DATA PROTECTION IMPACT ASSESSMENT (DPIA) PROCESS

1. Purpose of this document

Entrospective has ethical and legal responsibilities to protect, and to avoid unnecessary interference with, the privacy of individuals.

Occasionally, we might be required to undertake actions that may impact upon the privacy of:

- our own staff
- other members of the public

It is imperative that the possible impact of Entrospectives' actions upon the privacy of these individuals is understood and that any risks to privacy are robustly managed.

The Data Protection Impact Assessment supersedes the previous Privacy Impact Assessment (PIA) in line with GDPR requirements. This document establishes a DPIA process, to ensure that we have consistent and adequate means to achieve this.

The DPIA process set out in this document is based upon the guidance published by the Information Commissioner's Office (www.ico.gov.uk) and has been adapted to comply with GDPR requirements.

2. What is a Data Protection Impact Assessment (DPIA)?

GDPR states that a DPIA is to be undertaken before carrying out types of processing likely to result in high risk to individuals' interests.

In particular, the GDPR specify that organisations must carry out a DPIA if they plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

3. Why do a Data Protection Impact Assessment (DPIA)?

The main purpose of undertaking a DPIA is to ensure that risks to the privacy of individuals, arising from the actions of Entrospective, are identified and robustly managed so as to avoid unnecessary impact upon the individual privacy, dignity and well-being of people whose personal information we process.

Performing a DPIA at an early stage of planning any proposed change avoids problems being discovered at a later stage, when the costs of making significant changes will be much greater.

The DPIA process enables privacy solutions to be considered and implemented at an early stage, and as a fundamental part of key processes. It facilitates the development of processes which allow for a more robust and confident processing of personal information. The process also helps to provide assurance that Entrospective will meet all of its legal requirements in relation to processing personal information and protecting privacy.

By addressing privacy issues in a transparent and structured manner, the DPIA process will increase trust in Entrospective and protect the reputation of the organisation.

3. Key definitions

Privacy is pivotal in ensuring the integrity of an individual; their ability to choose and control what aspects of their person, their information and their behaviour are known to others, and to the protection of this choice and control from unsanctioned intrusion.

For the purpose of Entrospectives' DPIA process, the interpretation of 'privacy' can be defined in relation to the privacy of personal information:

> **Privacy of personal information** refers to the quality of privacy in relation to recorded information that identifies, or could potentially identify, individuals. Changes to the personal information that Entrospective collects, records, analyse, use, share, disclose or dispose of, or to the protections that we place upon these processes, may have an impact upon the privacy of personal information. In most cases, the privacy of personal information will be the main issue of consideration within Entrospectives' DPIA processes;

For the purpose of this document, the term **project**, is used to describe any planned process by which Entrospective changes the ways in which it does things. This includes the development of new policies, processes, methodology, guidance or training.

The **project lead** is the person with responsibility for delivery of a 'project'. This person may delegate responsibility for aspects of that project, including the DPIA process, but retains responsibility for delivery. Wherever this document refers to the 'project lead' it should be read as the person with overall responsibility or the person who has been delegated by that person with regard to performing the task in question.

Personal information refers to information that is related to, and could be used to identify an individual – either on its own, or when combined with other information held by Entrospective or likely to be available to any recipient of information provided by Entrospective. **Personal data** has a specific meaning within the Data Protection Act 2018. Any personal information relating to individuals that is processed by Entrospective is likely to be personal data as defined by that Act.

The term **processing** refers to obtaining, recording or holding information, or carrying out any operation on the data, including; organisation, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, publication, alignment, combination, blocking, erasure or destruction. In effect, anything that Entrospective does with information or data should be considered as 'processing'.

4. Objectives of the DPIA?

The key objectives of a DPIA are:

- the identification of the project's potential privacy impacts and risks;
- appreciation of those impacts from the perspectives of all stakeholders;
- an understanding of the acceptability of the project and its features by the organisations and people that will be affected by it;
- management of information risk, and other risks to privacy
- documentation of the outcomes.

5. Managing a DPIA

The project lead is responsible for conducting a DPIA, however, depending on the nature and type of the project, and the resources available, the task of conducting the DPIA may be delegated, outsourced to an external organisation and/or overseen by a project team. Anyone delegated to undertake a DPIA must be in a position to influence the design and development of the project, and to participate fully in the project design decisions.

The Entrospective Information Governance Group (IGG) will provide advice to the project lead, as required.

The Data Protection Officer (DPO) is responsible for maintaining a DPIA log and will retain copies of all initial screening assessments and reports.

The Senior Information Risk Owner (SIRO) is responsible for assessing the requirement to conduct a DPIA, and signing off reports. The SIRO will be supported by the IGG in performing this role.

The SIRO is responsible for ensuring that the DPIA process has been followed, by checking that the project has either:

- No foreseeable impact upon individual's privacy (e.g. does not involve any significant change to the way in which personal information is processed);
- An initial screening assessment, with a decision from IGG that a DPIA is not required; or
- A DPIA report, which has been reviewed and assessed by IGG as adequate to comply with the requirements of this process.

6. Managing privacy risk

The ICO must be informed if the organisation identifies a high risk for which they are unable to take measures to reduce.

7. Data Protection Impact Assessment (DPIA) process

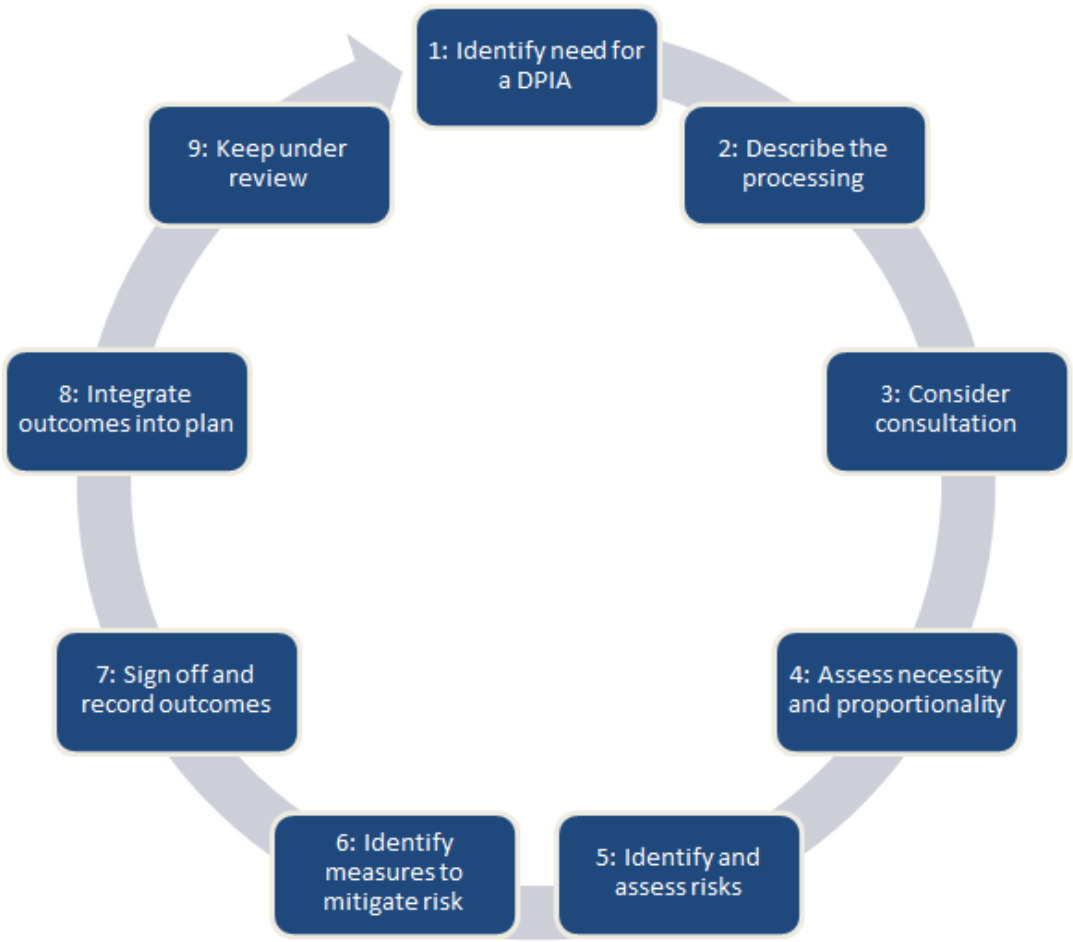

Figure: Information Commissioners Office – DPIA lifecycle

Initial preparation

Some work is required before a DPIA can be undertaken for any project:

- The purpose and objectives of the project must be sufficiently defined in order to be able to meaningfully articulate the proposed change to Entrospectives' way of working,
- An initial consideration must be made as to whether the proposed change is likely to have an impact upon personal privacy, for example by;
    - Introducing new processes for observing, monitoring or tracking the movements or actions of individuals,
    - Changing the way in which we collect, obtain or record personal information,
    - Combining items of personal information in a new way,
    - Combining items of anonymised (or pseudonymised) information in such a way as raises the risk that individuals may become identifiable,
    - Changing the way in which we store, analyse, manage, or dispose of personal information,
    - Reducing the level of protection provided to personal information,
    - Disclosing, sharing or publishing personal information in a new way,
    - Disclosing, sharing or publishing anonymised (or pseudonymised) information in such a way as raises the risk that individuals may become identifiable when that information is combined with information available to potential recipients of the information,
    - Introducing new technologies or information systems for collecting or processing personal information.

DPIA's should follow the following five phases:

<u>Phase 1: Preliminary phase</u>

The purpose of this stage is to develop an overall plan for how the DPIA will be conducted, and to begin to develop the background material for consultation.

To achieve this, the following tasks are recommended:

- Identify a lead and assign the task of carrying out the DPIA

- Identify relevant stakeholders that should be consulted as part of the DPIA, this may include; internal stakeholders (other Entrospective staff) or strategic partners, customers
- Obtain feedback from the Information Governance Group and establish the key privacy issues that require consideration.
- Prepare a background paper, to be used in the consultation

The purpose of the background paper is to provide consultees with the information required to understand the proposals, so as to facilitate their feedback. It should contain:

- A statement of the project's objectives, scope and rationale (i.e. what we are planning to do and why).
- An explanation of how this differs from what currently happens.
- A description of how it is proposed to implement the change in practice.
- An initial assessment of the key privacy issues and risks.
- A brief description of any options that have been identified, including both those that have already been dismissed (and why) and those that remain under consideration.
- Any other information or supporting documents required to understand the proposals.

Phase 2: Preparation phase

The purpose of this phase is to make the arrangements needed to enable the consultation and analysis to run smoothly.

To achieve this, the following tasks are recommended:

- Decide how various stakeholders will be consulted
- Decide how consultees will feed back to Entrospective (e.g. by answering a questionnaire, or through workshops) and make appropriate plans for these.
- Prepare a consultation plan and send it to the Data Protection Officer.

The consultation plan will be a short document setting out who will be consulted on the proposals, and how this will be done. The background document (prepared as part of phase 1) and any other relevant documents (such as questionnaires or workshop presentations) should be provided.

The consultation plan will be reviewed and must be approved by the Data Protection Officer

Phase 3: Consultation and analysis phase

This phase involves the actual consultation with stakeholders, and the collection and analysis of feedback.

This consultation may be a stand-alone process, or part of a pilot exercise or broader consultation process (i.e. a consultation that looks at other issues in addition to privacy).

Feedback on privacy issues should be collected and reviewed so as to identify any additional privacy risks or issues that had not previously been identified and to review and re-assess the existing privacy risks and issues.

Phase 4: Documentation phase

This phase involves the preparation of a Data Protection Impact Assessment and report:

Phase 5: Review and audit phase

The DPIA report must be submitted to the Data Protection Officer.

Any risks and mitigations must be transferred into the appropriate project and corporate risk registers.

The Senior Information Risk Owner (SIRO) may recommend that review of any privacy safeguards and information risk management/mitigations may be incorporated into Entrospectives' internal audit processes.

The SIRO will sign off the DPIA Report, or stipulate any further actions required to adequately complete the DPIA.

For some projects, several DPIA's may be conducted during the project lifecycle.