BancTrust Securities (Europe) Limited

Data Protection and Data Security Policy

Version: 1.0

February 2020

Contents

1 Purpose

This policy details how BancTrust Securities (Europe) Limited (the Firm) will manage data protection and data security and ensure a consistency of approach within the Firm and adherence to the Data Protection Regulation. The Firm recognises that failure to protect personal data poses a risk to employees and clients and to the reputation and good standing of the company, as well as risking financial penalties.

Data Protection is regulated and enforced in the UK by the Information Commissioners Office (ICO) (https://ico.org.uk/).

The Firm is authorised by the Financial Conduct Authority (FCA) and complying with some of the FCA rules requires the Firm to process personal data.

While the ICO will regulate data protection, the FCA will also consider compliance with these regulations under their rules, in particular the Senior Management Arrangements, Systems and Controls standards in the FCA handbook (https://www.handbook.fca.org.uk/handbook).

2 Review of Policy

This policy will be reviewed by the Management Body and the Compliance Officer on an ongoing basis in line with any regulatory changes but at least once a year.

3 Responsibilities

3.1 The Management Body

The Management Body are responsible for the compliance with data protection and ensuring that the Firm is able to produce evidence to demonstrate the steps that it has taken to comply.

The Firm is not required to appoint a Data Protection Officer because it is not a public authority and its core activities do not consist of large scale, regular or systematic monitoring of individuals or large scale processing of special categories of data or data relating to criminal convictions and offences. The Management Body has decided not to voluntarily appoint a Data Protection Officer.

3.2 Employee Responsibilities

All employees, volunteers and business associates, such as Appointed Representatives, are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

All employees who deal with personal information are required to handle that information confidentially and sensitively. Employees who undertake to process personal data supplied by the Firm must do so only in accordance with the Firm's instructions.

Employee obligations in respect of the Data Protection Act form part of their contract of employment.

4 Definitions

4.1 Personal data

Personal data is any information relating to an, directly or indirectly, identified or identifiable natural person (also known as a data subject).

4.2 Special category data /Sensitive personal data

Special category or sensitive personal data refers to data relating to racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, genetic data or biometric data.

4.3 Data controller

A controller determines when, why and how to process personal data. The Firm is the controller of all personal data relating to its employees, clients and others whose personal data is used in its business for its commercial purposes.

4.4 Data processor

A processor is responsible for processing personal data on behalf of a data controller and should act only on the controller's instructions. Processing is any activity that involves the use of personal data such as obtaining, recording, holding, amending, using, transferring, erasing or disclosing it.

The Firm is a processor of personal data.

5 The Data Protection Principles

Data Protection law sets out 6 principles which define the obligations of the Firm as a processor of personal data. These principles are as follows:-

a) Personal data shall be processed lawfully, fairly and in a transparent manner

b) Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in any manner incompatible with those purposes

c) Personal data shall be adequate, relevant and limited to what is necessary for the purpose for which they are processed

d) Personal data shall be accurate and, where necessary, kept up to date

e) Personal data shall be kept in a form which permits identification of the data subjects for no longer than necessary for the purposes for which the personal data are processed

f) Personal data shall be processed in a manner that ensures the security of personal data

The data protection law states that the Firm shall be responsible for, and be able to demonstrate compliance with, these principles.

5.1 Lawful basis for processing

The Firm will ensure that it has a lawful basis to process personal data. The Firm will ensure that the processing is necessary for its purpose and that there is no other reasonable way to achieve that purpose.

The Firm will determine and document the lawful basis before beginning processing. There may be more than one lawful basis that applies to the processing and, if this is the case, the Firm will document it. The Firm will ensure that it can justify its reasoning for the lawful basis chosen.

The six lawful bases for processing personal data are:

1) Consent – the data subject has given clear consent for the Firm to process their personal data for a specific purpose
2) Contract – the processing is necessary for a contract the Firm has with the data subject or because they have requested that the Firm take specific steps before entering into a contract
3) Legal obligation – the processing is necessary for the Firm to comply with the law
4) Vital interests – the processing is necessary to protect someone's life
5) Public task – the processing is necessary for the Firm to perform a task in the public interest
6) Legitimate interests – the processing is necessary for the Firm's (or a third party's) legitimate interests unless there is good reason to protect the individual's personal data which overrides those legitimate interests

When choosing the lawful basis for processing, the Firm will consider what it is trying to achieve, can it reasonably be achieved in another way and whether or not it has a choice to process the data.

The Firm has reviewed its lawful bases for processing in the light of the General Data Protection Regulations (GDPR) and updated them where necessary. These were communicated to the data subjects before 25th May 2018.

If there is a change in circumstances or a new purpose for processing the data then the Firm will review the lawful basis and make any changes ensuring that the data subjects are informed and the change documented.

5.1.1 Consent

When requesting consent, the Firm will:

- Make the request for consent prominent and separate from its terms and conditions
- Ask people to positively opt-in
- Not use pre-ticked boxes or other types of default consent
- Use clear, plain language that is easy to understand
- Specify why it wants the data and what it will do with it
- Give individual options to consent to different purposes and types of processing
- Name the Firm and any other third parties who will be relying on consent
- Tell people that they can withdraw consent at any time
- Ensure that people can refuse consent without detriment
- Not make consent a precondition of a service

The Firm will record when, how and from whom it obtained consent and what they were told at the time of consent.

The Firm has reviewed its existing consents in light of GDPR and obtained fresh consent where necessary.

5.1.2 Contract

When using contract as the lawful basis for processing personal data, the Firm will ensure that the processing is necessary to deliver its side of the contract and that it could not reasonably do what was required without processing the personal data.

5.1.3 Legal obligation

When using legal obligation as the lawful basis for processing personal data, the Firm will ensure that the processing is necessary to comply with a law or statutory obligation and that it could not reasonably do what was required without processing the personal data. The Firm will identify the specific legal provision or appropriate source of advice that sets out its obligation.

5.1.4 Vital interests

The Firm is unlikely to use vital interests as a lawful basis for processing personal data.

When using vital interests as the lawful basis for processing personal data, the Firm will ensure that the processing is necessary to protect someone's life and that it could not reasonably do what was required without processing the personal data. The Firm will not use vital interests as the lawful basis if the data subject is capable of giving their consent.

5.1.5 Legitimate interests

The Firm is aware that when it uses legitimate interests as the lawful basis for processing personal data that it takes on extra responsibility for protecting the people's rights and interests.

The Firm will avoid using legitimate interests as the lawful basis where individuals would not reasonably expect the processing or where their interests are likely to override the Firm's legitimate interests.

The Firm will use a legitimate interests assessment (LIA) to check whether it is appropriate to rely on legitimate interests as the lawful basis for processing personal data and will record this and the outcome to demonstrate compliance with accountability obligations. The LIA consists of 3 parts:

1) Purpose test – is the Firm pursuing a legitimate interest?
2) Necessity test – is the processing necessary for that purpose?
3) Balancing test – do the individual's interests override the legitimate interest?

Considerations for these 3 tests are listed in Annex 1 – Legitimate Interests Assessments. If the LIA identifies significant risks then the Firm will consider performing a Data Protection Impact Assessment (DPIA) to assess the risks and potential mitigation in more detail.

When the Firm uses legitimate interests as the lawful basis, the individual's right to data portability does not apply.

5.1.6 Special category data/sensitive personal data

The Firm will ensure that it meets at least one of the following conditions before processing special category data:

a) The data subject has given explicit consent to the processing of those personal data for a specified purpose

b) The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and social security and social protection law

c) The processing is necessary to protect the vital interests of the data subject or another person where the data subject is incapable of giving consent

d) The processing is carried out in the course of its legitimate activities with appropriate safeguards by a body, with a political, philosophical, religious or trade union aim, on condition that the processing relates solely to the members, or former members, of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

e) The processing relates to personal data which is clearly made public by the data subject

f) The processing is necessary for legal claims or courts acting in their judicial capacity

g) The processing is necessary for reasons of substantial public interest and is proportionate to the aim pursued, respectful of the right to data protection and provides measures to safeguard the fundamental rights and the interests of the data subject

h) The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

i) The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices which provides measures to safeguard the rights and freedoms of the data subject

j) The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which are proportionate to the aim pursued, respectful of the right to data protection and provides for measures to safeguard the fundamental rights and the interests of the data subject

The Firm will record any special category conditions that are applicable to the personal data it is processing.

5.1.7 Criminal offence data

Personal data on criminal convictions or offences can only be processed if the Firm has an official authority to do so, is processing the data in an official capacity or meets one of the specific conditions in Schedule 1 of the Data Protection Act 2018, which includes; preventing or detecting unlawful acts, protecting the public against dishonesty, regulatory requirements relating to unlawful acts and dishonesty, preventing fraud, suspicion of terrorist financing and money laundering and legal claims . The Firm has no official authority to process criminal offence data but does meet one or more of the specific conditions in Schedule 1 for the criminal offence data that it may process.

6 Rights of the individual/data subject

The Firm recognises that the data subjects/individuals have the following rights:

1) The right to be informed

2) The right of access
3) The right of rectification
4) The right to erasure
5) The right to restrict processing
6) The right to data portability
7) The right to object
8) Rights in relation to automated decision making and profiling

6.1 Right to be informed

The Firm will provide individuals with the following privacy information:

- The name and contact details of the Firm
- The purposes of the processing
- The lawful basis for the processing
- The legitimate interests for the processing (if applicable)
- The categories of personal data obtained (if the data is obtained from a third party)
- The recipients or categories of recipient of the personal data
- The details of any transfers of the personal data to any third countries or international organisations
- The retention periods of personal data
- The rights available to individuals in respect of the processing
- The right to withdraw consent (if applicable)
- The right to lodge a complaint with the ICO
- The source of personal data (if the data is obtained from a third party)
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (Note: this is not required when the personal data is obtained from sources other than the data subject)
- The details of any automated decision-making, including profiling (if applicable)

The Firm will provide this information to individuals at the time they collect the data from them. If the data is obtained from another source then the Firm will provide this information within a reasonable time and no later than a month after receiving the data. If the Firm is planning to communicate with the individual, it will provide the privacy information when it communicates for the first time. If the Firm is disclosing the information to a third party, the Firm will provide the individual with the privacy information at the latest when the data is disclosed.

The Firm will regularly review and update its privacy information. Any new uses of personal data will be brought to the data subject's attention before the new processing starts.

6.2 Right of access

The Firm recognises that individuals have the right to obtain: confirmation that their data is being processed, access to their personal data and the information provided in the privacy information.

The Firm will provide this information free of charge. The Firm may charge a fee, based on the administrative costs of processing the request, for requests for further copies of the same information.

Where an individual makes a request for a copy of their information, this should be managed by the Compliance Officer.

6.3 Right to rectification

The Firm will respond to any request for rectification of inaccurate or incomplete data within one month, or within three months if the request is complex. If the personal data has been disclosed to third parties, the Firm will inform them of the rectification.

6.4 Right to erasure

The Firm recognises that individuals have the right erasure in certain circumstances, and will erase the data without undue delay, contacting any third parties, to whom the data has been passed, to inform them to erase the data.

The circumstances in which the right to erasure exists are as follows:

- Where personal data is no longer necessary for the purpose for which it was originally collected or processed
- The data subject withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate reason for continuing the processing
- The personal data was unlawfully processed
- The personal data has to be erased to comply with a legal obligation

The Firm can refuse the request for erasure for the following reasons:

- To exercise the right of freedom and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific or historical research or statistical purposes
- For the exercise or defence of legal claims

6.5 Right to restrict processing

The Firm will restrict the processing of personal data on request from an individual where one of the following applies:

- Where an individual contests the accuracy of the personal data, the processing will be restricted until the accuracy of the data has been verified or corrected

- Where an individual objects to the processing (where it was necessary for performance of a public interest task or legitimate interests) and the Firm is considering whether the Firm's legitimate grounds override those of the individual
- When the processing was unlawful and the individual opposes erasure and request restriction instead
- If the Firm no longer needs the personal data but the individual needs it for a legal claim

When the processing has been restricted, the Firm will, except for the storage of the data, only process the data with the individual's consent. The Firm will inform individuals before a restriction on processing is lifted.

6.6 Right to data portability

Where individuals have provided personal data to the Firm based on consent or for the performance of a contract and the processing is carried out by automated means, the individual has the right to data portability. The Firm will provide the personal data, without undue delay and within one month, in a structured, commonly used and machine-readable form. The Firm will provide this information free of charge.

6.7 Right to object

The Firm recognises that individuals have the right to object to direct marketing (including profiling), processing for the purposes of scientific or historical research and statistics and processing based on legitimate interests or the performance of a task in the public interest or exercise of official authority.

If an objection is received, the Firm will no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the individual or the processing is for the exercise or defence of a legal claim. For direct marketing the Firm will stop the processing as soon as the objection is received.

The Firm will inform individuals of their right to object at the point of first communication and in the privacy notice.

7 Accountability and Governance

7.1 Contracts with processors

The Firm will ensure that it has written contracts in place with any data processors. The Firm will only appoint data processors that can provide sufficient guarantees that they can meet the GDPR requirements and that the rights of the individuals will be protected.

The contracts will include the following information:

- The subject matter and the duration of the processing
- The nature and purpose of the processing
- The type of personal data and categories of the data subjects
- The obligations and rights of the Firm

The contract will include the following terms:

- The processor must only act on written instructions from the Firm

- The processor must ensure that the people processing the data are subject to a duty of confidence
- The processor must take appropriate measures to ensure the security of processing
- The processor must only engage a sub-processor with the prior consent of the Firm
- The processor must assist the Firm in providing subject access and allowing individuals to exercise their rights
- The processor must assist the Firm in meeting its obligations in relation to the security of processing, notification of personal breaches and DPIAs
- The processor must delete or return all personal data to the Firm as requested at the end of the contract
- The processor must submit to audits and inspections and provide the Firm with any information it needs to meet its obligations
- The contract does not relieve the processor of its own responsibilities under GDPR

7.2 Documentation/Record keeping

The Firm will document the following information:

- The name and contact details of the Firm
- The purposes of its processing
- A description of the categories of individuals and categories of personal data
- The categories of recipients of personal data
- Details of transfers and mechanisms of transfer to third countries
- Retention schedules
- A description of its technical and organisational security measures

As part of the processing activities, the Firm will also document:

- The lawful basis for processing
- The legitimate interests for processing
- Individuals' rights
- The existence of automated decision-making (including profiling)
- The source of personal data
- Records of consent
- Contract between the Firm and any processors
- The location of personal data
- DPIA reports
- Records of personal data breaches
- Information required for processing of special category data or criminal conviction and offence data

7.3 Employee Training

Employees will be trained on their data protection and security responsibilities at induction and given the necessary ongoing training to perform their roles in line with the Firm's policy and the data protection law.

7.4 Data protection impact assessments (DPIA)

The Firm will use DPIAs to help it identify the most effective way to comply with its obligations and meet individuals' expectations of privacy.

The Firm will use DPIAs when using new technologies and when the processing is likely to result in a high risk to the rights and freedoms of individuals.

8 Data Security

The Firm will ensure that any personal data held will be processed in a manner that ensures its security. It will ensure that its systems and processes include protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The Firm will regularly review its procedures for ensuring that personal data held remains accurate and consistent. It will, in particular, ensure that:

- Its IT systems are designed, where possible, to encourage and facilitate the entry of accurate data
- Data on any individual will be held in as few places as necessary, and all employee and volunteers will be discouraged from establishing unnecessary additional data sets
- Effective procedures will be in place so that all relevant systems are updated when information about any individual change

The Firm has undertaken an assessment of its information risk to determine an appropriate level of security, reviewing the data held and how it is used as well as how the damage or distress it would cause if the data was compromised.

The Firm has considered confidentiality, integrity and availability when implementing its data security measures ensuring that:

- The data can be accessed, altered and deleted only by persons the Firm has authorised to do so
- The data held is accurate and complete for the purposes for which the Firm is processing it
- The data remains accessible and usable, so it can be recoverable in the event of accidental loss, alterations or destruction

The Firm's security measures take into account both physical and cybersecurity, including the following:

- The protection of the Firm premises
- How access to the premises is controlled and how visitors are supervised
- How paper or electronic waste is disposed of
- How IT equipment is keep secure
- The security of the network and information systems
- The security of the data within the systems

- The security of the website

The Firm will also ensure the resilience of its systems and services, to enable the systems to continue operating under adverse conditions and the ability to restore the systems to an effective state within a timely manner.

The Firm will carry out periodic checks to ensure that its security measures remain appropriate and up to date.

9 International transfers

The Firm will only transfer personal data to third countries where the receiving organisations have provided adequate safeguards. Individuals' rights must be enforceable.

Adequate safeguards may be provided by:

- A legally binding agreement between public authorities or bodies
- Binding corporate rules (agreements governing transfers made between organisations within in a corporate group)
- Standard data protection clauses in the form of template transfer clauses adopted by the Commission
- Standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission
- Compliance with an approved code of conduct approved by a supervisory authority
- Certification under an approved certification mechanism as provided for in the GDPR;
- Contractual clauses agreed authorised by the competent supervisory authority
- Provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

In the absence of an adequacy decision, personal data can be transferred outside the EU where one or more of the following conditions are met:

- It is made with the individual's informed consent
- It is necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request
- It is necessary for the performance of a contract made in the interests of the individual between the Firm and another person
- It is necessary for important reasons of public interest
- It is necessary for the establishment, exercise or defence of legal claims
- It is necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent
- It is made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register)

10 Cooperation with the ICO

The Firm will cooperate with the ICO when requested.

11 Personal data breaches

A personal data breach can be defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

If a security incident occurs, the Firm will establish whether a personal data breach has occurred and if so, establish the likelihood and severity of the resulting risk to people's rights and freedoms.

The Firm will investigate the cause of the breach and determine what steps are required to correct it and prevent a recurrence.

11.1 Notification to the ICO

Where a personal data breach occurs and it has been established that there is a likely risk to people's rights and freedoms, the Firm will notify the ICO as soon as possible and within 72 hours of becoming aware of it. If the Firm takes longer than 72 hours to notify the ICO, it will provide the ICO with reasons for the delay.

The notification to the ICO will include:

- A description of the nature of the breach including the categories and approximate numbers of individuals concerned and the personal data records concerned
- The name and contact details of the point of contact within the Firm
- A description of the likely consequences of the breach
- A description of the measures taken to deal with the breach and measures taken to mitigate any possible adverse effects

The information may be provided to the ICO in phases as soon as possible if it is not all available within 72 hours. In these cases the Firm will explain the delay to the ICO and advise when it expects to submit further information.

A failure to notify the ICO can result in a significant fine.

11.2 Informing individuals about a breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Firm will inform those concerned as soon as possible.

The Firm will provide the following information to individuals when telling them about a breach:

- The name and contact details of the point of contact within the Firm
- A description of the likely consequences of the breach
- A description of measures taken to deal with the breach and mitigate any possible adverse effects

11.3 Recording breaches

The Firm will record all personal data breaches, documenting the facts of the breach, its effects and any remedial action taken. Decisions whether to report the breach to the ICO, or inform individuals will also be recorded.

12 Breaches of Data Protection and Data Security Policy

Any breaches of the Data Protection and Security Policy will be recorded on the Firm's breach log in conjunction with its Regulatory Breach Policy.

13 Annex 1 – Legitimate Interests Assessment (LIA)

13.1 Purpose Test

Considerations:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

13.2 Necessity Test

Considerations:

- Does this processing actually 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?

13.3 Balancing Test

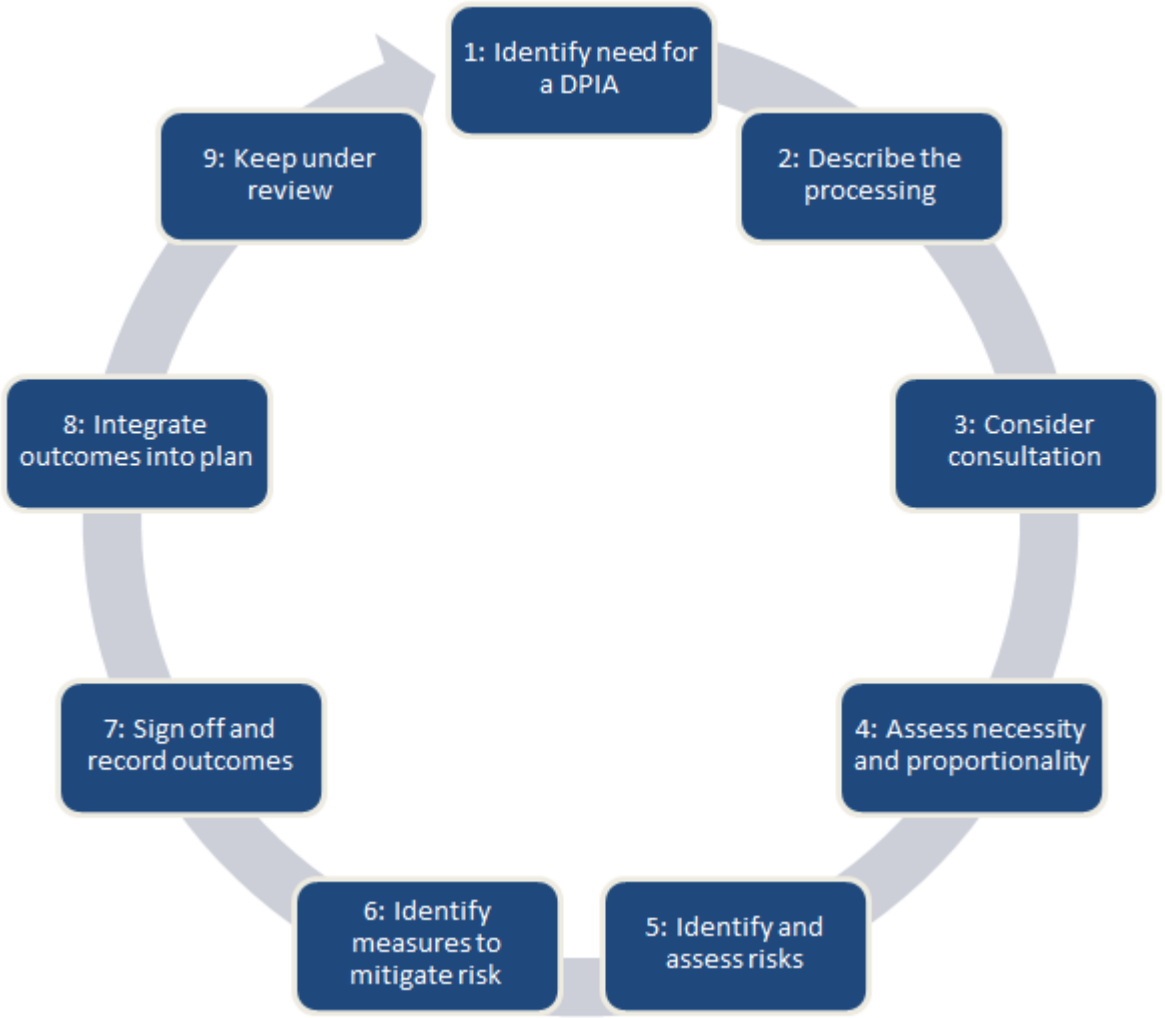
Considerations:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you 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?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

14 Annex 2 – Data Protection Impact Assessment (DPIA)

A DPIA must:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks



14.1 Identify the need for a DPIA

DPIAs must be used if the Firm is planning to:

- Use new technologies
- Use profiling or special category data to decide on access to services
- Profile individuals on a large scale
- Process biometric data
- Process genetic data

- Match data or combine datasets from different sources
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
- Track individuals' location or behaviour
- Profile children or target marketing or online services at them
- Process data that might endanger the individual's physical health or safety in the event of a security breach

14.2 Describe the processing

The description must include "the nature, scope, context and purposes of the processing".

14.2.1 Nature of processing

The nature of the processing is what the Firm plans to do with the personal data. This should include:

- How you collect the data
- How you store the data
- How you use the data
- Who has access to the data
- Who you share the data with
- Whether you use any processors
- Retention periods
- Security measures
- Whether you are using any new technologies
- Whether you are using any novel types of processing
- Which screening criteria you flagged as likely high risk.

14.2.2 Scope of processing

The scope of the processing is what the processing covers. This should include:

- The nature of the personal data
- The volume and variety of the personal data
- The sensitivity of the personal data
- The extent and frequency of the processing
- The duration of the processing
- The number of data subjects involved
- The geographical area covered

14.2.3 Context of processing

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include:

- The source of the data
- The nature of your relationship with the individuals
- The extent to which individuals have control over their data
- The extent to which individuals are likely to expect the processing
- Whether they include children or other vulnerable people
- Any previous experience of this type of processing
- Any relevant advances in technology or security
- Any current issues of public concern

14.2.4 Purpose of processing

The purpose of the processing is the reason why the Firm wants to process the personal data. This should include:

- Your legitimate interests, where relevant
- The intended outcome for individuals
- The expected benefits for you or for society as a whole

14.3 Consider consultation

The Firm should consult with individuals unless there is a good reason not to. If it is decided not to consult then the decision and rationale must be documented.

Data processors and all relevant internal stakeholders should also be consulted.

14.4 Assess necessity and proportionality

Considerations:

- Do your plans help to achieve your purpose?
- Is there any other reasonable way to achieve the same result?

The Firm should include how it ensures data protection compliance, in particular details of:

- Your lawful basis for the processing
- How you will prevent function creep
- How you intend to ensure data quality
- How you intend to ensure data minimisation
- How you intend to provide privacy information to individuals
- How you implement and support individuals rights

- Measures to ensure your processors comply
- Safeguards for international transfers

14.5 Identify and assess risks

The Firm must consider the potential impact on individuals, in particular whether the processing will contribute to:

- Inability to exercise rights (including but not limited to privacy rights)
- Inability to access services or opportunities
- Loss of control over the use of personal data
- Discrimination
- Identity theft or fraud
- Financial loss
- Reputational damage
- Physical harm
- Loss of confidentiality
- Re-identification of pseudonymised data
- Any other significant economic or social disadvantage

The Firm must include an assessment of the security risks, including sources of risk and the potential impact of each type of breach. To assess the level of risk, the Firm must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The Firm should also consider its own corporate risks, such as the impact of regulatory action and reputational damage.

14.6 Identify measures to mitigate risk

Against each risk identified, the Firm must record the source of that risk and then options for reducing that risk.

Options for mitigation can include:

- Deciding not to collect certain types of data
- Reducing the scope of the processing
- Reducing retention periods
- Taking additional technological security measures
- Training staff to ensure risks are anticipated and managed
- Anonymising or pseudonymising data where possible
- Writing internal guidance or processes to avoid risks

- Adding a human element to review automated decisions
- Using a different technology
- Putting clear data sharing agreements into place
- Making changes to privacy notices
- Offering individuals the chance to opt out where appropriate
- Implementing new systems to help individuals to exercise their rights

The Firm must record whether the measure would reduce or eliminate the risk. Take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

If a high risk is identified that cannot be mitigated, the Firm must consult the ICO before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to process the data, or ban the processing altogether.

14.7 Sign off and record outcomes

The Firm should record:

- What additional measures you plan to take
- Whether each risk has been eliminated, reduced, or accepted
- The overall level of 'residual risk' after taking additional measures
- Whether you need to consult the ICO

As part of the sign-off process, the DPO should advise on whether the processing is compliant and can go ahead. If it is decided not to follow the DPO's advice, the reasons for this should be recorded. Any reasons for going against the views of individuals or other consultees should be recorded.

14.8 Integrate outcomes into plan

The outcomes of DPIAs must be integrated back into project plans, identifying any action points and owners.

14.9 Keep under review

The Firm must monitor the ongoing performance of the DPIA.