to other people. **Example**: In almost every case scenario the Code Member will during the course of the desk-top research undertake database searches to gather information within the terms of their purpose. Even a basic search on an address will expose Personal Data on unrelated individuals who are otherwise linked for other purposes to the address. The Code Member should not further process the unrelated individuals' data.
ACCURACY	**Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay ('accuracy').** The Code Member should take all reasonable steps to ensure the Personal Data held is not incorrect or misleading as to any matter of fact. They may need to keep the Personal Data updated, although this will depend on what they are using it for. **Example:** The Code Member's record of a trace enquiry that is being retained for a reasonable period (within the principle of storage limitation), it would not be necessary for the Code Member to be continually updating findings and correcting any incorrect name/address. If it is discovered that Personal Data is incorrect or misleading, the Code Member must take reasonable steps to correct or erase it as soon as possible but if a record of the mistake must be kept and it may be in the Data Subject's interest that it is so recorded, then it must be clearly identified as a mistake. An individual has the absolute right to have incorrect Personal Data rectified. In practice, this means the Code Member must: • take reasonable steps to ensure the accuracy of any Personal Data; • ensure that the source and status of Personal Data is clear;

- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to periodically update the information.

The Code Member must always be clear about what they intend the record of the Personal Data to show. What they use it for may affect whether it is accurate or not. For example, just because Personal Data has changed doesn't mean that a historical record is inaccurate – but the Code Member must be clear that it is a historical record.

> **Example**: Having reported on a trace enquiry the Code Member later finds the individual moved house from London to Manchester. The Code Member's record saying that the individual currently lives in London will obviously be inaccurate. However, a record saying that the individual once lived in London remains accurate, even though they no longer live there.

The Code Member must carefully consider any challenges to the accuracy of Personal Data.

An area in which a Code Member will frequently encounter the need to address accuracy is in reports where opinion is expressed. The Code Member may be instructed specifically to gather other people's opinion of an individual to assess their credibility as a witness, for example.

A record of an opinion is not necessarily inaccurate Personal Data just because the individual disagrees with it, or it is later proved to be wrong. Opinions are, by their very nature, subjective and not intended to record matters of fact.

However, to be accurate, the Code Member's record must make clear that it is an opinion, and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, the Code Member should also record this fact to ensure their records are not misleading.

Verification as to the accuracy of facts and Personal Data are of course a core skill requirement for a Code Member. However, it may not always be practical to check the accuracy of Personal Data someone else provides. There is a frequent reliance by a Code Member on the data provided in their desk-top research using database information. To ensure that the records are not inaccurate or misleading the Code Member must:

- accurately record the information provided;
- accurately record the source of the information;
- take reasonable steps in the circumstances to ensure the accuracy of the information.

What is a 'reasonable step' will depend on the circumstances and the nature of the Personal Data and what it will be used for. The more important it is that the Personal Data is accurate, the greater the effort the Code Member should put into ensuring its accuracy. This may mean getting independent confirmation that the data is accurate.

STORAGE LIMITATION	**Personal data shall be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.** Even if the Code Member collects and uses Personal Data fairly and lawfully, they cannot keep it for longer than actually needed. There are close links here with the data minimisation and accuracy principles. It may in some instances be necessary to minimise the data rather than deleting it completely, where for example a record of the Code Member's relationship with the individual needs to be retained for a period after the relationship has ended simply to confirm that the relationship existed. Some minimal data may also be necessary to be retained for accounting or any legal or regulatory requirements. However, the retention must remain justified and kept under review. The UK GDPR does not set specific time limits for different types of data. This is up to the Code Member and will depend on how long the data is needed for the data specified purposes. It must be a proportionate approach, balancing the Code Member's needs with the impact of retention on individuals' privacy and of course the retention must always be fair and lawful. Ensuring that Personal Data is erased or anonymised when no longer needed will reduce the risk that it becomes irrelevant, excessive, inaccurate, or out of date. Apart from helping to comply with the data minimisation and accuracy principles, this also reduces the risk of data being used in error – to the detriment of all concerned. Personal data held for too long is likely to be unnecessary for the relevant purpose and there is therefore unlikely to be a lawful basis for its retention. The Code Member needs to consider the purposes for processing the Personal Data and that they can keep it as long as one of those purposes still applies but not indefinitely "just in case" or if there is only a small possibility that the data will be needed to meet one of those purposes. From a more practical perspective, it is inefficient to hold more Personal Data than needed, and there may be unnecessary costs associated with storage and security. It is good practice for the Code Member to limit the storage of data as much as possible and to keep a retention schedule as part of their case management. In practice the retention period may also be a term of the engagement agreement with the Client providing it is not an excessive and unnecessary period. Rarely will a Code Member be required to retain Personal Data for anything beyond a period of 2-years after the engagement has come to an end. The relevant and necessary data will have been recorded in a report submitted to the Client to retain, within the Client's own UK GDPR obligations. What shorter period could be applied will vary but could in some simple and short engagements be a matter of weeks or possibly months but unlikely to be beyond the 2-years, save in exceptional circumstances. Should the Code Member wish to retain a document for future use as a template, such as a detailed proposal or a report, then they must anonymise the contents, that is by removing all Personal Data.

Of significant importance also is the Code Member's obligation to a Data Subject, be it a subject access request for any Personal Data held, queries about retention periods and erasure. Such requests may be more difficult if the Code Member is holding old data for longer than needed.

In any event, the Code Member should review the necessity for the retention of Personal Data particularly in completed case instructions. This could be a reasonable period after the completion of the service, to allow for any dispute that may arise, to be resolved. In some instances the Code Member will be required to delete data immediately.

Example: In the Safeguards (Consent) type cases dealt with above, where the Data Subject does not provide consent, the Code Member must immediately delete all Personal Data without sharing the data with the Client or otherwise.

Example: Practitioners in the Investigation sector are habitual hoarders of data being under the misconception that the data could be used in a separate case, in breach of purpose limitation or under the misguided belief they owe a duty to their Client to retain data indefinitely and/or for six years in line with the subject matter of the Investigation usual statutory limitation period (in most contentious cases). Whilst a Code Member may find justification in using the statute of limitation as a reason to retain data for up to six years, it would then be incumbent on them to periodically update the status of the case to ensure the retention necessity has not expired early by reason of a settlement, dissolution of a company party or judicial decision. However, a simple term in the engagement contract between the Code Member and the Client specifying a reasonable maximum period would place the onus on the Client to review the necessity for extending the otherwise relatively short retention period.

Example: A Code Member processes Personal Data about a debtor so that it can find that individual on behalf of a creditor Client. Once it has found the individual and reported to the Client, there may be no need to retain the information about the debtor – the Code Member should remove it from their systems unless there are good reasons for keeping it. Such reasons could include if the Code Member has also been asked to provide litigation support during the debt recovery, for example to personally serve legal process, or other related instructions from the same Client.

INTEGRITY & CONFIDENTIALITY (SECURITY)	**Personal data shall be processed in a manner that ensures appropriate security of the Personal Data, whether physical or technical, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.** This means that the Code Member must have appropriate security in place to prevent the Personal Data held being accidentally or deliberately compromised. While information security is sometimes considered as cybersecurity (the protection of networks and information systems from attack), it also covers other things like physical and organisational security measures. Where appropriate, the Code Member should look to use measures such as pseudonymisation and encryption. The measures must ensure the 'confidentiality, integrity and availability' of the Code Member's systems and services and the Personal Data they process within them. The measures must also enable restoration and access to Personal Data in a timely manner in the event of a physical or technical incident. Poor information security leaves systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases. Some examples of the harm caused by a Code Member's loss or abuse of Personal Data include: identity fraud; targeting of individuals by fraudsters, potentially made more convincing by compromised Personal Data; witnesses put at risk of physical harm or intimidation; offenders at risk from vigilantes; breach of confidentiality of data and individuals involved in disputes; embarrassment of individuals, the subject of enquiry or even those commissioning an Investigation particularly those with high profile and/or media interest; exposure of the addresses of service personnel, police, and prison officers; and those at risk of domestic violence. Although these consequences do not always happen, the Code Member should recognise that individuals are still entitled to be protected from less serious kinds of harm, for example inconvenience. This is something that could easily happen were a Code Member to allow unauthorised access to confidential material or by misplacing legal papers entrusted to them, for example documents containing data on an individual who is the subject of Investigation and/or is a party to a case in which the Code Member is providing litigation support, particularly the delivery of court documents. Take for example a Code Member when attempting to personally serve court documents on an evasive party has the option under the rules of court to leave the papers in the party's presence where the party refuses to take them in hand. Were the documents so left in a public place and not retrieved by the party (as is often the case), they could fall into the wrong hands. The Code Member must consider the potential exposure of the Personal Data that will inevitably be included in the contents of the papers and take appropriate measures to secure against such a breach of the Personal Data, particularly when the

documents include Personal Data of other parties and not just that of the person being served.

It is important for the Code Member when appointing a sub-contractor that the instructions are entrusted only to a contractor suitably trained, trusted, accountable in at least UK GDPR and instructed in writing under Article 28 of the UK GDPR. There are for example numerous internet and email groups with numerous subscribers offering their services in the investigative and litigation support sector. The vetting process to become a subscriber may be minimal if any at all, and many subscribers use aliases and non-identifiable contact details thus raising a risk to the security of any instructions entrusted to them. The Code Member should resist appointing and entrusting instructions, which involve the processing of Personal Data, without the Code Member carrying out the minimum due diligence on the sub-contractor's authenticity, reliability, and UK GDPR and otherwise accountability, prior to any sub-contracting.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help demonstrate the Code Member's compliance with other aspects of the UK GDPR.

The security principle goes beyond the way the Code Member stores or transmits information. Every aspect of their processing of Personal Data is covered, not just cybersecurity. This means the security measures put in place should seek to ensure that:

> the data can be accessed, altered, disclosed, or deleted only by those who are authorised to do so (and that those people only act within the scope of the authority given);
> the data held is accurate and complete in relation to why the Code Member is processing it; and
> the data remains accessible and usable, i.e., if Personal Data is accidentally lost, altered, or destroyed, the Code Member should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as "confidentiality, integrity and availability" and under the UK GDPR, they form part of the Code Member's obligations.

The UK GDPR does not define the security measures that the Code Member should have in place. It requires them to have a level of security that is "appropriate" to the risks presented by their processing. They need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context, and purpose of the processing.

This reflects both the UK GDPR's risk-based approach, and that there is no "one size fits all" solution to information security. It means that what's "appropriate" for one Code Member will depend on their own circumstances, the processing they're undertaking, and the risks it presents to their organisation.

So, before deciding what measures are appropriate, the Code Member needs to assess the information risk. They should review the Personal Data held and the way they use it to assess how valuable, sensitive, or confidential it is – as well as the damage or distress

	that may be caused if the data was compromised. The Code Member should also take account of factors such as: the nature and extent of the organisation's premises and computer systems; the number of staff they have and the extent of their access to Personal Data; and any Personal Data held or used by a data Processor acting on the Code Member's behalf. An information security policy would assist to ensure the performance of appropriate security of Personal Data. Carrying out an information risk assessment is another example of an organisational measure, but the Code Member will need to take other measures as well, aiming to build a culture of security awareness within their organisation. Clear accountability for security will ensure that the Code Member does not overlook these issues, and that the overall security posture does not become flawed or out of date. Although an information security policy is an example of an appropriate organisational measure, a Code Member may not need a 'formal' policy document or an associated set of policies in specific areas. It depends on the size and the amount and nature of the Personal Data processed, and the way they use that data. However, having a policy does help demonstrate how the Code Member is taking steps to comply with the security principle. Whether or not the Code Member has such a policy, they still need to consider security and other related matters, such as: co-ordination between key people in their organisation; access to premises or equipment given to anyone outside the organisation (e.g., for computer maintenance) and the additional security considerations this will generate; business continuity arrangements that identify how the Code Member will protect and recover any Personal Data held; and periodic checks to ensure that the security measures remain appropriate and up to date. Technical measures are sometimes thought of as the protection of Personal Data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen, or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security. When considering physical security, the Code Member should look at factors such as: the quality of doors and locks, and the protection of their premises by such means as alarms, security lighting or CCTV; how they control access to their premises, and how visitors are supervised; how they dispose of any paper and electronic waste; and how they keep IT equipment, particularly mobile devices, secure.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible for the Code Member to assume that their systems are vulnerable, and they need to take steps to protect them.

When considering cybersecurity, the Code Member should look at factors such as:

system security – the security of their network and information systems, including those which process Personal Data;
data security – the security of the data held within their systems, e.g., ensuring appropriate access controls are in place and that data is held securely;
online security – e.g., the security of their website and any other online service or application that they use; and
device security – including policies on BYOD.

When considering what procedures to put in place, the Code Member should undertake a risk analysis and document their findings.

Confidentiality, integrity and availability are collectively known as the 'CIA triad'. They are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for the Code Member, as a data Controller, their Client and for the individuals whose data they process.

The information security measures implemented should seek to guarantee confidentiality, integrity and availability, both for the systems themselves and any Personal Data they process.

The CIA triad has existed for several years and its concepts are well-known to security professionals.

Code Members are also required to have the ability to ensure the "resilience" of their processing systems and services. Resilience refers to:

whether the Code Member's systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident; and
their ability to restore them to an effective state.

This refers to things like business continuity plans, disaster recovery, and cyber resilience.

A Code Member must have the ability to restore the availability and access to Personal Data in the event of a physical or technical incident in a "timely manner". The key point is that they have taken this into account during the information risk assessment and selection of security measures. For example, by ensuring that they have an appropriate backup process in place and thus will have some level of assurance that if their systems do suffer a physical or technical incident they can restore them, and therefore the Personal Data they hold, as soon as reasonably possible.

		Example: The minimum security measures for a Code Member to have in place as a matter of policy include: • Password protected access to computers. • Work environments in which Personal Data may be kept should be inaccessible to the unauthorised (e.g., keep office/work areas locked). • The Code Member takes regular backups of its systems and the Personal Data held within them, following the "3-2-1" backup strategy, that is, three copies, with two stored on different devices and one stored off-site. • Back-up and other memory devices should be kept locked away. • Transfer of Personal Data only in encrypted format or within password protected files (especially when transferred by email).
ACCOUNTABILITY		Accountability is one of the key principles in Data Protection Law – it makes the Code Member responsible for complying with the legislation and says that they must be able to demonstrate compliance. It's a real opportunity to show that the Code Member sets high standards for privacy and leads by example to promote a positive attitude to data protection. Accountability enables the Code Member to minimise the risks of what they do with Personal Data by putting in place appropriate and effective policies, such as the model documents available to ABI Members, their procedures, and measures. These must be proportionate to the risks, which can vary depending on the amount of data being handled or transferred, its sensitivity and the technology used. Regulators, business partners and individuals need to see that the Code Member is managing Personal Data risks if they want to secure their trust and confidence. This can enhance the Code Member's reputation and give them a competitive edge, helping their business to thrive and grow. There are a number of measures that the Code Member can, and in some cases must, take including: adopting and implementing data protection policies; taking a 'data protection by design and default' approach [23];

[23] Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything the Code Member does, throughout all their processing operations. The UK GDPR suggests measures that may be appropriate such as minimising the data collected, applying pseudonymisation techniques, and improving security features. A DPIA is an essential accountability tool and

putting written contracts in place with organisations that process Personal Data on their behalf [24];
maintaining documentation of their processing activities [25];
implementing appropriate security measures;
recording and, where necessary, reporting Personal Data breaches;
carrying out data protection impact assessments for uses of Personal Data that are likely to result in high risk to individuals' interests;
appointing a data protection officer; and
adhering to relevant codes of conduct and signing up to certification schemes.

Accountability obligations are ongoing so the Code Member must review and, where necessary, update the measures put in place. Being accountable can help the Code Member build trust and confidence with their Clients and the individuals who have the right to be informed about what Personal Data the Code Member collects, why it is used and shared with and may help mitigate enforcement action.

There are two key elements.

First, the accountability principle makes it clear that the Code Member is responsible for complying with the UK GDPR.

Second, the Code Member must be able to demonstrate compliance.

This also means the Code Member:

ensures a good level of understanding and awareness of data protection amongst their staff;

a key part of taking a data protection by design approach. It helps to identify and minimise the data protection risks of any new cases being undertaken.

[24] Whenever a Code Member uses a Processor to handle Personal Data on their behalf, it needs to put in place a written contract that sets out each party's responsibilities and liabilities. Contracts must include certain specific terms as a minimum, such as requiring the Processor to take appropriate measures to ensure the security of processing and obliging it to assist the Controller in allowing individuals to exercise their rights under the UK GDPR. Using clear and comprehensive contracts with Processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

[25] Under Article 30 of the UK GDPR, most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention. Documenting this information is a great way to take stock of what the Code Member does with Personal Data. Knowing what information they have, where it is and what they do with it makes it much easier for the Code Member to comply with other aspects of the UK GDPR such as making sure that the information held about people is accurate and secure. As well as their record of processing activities under Article 30, the Code Member also needs to document other things to show compliance with the UK GDPR. For instance, they need to keep records of consent, subject access requests and any Personal Data breaches.

	implements comprehensive but proportionate policies and procedures for handling Personal Data; keeps records of what they do and why; they must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR; the measures should be risk-based and proportionate; and they need to review and update the measures as necessary. Taking responsibility for what the Code Member does with Personal Data, and demonstrating the steps they have taken to protect people's rights not only results in better legal compliance, it also offers them a competitive edge. Accountability is a real opportunity to show, and prove, how the Code Member respects people's privacy. This can help them to develop and sustain people's trust and with it the confidence of their Clients. Furthermore, if something does go wrong, then being able to show that they actively considered the risks and put in place measures and safeguards can help the Code Member provide mitigation against any potential enforcement action. On the other hand, if they can't show good data protection practices, it may leave them open to fines and reputational damage.

Appendix III - Legitimate Interests Examples

The following are simple brief examples where the Code Member considers legitimate interests or consent as the lawful basis. It is important for the Code Member to carry out their own LIA in each case to ensure all parts of the LIA three-part test are met prior to any processing.

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 could accept the Client's instructions on condition that if the Data Subject is located, the Code Member will have to undertake new processing to contact the Data Subject to explain the instructions. This new processing would require an appropriate legal basis which will be fact-sensitive. Specifically, if the Code Member relies on the Client's consent then if it unable to achieve it 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 Data Subject. This will be a fact-sensitive and case-by-case assessment and further guidance is referred to in Part B paragraph 0.	If the 3-part LIA is met, the Code Member's legitimate interest will enable the pre-trace processing and thereafter the Code Member will consider a further LIA for the new processing. Alternatively, the Code Member could rely on consent if appropriate.
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 a Data Subject 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 on being satisfied as to the genuine existence of the debt / claim (regardless of whether it may be disputed), may accept the Client's 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 Data Subject. The latter, in any event, is unlikely to consent to the processing of their Personal Data for the Client's purpose.	Subject to the Code Member's LIA meeting the 3-part test no further safeguards such as the Data Subject's consent would be required or likely to be forthcoming and may compromise the Client's purpose were consent sought.

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 3-part test is likely to conclude that the Client's purpose does not give rise to a legitimate interest; however, if a compelling reason existed the Code Member could consider processing limited to locating the Data Subject in order that they may be able to seek their consent prior to any further processing, in particular the sharing of data. In the event consent is declined, the Code Member must cease further processing including the deletion of the Personal Data.	Curiosity is unlikely to meet the Code Member's LIA 3-part test. The Data Subject's consent could be considered by the Code Member if a compelling purpose exists.
	The Client wishes to seek resolution concerning the Data Subject's child, e.g., child support, access, custody, or a financial or property issue requires resolution.	The purpose is potentially contentious, and the Client has a legitimate interest that outweighs the interests and fundamental rights of the Data Subject.	Subject to the Code Member's LIA meeting the 3-part test the Code Member may proceed.
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 Data Subject. If the Client's suspicion is found to be true, the Data Subject may expose the Client to some financial risk or other harm.	Subject to the Code Member's LIA meeting the 3-part test the Code Member may proceed but where Special Category 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 an Article 6 lawful basis.
	The Client has reasonable cause to suspect their partner's infidelity.	The purpose is potentially contentious and the Code Member must consider the legitimate interest of the Client. It may not outweigh the interests and fundamental rights of the Data Subjects. The key test will be whether the harm of infidelity alone meets the third part of the LIA. Unless circumstances provide, it may be unlikely to do so. The Code Member should also consider Article 9 or 10 conditions where information involves Special Category Data, for example a Data Subject's sex life and/or Criminal Offence Data.	Infidelity alone is unlikely to meet the Code Member's LIA three-part test. It must be shown that the legitimate interests of the third party (the Client) outweigh the rights and freedoms of the Data Subject. If the Code Member is satisfied that given the circumstances involved, the potential harm caused to the Client outweighs these rights and freedoms then the member may proceed but where Special Category 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 an Article 6 lawful basis.

DUE DILIGENCE / BACKGROUND CHECKS			
CLIENT'S INSTRUCTIONS	PURPOSE	CODE MEMBER'S ACTION	SAFEGUARDS
To investigate the background and/or financial reliability of the Data Subject.	An elderly relative, a widower, has formed a new relationship with a much younger person. The family, (Client) suspects that the younger person is interested in a financial gain and may be taking advantage of them. They would like to know more about the person in order to allay their fears or confront the person / warn the elderly relative.	On being satisfied that the cause for concern is genuine and reasonable on carrying out the LIA the Code Member is likely to be satisfied the 3-part test is met and the instructions to conduct reasonable Investigation is justified.	Subject to the Code Member's LIA meeting the 3-part test the Code Member may proceed.
	In anticipation of the Client's commitment to a business involvement on the Data Subject's proposal for the Client's investment.	The Client requires due diligence be carried out on the Data Subject to mitigate the risks to the Client's financial exposure and/or reputation. The Data Subject would reasonably expect the Client to undertake such an Investigation prior to entering the commitment.	Subject to the Code Member's LIA meeting the 3-part test the Code Member may proceed. However, where no proposal has been initiated by the Data Subject and the Client's interest is exploratory, invisible processing would not be justified but the Code Member could consider obtaining the Data Subject's consent prior to any processing.

Appendix IV - Data Protection Impact Assessment - Template

Name of Controller	*Code Member*
Name of Controller contact	
Contact details	

DATA PROTECTION IMPACT ASSESSMENT
PROJECT NO: .....

1: The need for the DPIA:	**Code Member's Answers / Conclusions**
Explain broadly what 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 other: 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 Data Subjects; vii. innovative technological or organisational solutions; viii. processing that involves preventing Data Subjects 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 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. The Code Member may be able to justify a decision not to carry out a DPIA if confident that the processing is nevertheless unlikely to result in a high risk, but the reasons should be documented. In some cases a DPIA may be needed if only one of the above factors is present – and it is good practice to do so.	

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 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 and/or criminal data.	
iv. The extent and frequency of the processing.	
v. The duration of the processing.	
vi. The number of Data Subjects 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 codes of practice, guides, policies [26].	
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:	
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 their Client	

[26] Such as

(a) The Association of British Investigators Policy & Good Practice Guide - Use & Deployment of Global Positioning System (GPS) Electronic Tracking Devices, CLICK HERE

(b) Certified to BS102000/2018 Code of Practice in the Provision of Investigative Services

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. Data subject, such as in the SAFEGUARDS (CONSENT) scenarios. In most cases it should be possible to consult relevant stakeholders in some form. However, if you decide this is not appropriate, you should 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.	
4**: 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. To provide privacy information to individuals. d. To support individuals' rights. e. To ensure sub-contractors comply.	

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 Data Subjects, a layoff and/or a financial jeopardy.

		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
	Total overall risk to be reduced			

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		
		Eliminated (E), Reduced (R), or Accepted (A)	***Low (L), Medium (M), or High***	***Risks reduced from I – xi in section 5***
i.	Deciding not to collect certain types of data.	Effect on risk	Residual risk	Which risks
ii.	Reducing the scope of the processing.	Effect on risk	Residual risk	Which risks
iii.	Reducing retention periods.	Effect on risk	Residual risk	Which risks
iv.	Taking additional technological security measures.	Effect on risk	Residual risk	Which risks
v.	Training staff to ensure risks are anticipated and managed.	Effect on risk	Residual risk	Which risks
vi.	Anonymising data where possible.	Effect on risk	Residual risk	Which risks
vii.	Writing internal guidance or processes to avoid risks.	Effect on risk	Residual risk	Which risks
viii.	Using a different technology.	Effect on risk	Residual risk	Which risks
ix.	Making changes to privacy notices.	Effect on risk	Residual risk	Which risks
x.	Offering individuals, the chance to opt out where appropriate.	Effect on risk	Residual risk	Which risks
xi.	Implementing new systems to help individuals to exercise their rights.	Effect on risk	Residual risk	Which risks
xii.	Other.	Effect on risk	Residual risk	Which risks
xiii.	Other.	Effect on risk	Residual risk	Which risks

7: Sign off and record outcomes: 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 risk' after taking additional measures; and iv. whether you need to consult the ICO.	**Code Member's Conclusions**

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

Click HERE to download this template

Appendix V – Code Member Criteria

The Criteria are set at a standard readily achievable by any practicing Code Services provider and represents the minimum requirement to achieve membership of the ABI sufficient to satisfy most Client's expectations for their chosen service provider.

Criteria	Evidence requested	Guidance
ABI Membership criteria.	[***This evidence is optional. If a Code Member meets this control measure, the rest of the evidence requested in this Criteria will be met***] Proves Full / Provisional ABI membership	Appears on the list of Full / Provisional members of the ABI available at https://www.theabi.org.uk/membership-search .
	Proves 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 3 months should be provided.
	Holds professional indemnity insurance with a minimum cover set at least £250,000.	A letter from the insurer confirming the professional indemnity insurance cover is provided at the level prescribed and for the current period. Any relevant certification of insurance.
	Correctly registered with the ICO.	An up-to-date ICO registration certificate or a link to the ICO register with the correct contact and address details provided.
	Produced 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.
	Provided two satisfactory professional or character references.	References should include details on your qualifications, work ethic, skills, strengths and achievements.

Criteria	Evidence requested	Guidance
	Provided a comprehensive CV.	The CV should cover all qualifications, education and relevant work experience.
	Passed a personal and corporate financial probity check that is free of monetary judgments or insolvency.	A financial probity check may be done through a variety of providers.
	Provided two redacted reports as work samples in the area of Investigation or Litigation Support Services.	All Personal Data should be redacted from the reports and should be from the last 2 years.
Training	Adequately trained and competent in professional Investigation and sector specific Data Protection Law.	Adequate training means satisfactorily completing either the level 3 award in professional Investigation and data protection to the level comparable to the ABI UK GDPR compliance workshop, or training to an equivalent standard on the focus areas covered by the Code.
	Maintained an adequate record of training completion and performance.	Retains a log of training completed and scores on any assessments undertaken.
	Analysed training needs to ensure they are fit for purpose.	Uses ABI recommended training modules to cover the key areas of the Code.
	Training content covering roles and responsibilities.	The training in this scope must cover the difference in the roles of a Controller, Joint Controller and that of a Processor, and be able to assess the Code Member role in varying case scenarios.
	Training content covering DPIAs.	This training in this scope should cover 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 Data Subjects and measures envisaged to address risks.
	Training content covering lawful bases under Article 6 of the UK GDPR.	The training in this scope must cover what the lawful bases are, when processing is necessary, why lawful bases for processing are important, how to decide which

Criteria	Evidence requested	Guidance
		lawful basis applies, how to document the lawful basis and what information needs to be provided to individuals.
	Training content covering LIAs	The training in this scope should cover how to complete an LIA, why an LIA needs to be done, how to decide the outcome of an LIA and next steps and how LIAs overlap with DPIAs.
	Training content covering the seven data protection principles.	The training in this scope must cover what the seven data protection principles are under the UK GDR and why the principles are importance in the context of private investigating.
Annual desktop assessment	A sample of up to three DPIAs from live cases conducted by the Code Member during the previous period 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.
	Case extracts, with an outline of the lawful basis for the processing under Article 6, 9 and/or 10 of the UK GDPR that it is fair and transparent for the processing of Personal Data relied on.	Code Members should 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; (iii) where Special Category / Criminal Offence Data is processed, a condition for processing such data is identified
	A sample of up to three LIAs from live cases conducted by the Code Member during the previous period, as required by the MB.	The LIAs should be applied 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.

Criteria	Evidence requested	Guidance
Legislative compliance.	A legislation declaration certifying their compliance with the relevant legislation.	Code Members should review all relevant aspects of applicable legislation before making the legislation declaration.
Address non-conformance report(s) (NCR).	Adequate response to an NCR in full and address all the points raised within the time frame for remedying them.	NCRs are issued if the MB considers the Code Member does not meet all the Criteria in the Code. Code Members should respond to an NCR by setting out in detail how they seek to address an NCR which may include updating DPIA and LIAs to ensure compliance with the UK GDPR and providing further evidence on the legal basis for processing Personal Data.
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 all the points raised within the time frame for remedying them.	Code Members should 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 evidence of operational email accounts. Where the MB has communicated with the Code Member, the Code Member must be able to demonstrate it has corresponded appropriately to cooperate with the MB, including in investigations over alleged infringements of the Code.
Roles and Responsibilities	Evidence that the applicant Code Member understands their role and responsibilities and document them 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, an applicant Code Member should be able to establish if it is acting as a Processor, Controller, or a Controller jointly with another Controller for specific data processing.
	Evidence that the applicant Code Member communicates data protection roles and responsibilities to its Client at an appropriate time.	Code Members should provide the MB with samples of documents sent to Clients detailing their roles and responsibilities on request. This may include formal engagement letters and email correspondence detailing the applicant Code Member's role as a Controller, Processor or Joint Controller as applicable.
DPIA	Provides a sample of DPIAs completed within the previous year. Provides any	Code Members should be able to determine when a DPIA is required and understand how to carry out the assessment

Criteria	Evidence requested	Guidance
	evidence of DPIAs carried out as requested.	
Demonstrate sectoral expertise	Provides evidence of recent work completed as requested including details on Investigations carried out and the Personal Data collected.	Code Members should keep up to date on the seven data protection principles under Article 5 of the UK GDPR and how they apply to the Code Member's activities.
Protect children's interests	Provides evidence of any relevant work completed where particular attention was given to processing the Personal Data of children.	Evidence provided by Code Members could 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.
Criminal convictions	Evidence may be required that the Code Member does not maintain a comprehensive register of criminal convictions such as by way of a written declaration.	Code Members are required to not maintain a comprehensive register of criminal convictions. To evidence this, evidence such as an annual written declaration may be required to ensure on-going compliance.
Lawful basis (legitimate interests).	Evidence may be required of any LIA undertaken which includes the thought process in reaching a decision and justification of the outcome.	Code Members are required to determine the appropriate legal basis for processing and, where relevant, keep a record of the LIA completed. The LIAs should be applied in accordance with Article 6(1)(f) of the UK GDPR. The three-part test should be applied being: the purpose test, the necessity test and the balancing test. For more information, please refer to the ICO's guidance here.
Trace/Locate	Provide evidence that the Code Member has considered and recorded lawful basis appropriately with particular reference to trace or locate instructions.	There is no standard form for documenting the legal bases for processing Personal Data, however Code Members should 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 that point and the Code Member should use that guidance to support its evidence of the thought process in reaching a decision and justification of the outcome.

Criteria	Evidence requested	Guidance
Complaints	Provides evidence of any complaints it has received from Data Subjects in relation to data protection and the steps it took to respond to the complaint.	Code Members should respond to Data Subjects' 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.
Reputation	Due diligence on the applicant among industry professionals has not revealed material reputational risks.	Code Members should not bring the profession into disrepute. Compliance with the Code is a certification that the applicant has the mark of approval within the industry. It should not be granted to those with existing reputational risks, in particular where those relate to data. Specialist industry advice may be sought for this criterion.
Knowledge	Provide evidence that the Code Member has sufficient working knowledge of the relevant law by way of a written declaration and evidence of training completed and answered questions if requested.	Applicants are expected to be sufficiently knowledgeable in areas of law and procedure relating to professional investigator work, as well as issues of privacy, human rights and data protection. Applicants may be asked specific questions on past work and should be able to demonstrate they are sufficiently knowledgeable about relevant law.
Risk	Evidence may be sought about the Code Member and whether they present a risk to fellow professionals or members of the public in their processing of Personal Data.	The Code Member must not be a risk to fellow professionals or members of the public. The MB may seek references from other colleagues in respect of the Code Member's professionalism and conduct in respect of their processing of Personal Data.