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 ABI 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 ABI Member finds later 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. • An ABI 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 ABI 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 ABI Member's processing of Personal Data following the Client's concerns about fraud or some other harmful and contentious issue. • An ABI 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 ABI 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[1].

[1] 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.

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 ABI 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). • An ABI 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. This requirement aims to ensure that the ABI Member is clear and open about the reasons for obtaining Personal Data, and that what the ABI 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 ABI Member. This is especially important for the ABI 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 ABI 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 ABI Member uses Personal Data. There are clear links with other principles – in particular, the fairness, lawfulness, and transparency principle. Being clear about why An ABI Member is processing Personal Data will help to ensure the processing is fair, lawful, and transparent. **Example:** A Client bank instructs the ABI 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 ABI Member in the specific task (purpose). Coincidentally and shortly after the ABI Member is instructed by a separate Client in a domestic dispute unrelated to the bank's purpose but concerning the same Data Subject. 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 ABI Member will not collect any more information than is necessary and required in order to perform the processing activity. The ABI 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 ABI 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 ABI 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 ABI 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 ABI Member must 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 ABI Member is engaged to find a particular debtor. The ABI Member collects information on several people with a similar name to the debtor. During the enquiry some of these people are discounted. The ABI Member must 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 ABI Member needs to process information about certain individuals only, they must 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 ABI 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 ABI Member must 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 ABI Member must 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 ABI 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 ABI Member to be continually updating findings and correcting any incorrect name/address. If it is discovered that Personal Data is incorrect or misleading, the ABI 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 ABI 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 ABI 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 ABI Member must be clear that it is a historical record. **Example**: Having reported on a trace enquiry the ABI Member later finds the individual moved house from London to Manchester. The ABI 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 ABI Member must carefully consider any challenges to the accuracy of Personal Data. An area in which An ABI Member will frequently encounter the need to address accuracy is in reports where opinion is expressed. The ABI 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 ABI 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 ABI Member must 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 An ABI Member. However, it may not always be practical to check the accuracy of Personal Data someone else provides. There is a frequent reliance by An ABI Member on the data provided in their desk-top research using database information. To ensure that the records are not inaccurate or misleading the ABI 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 ABI Member must 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 ABI 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 ABI 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 Data Protection Law does not set specific time limits for different types of data. This is up to the ABI Member and will depend on how long the data is needed for the data specified purposes. It must be a proportionate approach, balancing the ABI 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 ABI 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 ABI 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. Subject to other regulatory requirements, for example by the FCA or the SRA, if and when applicable, or contractual or Controller obligations, rarely will An ABI 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 Data Protection Law 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 ABI 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 ABI 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 ABI Member is holding old data for longer than needed.

In any event, the ABI Member must 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 ABI 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 ABI Member must immediately delete all Personal Data without sharing the data with the Client or otherwise.

Example: Practitioners in Code Services 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 Code Services usual statutory limitation period (in most contentious cases). Whilst An ABI 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 ABI 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: An ABI 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 ABI Member must remove it from their systems unless there are good reasons for keeping it. Such reasons could include if the ABI Member has also been asked to provide Code Services 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 ABI 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 ABI Member should look to use measures such as pseudonymisation and encryption. The measures must ensure the 'confidentiality, integrity and availability' of the ABI 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 An ABI 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 Code Services 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 ABI Member must 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 An ABI 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 ABI Member is providing Code Services, particularly the delivery of court documents. Take for example An ABI 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 ABI 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[2].

It is important for the ABI Member when appointing a sub-contractor that the instructions are entrusted only to a contractor suitably trained, trusted, accountable in at leas Data Protection Law and instructed in writing under Article 28(3) of the UK GDPR. There are for example numerous internet and email groups with numerous subscribers offering Code Services. 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 ABI Member must resist appointing and entrusting instructions, which involve the processing of Personal Data, without the ABI Member carrying out the minimum due diligence on the sub-contractor's authenticity, reliability, and Data Protection Law 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 ABI Member's compliance with other aspects of the Data Protection Law.

The security principle goes beyond the way the ABI 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 must 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 ABI Member is processing it; and
- the data remains accessible and usable, i.e., if Personal Data is accidentally lost, altered, or destroyed, the ABI Member must 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 Data Protection Law, they form part of the ABI Member's obligations.

The Data Protection Law does not define the security measures that the ABI 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

[2] For guidance on this issue An ABI Member may find it helpful to consider the judgments in *Howard Field v Giovanni del Vecchio* [2022] EWHC 1117 (Ch) and [2022] EWHC 1118 (Ch) and *Gorbachev v Guriev* [2019] EWHC 2684 (Comm).

purpose of the processing.

This reflects both the Data Protection Law'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 ABI 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 ABI Member needs to assess the information risk. They must 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 ABI Member must 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 ABI 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 ABI 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 ABI 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, An ABI 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 ABI Member is taking steps to comply with the security principle.

Whether or not the ABI 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 ABI 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 ABI Member must 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 ABI Member to assume that their systems are vulnerable, and they need to take steps to protect them.

When considering cybersecurity, the ABI Member must 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 ABI Member must 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 ABI Member, as a data Controller, their Client and for the individuals whose data they process.

The information security measures implemented must 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.

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

- whether the ABI 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.

An ABI 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 An ABI 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 must be inaccessible to the unauthorised (e.g., keep office/work areas locked).
- The ABI 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 must 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 ABI 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 ABI Member sets high standards for privacy and leads by example to promote a positive attitude to data protection. Accountability enables the ABI 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 ABI Member is managing Personal Data risks if they want to secure their trust and confidence. This can enhance the ABI Member's reputation and give them a competitive edge, helping their business to thrive and grow. There are several measures that the ABI Member can, and in some cases must, take including: • adopting and implementing data protection policies; • taking a 'data protection by design and default' approach [3]; • putting written contracts in place with organisations that process Personal Data on their behalf [4]; • maintaining documentation of their processing activities [5];

[3] Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything the ABI Member does, throughout all their processing operations. The Data Protection Law 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 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.

[4] Whenever An ABI 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 Data Protection Law. 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.

[5] 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

	• 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 ABI Member must review and, where necessary, update the measures put in place. Being accountable can help the ABI Member build trust and confidence with their Clients and the individuals who have the right to be informed about what Personal Data the ABI 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 ABI Member is responsible for complying with the Data Protection Law. Second, the ABI Member must be able to demonstrate compliance. This also means the ABI Member: • ensures a good level of understanding and awareness of data protection amongst their staff; • 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 Data Protection Law; • the measures must be risk-based and proportionate; and • they need to review and update the measures as necessary. Taking responsibility for what the ABI Member does with Personal Data, and demonstrating the steps they have taken to protect people's rights not only results in

information is a great way to take stock of what the ABI 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 ABI Member to comply with other aspects of the Data Protection Law 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 ABI Member also needs to document other things to show compliance with the Data Protection Law. For instance, they need to keep records of consent, subject access requests and any Personal Data breaches.

	better legal compliance, it also offers them a competitive edge. Accountability is a real opportunity to show, and prove, how the ABI 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 ABI 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.