Data Protection Impact Assessment Procedure

1. Introduction

1.1 This Data Protection Impact Assessment Procedure (this "procedure") sets out guidance and procedures to be followed by all employees, workers and contractors ("personnel", "you", "your") of [Subject] ("Middleton Asset Management", "we", "us", "our") when carrying out a data protection impact assessment ("DPIA"). This procedure relates to individuals whose personal data we collect and process ("data subjects").

1.2 This procedure has been prepared with due regard to the data protection laws applicable to D[redacted] and our personal data processing activities. These data protection laws include the UK General Data Protection Regulation ("UK GDPR") and / or EU General Data Protection Regulation ("EU GDPR" - EU Regulation 2016/679) (whichever is applicable) and the Data Protection Act 2018 ("DPA 2018") (collectively referred to as the "Data Protection Law").

1.3 This procedure should be read together with the following related documents:

a) D[redacted] Data Protection Impact Assessment
b) Template Middleton Asset Management Data Protection by Design & by
c) Default Policy Middleton Asset Management Data Protection Policy

2. Purpose of this Procedure

2.1 A DPIA is required by law for specific personal data processing activities or any other processing that is likely to result in a high risk to the rights and freedoms of data subjects. A DPIA is also required in specific circumstances mandated by the relevant supervisory authorities. The supervisory authority in the UK is the Information Commissioner's Office (ICO).

2.2 The purpose of this procedure is to provide guidance on DPIAs (including their purpose and the meaning of certain concepts), together with a formal procedure to follow when carrying out DPIAs on behalf of Middleton Asset Management. This procedure should be used in conjunction with the Middleton Asset Management DPIA Template.

2.3 This procedure applies to all Middleton Asset Management personnel. You must follow this procedure when carrying out a DPIA. Any failure to do so may result in disciplinary action.

3. Scope

3.1 This policy applies to all personal data processed by Middleton Asset Management, whether held in electronic form or in physical records, and regardless of the media on which that data is stored.

3.2 D[redacted] is registered as a data controller with the [Information Commissioner's Office/Relevant Supervisory Authority] having registration numberC1331941

4. About DPIAs

4.1 <u>What is a DPIA?</u>

A DPIA is process used to identify and assess the risks associated with processing personal data and the measures and controls that can be applied to mitigate the risks whilst meeting the objectives of the processing, where possible. A DPIA should take account of the risks to rights and freedoms of data subjects and of the compliance risks to Middleton Asset Management.

4.2 DPIAs are appropriate at the start of a new project that involves processing personal data and during the life of the processing, especially if the processing activity changes in a material way.

4.3 DPIAs are important to Middleton Asset Management because we collect, hold and process personal data. DPIAs help us manage the risks associated with these processing activities. They also help embed 'data protection by design and by default' in our working practices, IT systems and customer applications and assist in demonstrating accountability. These are legal requirements but are also necessary when building trust and engagement with our customers and employees.

4.4 <u>What is meant by risk?</u>

Risks to data subjects means the potential for harm, including physical, material and non-material (e.g. distress) harm to individuals or to society at large. A DPIA should consider the likelihood and the severity of the impact on individuals. Whilst the likelihood of harm might be low, the severity may be high. Likewise, the likelihood might be high but the severity or impact to data subjects might be low.

4.5 Risks to data subjects may arise, for example, from misuse or overuse of their personal data, lack of transparency, collecting too much of their personal data than is necessary or not protecting the confidentiality of their personal information.

4.6 Compliance risks are those which affect Middleton Asset Management, such as a breach of the UK GDPR and/or the EU GDPR and/or the DPA2018, which may result in a fine or other regulatory action and damage to our reputation.

4.7 A DPIA does not have to eradicate all risks but should help minimise risks to a tolerable level or, where this is not possible, identify situations where we need to consult with the relevant supervisory authority before processing personal data.

4.8 <u>When should I carry out a DPIA?</u>

A DPIA must be carried out when required by law or by the relevant supervisory authority. As a general rule, a DPIA must be carried out where a processing activity (including the use of an IT system or technology) is likely to result in a high risk to the rights and freedoms of data subjects.

4.9 For new projects, DPIAs help ensure data protection by design and build in data protection compliance at an early stage when there is most scope for influencing how the processing activity is developed and implemented. Carrying out a DPIA as a part of our project management processes enables us to integrate the outcomes of the DPIA back into our project planning.

❖

4.10 Because the risks associated with personal data processing activities will change over time, a DPIA should not be seen as a one-off exercise but as an ongoing process and subject to regular reviews. An existing processing activity may have started as a low-risk activity but may grow in risk over time, especially if new uses are made of the personal data in question or if we start collecting more personal data within an existing processing activity. As such, a DPIA should be seen as a 'living' process to help us manage processing risks and the safeguards we've put in place on an ongoing basis.

4.11 What should a DPIA include?

As a minimum, a DPIA must:

- Describe the processing activity and the purposes of the processing;
- Assess the necessity and proportionality of the processing in the context of the purposes of the processing;
- Identify and assess the risks to individual data subjects; and
- Identify measures to mitigate the risk and protect the personal data.

4.12 This procedure sets out the steps to take when carrying out a DPIA. The Middleton Asset Management DPIA Template should be used when carrying out a DPIA.

4.13 What if risks are still high even if we apply safeguards identified by the DPIA?

A DPIA should help identify safeguards to reduce the risks to data subjects to a manageable and acceptable level. If a DPIA indicates that risks are still likely to be high even after implementing safeguards it is an indication that the processing may not be appropriate and should not proceed.

4.14 If, in these circumstances, we still wish to proceed with the processing activity covered by the DPIA we can consult with the relevant supervisory authority and ask for their approval. This involves sharing the DPIA with them together with additional information they request.

4.15 The relevant supervisory authority is entitled to advise us that:

- The risks are acceptable, and we can proceed;
- We need to take further measures to reduce the risks;
- We have not identified all risks and need to review our DPIA;
- The DPIA is not compliant and must be repeated; or
- The processing cannot proceed

4.16 In some circumstances, the relevant supervisory authority may take more formal action.

5. DPIA Obligations

5.1 A DPIA must be carried out before or when we plan to:

- Undertake any type of processing which is likely to result in a high risk to the rights and freedoms of data subjects;
- Use systematic and extensive profiling based on automated processing with legal or similar significant effects on data subjects;
- Process special category or criminal offence data on a large scale;
- Systematically monitor publicly accessible places on a large scale; or
- Undertake any other processing activity in a country in which the relevant supervisory authority has mandated that the processing activity necessitates a DPIA.

6. DPIA Roles & Format

6.1 All DPIAs must be carried out under the direction of the Middleton Asset Management HSE & Compliance Manager and be signed off by the Managing Director. The Middleton Asset Management DPIA Template must be used unless otherwise agreed.

6.2 The Managing Director may outsource the DPIA to a professional adviser, may delegate responsibility for a specific DPIA to a specific person within Middleton Asset Management or may carry out the DPIA themselves.

6.3 Stakeholders to involve when carrying out a DPIA include:

- [Asset Remarketing Services's DPO and **HSE & Compliance Manager**
- Other Middleton Asset Management stakeholders deemed necessary by the Managing Director
- Data Processors deemed necessary by the Managing Director.
- Professional advisers deemed necessary by the Managing Director. (if any).

7. DPIA Steps to Take

4.1 DPIAs should begin early in the life of a project and be kept under ongoing review. The steps to follow when performing a DPIA are as follows:

4.2 <u>Step 1: Identify the need for a DPIA</u>

A DPIA is required in the circumstances as set out at Section 5 above. When determining whether a DPIA is required you should consult with the DPO

If you determine that a DPIA is not required, you are required to document the decision and your reasons (including the and to keep this on file. This is required to demonstrate we have met our obligations.

7.3 <u>Step 2: Describe the processing</u>

The description should cover the nature, scope, context and purposes of the processing:

- **Nature of the processing** is what you plan to do with the personal data.
- **Scope of the processing** is what the processing covers.
- **Context of the processing** is the wider picture, including internal and external factors which might affect expectations or impact.
- **Purpose of the processing** is the reason why you want to process the personal data.

Detailed factors to include when addressing the nature, scope, context and purposes of processing are set out at Schedule 1 of this procedure.

7.4 Step 3: Consider consultation

The views of data subjects whose personal data will be processed should be sought unless there is a good reason not to.

7.5 Views can be gathered through a variety of means, depending on the context. These include as part of a study, through formal questions to representatives of the data subjects or through surveys sent to data subjects. If the DPIA relates to individuals we have not yet identified, options include a more general public consultation process or targeted research.

7.6 It may not always be appropriate to seek the views of data subjects for reasons of confidentiality or because it might undermine security, be disproportionate or impractical. If the decision is taken not to consult, this should be recorded in the DPIA with an explanation.

7.7 Step 4: Assess necessity and proportionality

The DPIA must address the following questions:

- Do our processing plans achieve the intended purpose of the processing, as recorded at Step 2 above?
- Is the processing activity proportionate to the purpose or can we achieve the purpose another way, without the need to process personal data or as much personal data?

7.8 The DPIA should also include the following:

- The lawful basis for processing
- How ‘function creep’ will be managed, to prevent personal data being used for new purposes
- How data quality will be ensured
- How data minimisation will be ensured
- How privacy information will be provided to data subjects
- How data subject rights will be facilitated
- Measures used to ensure data processor compliance
- Safeguards for any international transfers

7.9 Step 5: Identify and assess risks

The DPIA should consider the potential impact on data subjects, especially harm or damage that might be caused by the processing activity. This includes material, physical and emotional harm. Common risks include (but are not limited to):

- loss of control over the use of personal data;
- loss of confidentiality;
- identity theft or fraud;
- discrimination;
- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- financial loss;
- reputational damage;
- physical harm; and
- other significant economic or social disadvantage

7.10 The DPIA should include an assessment of security risks, including the sources of risk and the potential impact of each type of breach.

7.11 Risks should be assessed objectively, using the risk matrix annexed to the Middleton Asset Management DPIA Template (or an alternative risk scoring methodology approved by the DPO. To assess whether a risk is a high risk, consideration must be given to the likelihood and severity of the possible harm.

7.12 Corporate risks should also be addressed in the DPIA. These include the potential impact of regulatory action (such as a fine) and damage to our reputation.

7.13 Step 6: Identify measures to mitigate the risks

Risks must be identified together with the source of the risk. Measures for reducing the risk should then be considered and recorded. This should include an assessment of whether the measure would eliminate or reduce the risk and whether the measure is appropriate having taken in to account the costs and benefits.

7.14 Options and measures for reducing risks to data subjects include (but are not limited to):

- 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; or
- implementing new systems to help individuals to exercise their rights.

7.15 Step 7: Sign off and record outcomes

The DPIA should record:

- What additional measures will be taken to reduce the risks identified;
- Whether each risk has been eliminated, reduced or accepted;
- The level of remaining or residual risk after taking the additional measures; and
- Whether it is necessary to consult the relevant supervisory authority.

7.16 It is not necessary to eliminate every risk, but if the DPIA identifies a high risk that is not reduced by the measures identified in the DPIA, processing cannot proceed without the agreement of the relevant supervisory authority.

7.17 The sign-off process must include the DPO advice on whether the processing activity is compliant and can proceed. Reasons must be given if the views of data subjects (as required at Step 3) are not taken into account or the processing decision goes against their views.

7.18 Step 8: Integrate outcomes into project plan

The outcome of the DPIA including the measures to be implemented must be integrated back into the project plan for the proposed processing activity (or a change management plan for existing processing activities). Actions points and individuals responsible implementing them should be identified. This is especially important in respect of the measures identified as necessary to reduce the risks recorded in the DPIA. The project management (or change management) process should ensure all action points and measures are implemented.

7.19 Step 9: Keep the DPIA under review

The DPIA must be kept under review and may need to be further developed during a project or repeated during the life of a processing activity, especially is there are material changes to the nature, scope, context or purposes of the processing activity.

8. Implementation & Policy Management

This procedure shall be deemed effective as of 1St June 2022 No part of this procedure shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This procedure will be reviewed by the DPO annually and following any personal data breach.

Schedule 1

Factors to consider in relation to the nature, scope, context and purposes of the processing

Nature of the Processing

- How the data is collected
- How the data is stored
- How the data is used
- Who has access to the data
- Who the data is shared with
- Data processors used
- Retention periods
- Security measures
- Use of novel or new technologies
- Use of novel or new types of processing
- Which screening factors flagged the likelihood of high risk
- Security measures implemented
- Whether we are using any new technologies
- Whether we are using any novel types of processing
- Which screening criteria we flagged as likely high risk.

Scope of the Processing

- Nature of the personal data
- Volume and variety of the personal data
- Sensitivity of the personal data
- Extent and frequency of the processing
- Duration of the processing
- Number of data subjects involved
- Geographical area covered

Context of the Processing

- Source of the data
- Nature of our relationship with the individuals
- Extent to which individuals have control over their data
- 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
- Whether we comply with any UK GDPR and/or EU GDPR codes of conduct or certification schemes (once approved)
- Whether we have considered and complied with relevant codes of practice

Purpose of the Processing

- Our legitimate interests, where relevant
- The intended outcome for data subjects
- The expected benefits for Middleton Asset Management or for society as a whole