MEMORANDUM TO BOARD OF DIRECTORS

The Board of Directors

Audax UK

The EU General Data Protection Regulation (GDPR) will become effective on 25 May 2018. The GDPR will bring considerable changes to data protection law in the UK and across the European Economic Area (EEA) more widely, and will include significantly greater fines for breaches of up to €20 million or 4% of total worldwide annual group turnover. This memorandum summarises the need for action, for compliance with the GDPR.

ISSUES CONCERNING DATA PROTECTION UNDER THE GDPR

An immense volume of personal data continues to proliferate and flow daily around the UK and between the UK and other countries in the world. Some of this personal data needs to be accessible beyond the UK's borders.

Personal data is defined broadly and comprises data relating to any living individual who can be identified from that data. Personal data and includes:

- Names.
- Addresses.
- Social security numbers.
- Telephone numbers.
- Health information of, for example, customers and employees.

There are many potential ramifications of failure to comply with the GDPR, including:

- Prosecution of or regulatory enforcement action.
- Adverse publicity, potentially leading to reputational damage and lost trust.
- Missed opportunities and wasted resources.
- A variety of sanctions in different jurisdictions.
- Increased scrutiny from data protection authorities whose confidence and powers are increasing substantially under the GDPR.
- Civil liability or punitive damages for employment-related breaches.
- Criminal liability for directors and senior managers resulting in imprisonment and substantial penalties.
- Critical system delays and failures.
- Orders issued by the Information Commissioner's Office in the UK, and data protection authorities in other key markets, that seriously impact business. Investigative powers include a power to carry out audits, as well as to require

information to be provided, and to obtain access to premises.

- Business continuity issues.
- Becoming embroiled in litigation and its attendant time, effort and expense.

The aim of the GDPR is to ensure good information handling practice. For example, identity theft, stolen credit cards and failure to comply with privacy policies may result in fraud, theft and deception. Abuse of health data, financial data or children's data can have an adverse impact on insurance, credit, jobs or parental control.

An individual has a fundamental right in the UK and across the EEA to have their personal data protected and their personal data may only be processed (that is, obtained, recorded, held, used or disclosed) under certain circumstances. This has a wide impact on Enterprise business.

THE PROGRAMME

A well-constructed and comprehensive organisation-wide programme (Programme) can provide a solution to these various competing interests and represents an effective risk management tool. It is essential for compliance and to inform organisers, delegates, members, regulators and the courts of our commitment to data protection.

Board's duty to know about and oversee the Programme

The Board has a duty to know about the content and operation of the Programme, and to oversee its implementation and effectiveness appropriately. The GDPR's new accountability principle requires data controllers to be able to demonstrate compliance with the GDPR by showing the supervisory authority (the Information Commissioner's Office in the UK) and individuals how the data controller complies, on an ongoing basis, through evidence of:

- Internal policies and processes that comply with the GDPR's requirements.
- The implementation of the policies and processes into the organisation's activities.
- Effective internal compliance measures.
- External controls.

IMPLEMENTING THE PROGRAMME

Organisational culture and chain of command

We must display an organisational culture that encourages compliance and provides organisers and delegates with the clear guidance and tools they need to achieve it. It also requires that they behave appropriately or are held accountable by the Board.

Standards and procedures

The privacy policy is a key element of the Programme. Amendments are likely to be needed to the existing policy. The policy needs to be accessible at every relevant personal data collection point, for example:

- Website
- Event Entry forms.
- Membership applications and renewals.

In particular, we will need to carefully review existing procedures in circumstances where need to obtain an individual's consent as a legal basis for processing personal data. For example, we will need to ensure that any consent obtained indicates affirmative agreement from the individual (opt in) (for example, ticking a blank box). Mere acquiescence (for example, failing to un-tick a pre-ticked box) does not constitute valid consent under the GDPR. Furthermore, we must demonstrate that this explicit consent has been obtained, ensure that an individual can easily withdraw their consent at any time.

We must also be in a position at all times to respond quickly to any data subject's request (such as for a copy of all of the personal data held or to erase all such personal data). This is likely to require substantial modifications to the Enterprise's technological infrastructure and its organisational processes.

Under the GDPR, we will also be required to implement "privacy by design" (for example, when creating the new website) and "privacy by default" (for example, data minimisation). We must also carry out "privacy impact assessments" before carrying any processing that uses new technologies (and taking into account the nature, scope, context and purposes of the processing) that is likely to result in a high risk to data subjects, takes place.

The GDPR also requires businesses to notify the supervisory authority of all data breaches without undue delay and where feasible within 72 hours. We will therefore need to look carefully at its data breach response plans and procedures.

The above represents only a short synopsis of the requirements under the GDPR. There are many more that are not included in this note for the sake of brevity.

Adequate resources

Financial, technological and human resources should be sufficient to reasonably prevent and detect non-compliance and promote compliance with the GDPR.

Training and enforcement

Effective compliance briefings are required for personnel at all levels, including

directors, organisers and delegates.

Serious misconduct should be addressed with appropriate disciplinary action, regardless of seniority.

Regular reviews

From time to time, the Programme should be reviewed and updated in the light of new laws and business activities and changes to cross-border data flows.