PRIVACY IMPACT ASSESSMENTS POLICY AND PROCEDURE

As a firm handling personal data, we are required by the General Data Protection Regulation (GDPR) to implement a wide range of measures to reduce the risk of any breach. One of the most significant actions we must take is to produce a Privacy Impact Assessment ('PIA'). A PIA should be created when our firm is looking to start a new project or is deciding upon an action which may have the propensity to affect an individual's privacy rights.

A PIA is an assessment to identify and minimise non-compliance risks. Specifically, our firm must ensure that a PIA has been run on any "high risk" processing activity before it is commenced (this is measured by reference to the risk of infringing a natural person's rights and freedoms). Our firm will ensure that all PIAs we produce include:

- A description: of the processing activities and their purpose;
- An assessment of the need for and proportionality of the processing, the risks arising, and measures adopted to mitigate those risk, in particular safeguards and security measures to protect personal data and comply with the GDPR.

A supervisory authority must be consulted before any data processing commences if a PIA identifies a high unmitigated risk. If it is necessary in the circumstance, we will seek the views of affected data subjects "or their representatives" in conducting a PIA, if appropriate.

Our firm follow a routine procedure in the production of any PIA; our procedure takes place as follows:

1. Identifying the need for the PIA

The need for a PIA can be identified as part of our usual project management process,

2. Describing the information flows

Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information.

3. Identifying the privacy and related risks

Some will be risks to individuals – for example – damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy,

Some risks will be to our firm, for example damage to reputation, or the financial costs or a data breach. Legal

compliance risks include the GDPR, the Data Protection Act 2018 & the Privacy & Electronic Communications

Act,

4. Identifying and evaluating privacy solutions

We will explain how we could address each risk concerned. Some might be eliminated altogether, whilst others may only be reduced. Most projects will require use to accept some level of risk and will have some impact on privacy.

We will evaluate the likely costs and benefits of each approach. We will think about the available resources, and the need to deliver a project which is still effective.

5. Signing off and recording the PIA outcomes.

Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of our wider project approval.

Our PIA report will summarise the process, and the steps taken to reduce the risks to privacy. It will also record the decisions taken to eliminate, mitigate, or accept the identified risks.

By publishing a PIA report, our firm will be able to improve its transparency and accountability and will let data subjects learn more about how our project may affect them.

6. Integrating the PIA outcomes back into the project plan

Our PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

Our PIA might generate actions which will continue after the assessment has finished, and so in accordance, we will revisit the PIA to ensure that these are monitored.

We will also record what we learn from the PIA for the purpose of future projects.