Access Intelligence Data Protection Policy

1.0 Policy Objectives

- To ensure that Access Intelligence shall at all times remain legally compliant with the requirements of the UK and EU General Data Protection Regulations ("GDPR"), United Kingdom Data Protection Act 2018 (the "Act"), any other applicable laws, rules or regulations concerning data privacy which may be amended or introduced from time to time, any associated guidance by supervisory authorities including the Information Commissioner and all contractual obligations with its customers in connection with the collection, processing, storing and removal of all personal data.

- To ensure that Access Intelligence is properly undertaking the activities and implementing the controls required by GDPR, and that full and accurate data protection records are created and maintained to demonstrate compliance.

2.0 Data Protection Definitions

- **Personal Data** means 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 specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Special Categories of Personal Data** refers to five sub-sets of personal data, being
    - Information on an individual's racial or ethnic origins
    - Information on an individual's health
    - Information on an individual's sex life or sexual orientation
    - Information on an individual's political, religious or philosophical opinions or beliefs
    - Information on any trade union membership held by the individual

- **Data Controller** means 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 Processor** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

- **Processing** means 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.

3.0 Policy Scope

Access Intelligence Data Protection Policy shall include the following:

- All Personal Data acquired, received, processed, stored, amended, disclosed and erased by Access Intelligence. This shall include Access Intelligence data, as well as Personal Data owned by an external organisation, and entrusted to Access Intelligence under a contract which specifically communicates data protection requirements.

- All Access Intelligence activities related to the Processing of Personal Data, either as Data Controller, or as Data Processor acting under the lawful instructions of a third party.

- All employees, contractors, external Data Processors, and any other organisation or individual associated with the processing of personal data.

4.0 Policy Statements

Access Intelligence shall:

- Ensure that personal data is processed with due attention to the 7 key principles as detailed within Art 5 of the GDPR:
  - lawfulness, fairness and transparency
  - purpose limitation
  - data minimisation
  - accuracy
  - storage limitation

  - integrity and confidentiality
  - accountability

- Keep all personal information (including employee information) secure, regardless of its format or category, or the process or activities which use it, so as to prevent accidental or unauthorised loss, theft or breach.

- Maintain a full and accurate inventory of all personal data which is under its control.

- Provide regular data protection training to all personnel and third parties who are engaged in delivering any activity which involves the processing of personal data.

- Provide specific data protection training for those employees with specific GDPR responsibilities, including Senior Management and the organisation's Data Protection Officer.

- Ensure that all data processing activities are subject to full and accurate Privacy Impact Assessments, and promptly acting to remediate the findings of such assessments.

- Ensure that personal data processing activities are afforded suitable protection by conducting risk assessments of the physical, technical and personnel elements of the activity (for example as part of the organisation's Information Security Management System).

- Validate that personal data is afforded the protection which is documented with the Company's Acceptable Use Policy and Access Control Policy.

- Only process personal data for legitimate business purposes, and in accordance with the Privacy Impact Assessment which has been prepared to cover that purpose.

- Ensure that all personal information is properly returned or effectively deleted or destroyed when it is no longer required, in accordance with supporting Privacy Impact Assessments.

- Implement a suitable mechanism and supporting records for recording data subject consent for the processing of their personal data, and using these records as a reference point when deciding how personal data is to be processed.

- Clearly communicate, when appropriate, to data subjects how their personal data is to be processed, where it is to be transferred to (if applicable), and their rights as data subjects.

- Maintain clear and concise Privacy Notices, and related information for data subjects.

- Ensure that third parties involved in personal data processing activities understand this Policy and related GDPR documentation, and can evidence their own levels of GDPR compliance.

- Ensure that effective processes, technical controls and competent resources are in place to undertake tasks promptly and diligently related to delivering the rights of data subjects.

- Implement effective processes and monitoring controls to provide protection for personal data, and to detect any loss, theft or data breaches.

- Authorise any off-site or off-shore processing of personal data before being approved, and updating and reissuing the corresponding Privacy Impact Assessment.

- Undertake to promptly report any actual or suspected data breaches internally (see ISDL04), and to the Supervisory Authority within the required timeframes, and to communicate the breach to affected data subjects.

- Willingly and fully co-operate with any investigations into data breaches as may be required by the Supervisory Authority or similar legislative function.

5.0 Responsibilities

- Senior Management shall be responsible for:
  - ensuring that Access Intelligence remains fully compliant with GDPR
  - providing the personnel, resources, infrastructure and training required

  - ensuring that mandatory data protection training is delivered on a regular basis
  - nominating a suitably qualified and experienced Data Protection Officer
  - maintaining visibility of issues identified within Privacy Impact Assessments

- Access Intelligence Data Protection Officer shall:
  - maintain professional awareness of GDPR and its requirements
  - have visibility of and sign-off to the organisation's Privacy Impact Assessments
  - have the seniority to escalate and report GDPR compliance issues to the Board
  - advise Senior Management of any changes to data protection legislation
  - act as a reference point to the organisation's management and staff
  - maintain communications with the Supervisory Authority
  - co-ordinate breach reporting activities, and any follow-up investigative actions

- All employees, contractors, and third parties, as defined within the Scope of this Policy, shall:
  - understand and fully comply with this Data Protection Policy
  - maintain an understanding of GDPR, and their role in ensuring full compliance
  - only undertake activities in accordance with published Privacy Impact Assessments
  - promptly identify and report any data losses or breaches of which they become aware
  - undertake Privacy Impact Assessments, if identified as an activity owner
  - assist in understanding and resolving issues arising from Privacy Impact Assessments
  - attend data protection training which has been provided by Access Intelligence

All individuals specified within the Policy Scope of this Data Protection Policy (see section 3.0) shall have individual responsibility for complying with every aspect of this policy. The requirement to comply with Access Intelligence policies is included within the Terms and Conditions of Employment and is noted within each individual user's job description. Any failure to adhere to the requirements of this policy shall result in disciplinary action being taken.

6.0 Document Version Control

This policy needs to be reviewed annually as an absolute minimum, or if required changes are identified to address one or more of the following:

- An identified shortcoming in the effectiveness of this policy, for example because of a reported information security incident, formal review or audit finding.
- A change in business activities (e.g. mergers and acquisitions) which will or could possibly affect the current operation of the Access Intelligence Information Security Management System, and the relevance of this document.
- A change in the way in which Access Intelligence manages or operates its information assets and/or their supporting assets, which may affect the validity of this document.

The current version of this policy, together with its previous versions, shall be recorded below.

Version History

Revision	Author	Date	Reason for issue
1.0	David Roud	31/10/2018	Initial version, to enable Access Intelligence to achieve ISO 27001:2013 accreditation
2.0	Andy Olliver / Ato Abraham	26/05/2020	Change of leadership team; ISO 27001:2013 certification needs to be renewed.
3.0	Adam Palmer	14/10/2020	Reviewed and published; ISO 27001:2013 certificate has been renewed.
4.0	Adam Palmer	15/01/2021	Added reference to UK GDPR

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		14/10/2020
Mark Fautley	**Chief Financial Officer**		**26/02/2021**