DATA PROTECTION POLICY STATEMENT

Policy, scope and objectives

- The Board of Directors and management of Kinetic Solutions are committed to compliance with relevant Data Protection laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information Kinetic Solutions collects.

Scope

- The scope includes data collection, storage, processing, and onward transfer, taking into account organisational structure, management responsibility, jurisdiction and geography.

Objectives of this Data Protection Policy

- Kinetic Solutions's objectives for this Policy Statement are: that it should enable Kinetic Solutions to define and meet requirements for the management of personal information; that it should support organisational objectives and obligations; that it should impose controls in line with Kinetic Solutions's acceptable level of risk; that it should ensure that Kinetic Solutions meets applicable statutory, regulatory, contractual, and professional duties; and that it should protect the interests of individuals and other key stakeholders.

- Kinetic Solutions is committed to complying with data protection legislation and general good practice including:
- processing personal information only where this is strictly necessary for legitimate organisational purposes;
- collecting only the minimum personal information required for these purposes and not processing excessive personal information;
- providing clear information to individuals about how their personal information will be used and by whom;
- only processing relevant and adequate personal information;
- processing personal information fairly and lawfully;
- maintaining an inventory of the categories of personal information processed by Kinetic Solutions;
- keeping personal information accurate and, where necessary, up to date;
- retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
- respecting individuals' rights in relation to their personal information, including their right of subject access;
- keeping all personal information secure;
- only transferring personal information outside the applicable jurisdiction in circumstances where it can be adequately protected;
- the application of the various exemptions allowable by data protection legislation;
- developing and implementing processes to enable the policy to be implemented;
- where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of Kinetic Solutions's Data protection processes; and
- the identification of workers with specific responsibility and accountability for the protection of personal data.

Definitions used by the organisation

- **Personal data** – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Special categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- **Data controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

- **Data subject** – any living individual who is the subject of personal data held by an organisation.

- **Processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Profiling –** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

- **Personal data breach –** a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the applicable supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

- **Data subject consent -** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

- **Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

- **Filing system** – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Responsibilities

- Top Management and all those in managerial or supervisory roles throughout Kinetic Solutions are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.
- Compliance with data protection legislation is the responsibility of all members of Kinetic Solutions who process personal information.
- Kinetic Solutions's Data Security team are to provide training and awareness requirements in relation to specific roles and to members of Kinetic Solutions generally.
- Members of Kinetic Solutions are responsible for ensuring that any personal data supplied by them, and that is about them, to Kinetic Solutions is accurate and up-to-date.

The Kinetic Solutions affiliate businesses, hereafter referred to as affiliates, represent the many various business units that comprise the group, are to, where applicable: -

Notification

- notify the appropriate Supervisory Authority of their data controller designation and of the information about data subjects they process. Kinetic Solutions has identified the employee personal data that it processes within the Digital Workplace set of systems and this is contained in the Kinetic Solutions Data Inventory Register.

- compile and maintain a Data Inventory Register of the personal data that they process.
- apply the defined Security Incident Handling Procedures as prescribed by the Kinetic Solutions Director Data Security, upon data breach detection.
- retain notification details of the applicable Supervisory Authority.
- appoint a suitable person as the Data Protection Owner.
- The applicable affiliate Data Protection Owner is responsible, each year, for reviewing the details of notification, in the light of any changes to their business' activities (as determined by changes to their Data Inventory Register and the management review) and to any additional requirements identified by means of data protection impact assessments.

Risk Assessment

- Kinetic Solutions has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing undertaken by other organisations on behalf of Kinetic Solutions. Kinetic Solutions and affiliates shall manage risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

- Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, Kinetic Solutions and affiliates shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Data protection principles

1) All processing of personal data must be completed in accordance with the following data protection principles. Kinetic Solutions's policies and procedures are designed to ensure compliance with them.

a) Personal data must be processed lawfully, fairly and transparently.

i) Kinetic Solutions's Fair Processing Procedure for the Digital Workplace set of systems is set out in its Fair Processing Procedure document.
ii) The specific information that must be provided to the data subject must as a minimum include:
- the identity and the contact details of the controller and, if any, of the controller's representative;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

b) Personal data can only be collected for specified, explicit and legitimate purposes.
i) Data obtained for specified purposes must not be used for a purpose that differs from those formally notified.

c) Personal data must be adequate, relevant and limited to what is necessary for processing.
i) Information, which is not strictly necessary for the purpose for which it is obtained, is not to be collected.
ii) All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must follow these principles.

d) Personal data must be accurate and kept up to date.
i) Data that is kept for an extended time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

ii) The Head of HR for each Kinetic Solutions affiliate businesses are responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
iii) It is also the responsibility of individuals to ensure that data held by Kinetic Solutions is accurate and up-to-date.
iv) Employees/Staff should notify the applicable Kinetic Solutions affiliate business of any changes in circumstance to enable personal records to be updated accordingly. These instructions for updating records are to be maintained by the applicable business.
v) On at least an annual basis, the Data Security Director will review all the personal data maintained by Kinetic Solutions digital workplace, by reference to the Data Inventory Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed.

e) Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
i) Within the Digital Workplace systems, where personal data is retained beyond the processing date, it will be treated [minimised/encrypted/pseudonymised] as applicable in order to protect the identity of the data subject in the event of a data breach.

f) Personal data must be processed in a manner that ensures its security.
i) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
ii) These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

2) Kinetic Solutions's compliance with this principle is aligned with its Information Security Management framework ISO/IEC 27001 series and the Information Security policy.

a) Personal data collected will be the minimal possible to achieve the objective.
b) Personal data shall not be transferred to a country or territory outside the applicable territory (e.g. European Union) unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.
c) The transfer of personal data outside of the territory (e.g. EU) may require additional specified safeguards be applied.

i) Safeguards

- An assessment of the adequacy by the data controller taking into account the following factors:
- ♦ the nature of the information being transferred;
- ♦ the country or territory of the origin, and final destination, of the information;
- ♦ how the information will be used and for how long;
- ♦ the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and

ii) Model contract clauses

- Kinetic Solutions may adopt approved model contract clauses for the transfer of data outside of the EU.
- ♦ If Kinetic Solutions adopts the model contract clauses approved by the relevant Supervisory Authority, there is an automatic recognition of adequacy.

iii) Accountability

- Kinetic Solutions and affiliate businesses are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Processing Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

3) Security of data

a) All Employees/Staff are responsible for ensuring that any personal data which Kinetic Solutions and/or affiliates hold and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Kinetic Solutions or the Kinetic Solutions affiliate businesses to receive that information and has entered into a confidentiality agreement.

b) All personal data should be accessible only to those who need to use it, and access may only be granted in line with applicable Access Control Policy.

4) Retention and disposal of data

a) Personal data may not be retained for longer than it is required. Once a member of staff has left Kinetic Solutions or affiliate businesses, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. Applicable data retention and data disposal procedures are to be applied.

5) Disposal of records

a) Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with appropriate secure disposal best practices

This policy was approved by the Data Security Steering committee on behalf of the Kinetic Solutions on 21st May 2018 and is issued on a version controlled basis under the signature of the Director Data Security.