ADDLESHAW GODDARD PROCUREMENT POLICY AND SUPPLIER CODE OF CONDUCT

INTRODUCTION

Addleshaw Goddard (AG) is a London headquartered, international, full-service law firm that consistently delivers high-quality outcomes for our clients globally. We have been advising clients for 250 years, and today we support over 5000 of the world's most respected organisations. We help them in over 50 areas of business law, across more than 100 countries.

AG is committed to conducting our business in a responsible, sustainable and ethical manner, meeting regulatory requirements in place wherever we operate. AG expects the same level of commitment from its suppliers, who play a vital role in the delivery of our services and the achievement of our strategic goals.

This Procurement Policy and Supplier Code of Conduct (the Code) sets out the minimum standards that AG requires from its suppliers. The Code applies to all suppliers who provide goods or services to any AG group entity. This Code supplements (and does not replace) any contract agreed between AG and the relevant supplier.

You can find further information on our commitment to responsible and sustainable business practices, and what suppliers can expect from AG, in our Responsible Procurement Policy which is available on our website.

ADDLESHAW GODDARD

MORE IMAGINATION MORE IMPACT

THE LAWYER Awards 2024 LAW FIRM OF THE YEAR

OVERVIEW OF THE CODE

This Code is split into several sections. We summarise and provide links to these sections below.

A. GENERAL REQUIREMENTS 	This section explains the applicability of this Code and sets out some general requirements.
B. PAYMENT, INVOICING AND EXPENSES 	This section explains AG's approach to approvals, invoicing, payment and expenses.
C. ETHICAL PEOPLE PRACTICES 	AG respects the human rights and dignity of all people. This section details AG's requirements related to ethical people practices, including modern slavery and labour practices.
D. ENVIRONMENTAL RESPONSIBILITY 	AG recognises the importance of protecting the environment and reducing its environmental impact. This section details AG's requirements related to environmental practices.
E. FINANCIAL CRIME 	AG conducts its business lawfully and with integrity, transparency and accountability. This section details AG's requirements relating to financial crime.
F. CONFIDENTIALITY AND DATA PROTECTION 	The confidentiality and security of AG's and its clients' information and data is paramount. This section details AG's requirements relating to confidentiality and data protection.
G. RESPONSIBLE USE OF AI 	AG supports the use of AI, in an ethical, secure and compliant manner, to deliver tangible benefits to clients. This section details AG's requirements relating to the use of AI.
H. INFORMATION SECURITY MINIMUM REQUIREMENTS 	This section details AG's Information Security Minimum Requirements, to which all Suppliers shall adhere.
I. AG SITE HEALTH AND SAFETY RULES 	This section details AG's health and safety requirements where Suppliers are working at AG sites. If you do not have personnel working at AG sites, this section will not apply.
J. DEFINITIONS USED IN THIS DOCUMENT 	This section explains the meaning of some key terms used in this Code.

A. GENERAL REQUIREMENTS

1 The Supplier shall comply with this Code and ensure that its Representatives are aware of it and comply with it.

2 The Supplier shall comply with all applicable Laws, including those related to issues addressed in this Code. This includes compliance with all applicable competition Laws, including those relating to teaming and information sharing with competitors, price fixing and rigging bids.

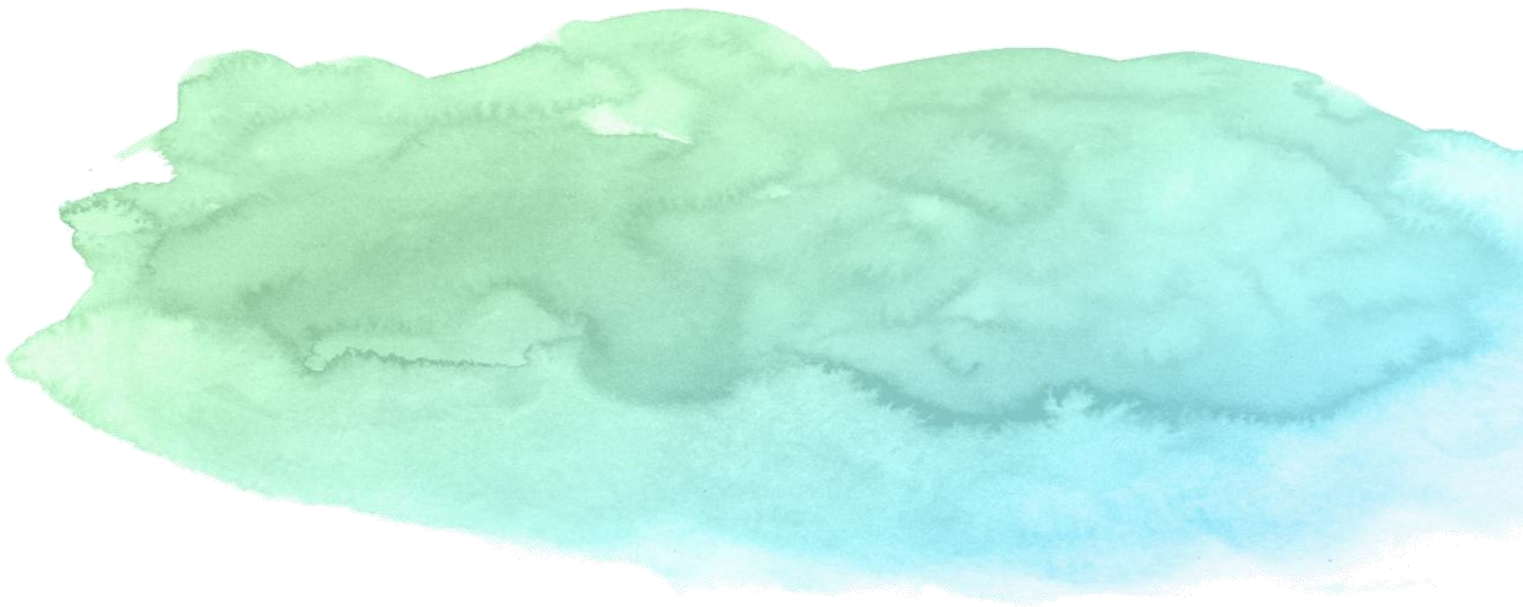
3 AG's Standard Terms and Conditions for the Purchase of Goods and Services, which include Data Protection Terms, can be found here. These terms will govern the relationship between AG and the Supplier, unless a specific contract has been agreed by AG and the Supplier (in which case that specific contract will apply).

4 If there is a conflict between any applicable Law, the provisions of a contract between the Supplier and AG, and the provisions of this Code, the Supplier shall meet the most stringent standard.

5 AG reviews this code periodically (and at least annually) and may update it. If it does so, AG will make the updated code available on its website. Where required by Law, AG may conduct audits and inspections to verify the Supplier's compliance with this Code, which the Supplier shall facilitate. In doing so, where allowed by Law, AG will provide reasonable notice and minimise the scope of any such inspection or audit.

6 If requested by AG, the Supplier shall provide evidence demonstrating its compliance with this Code, or with specific requirements within it. The Supplier shall report any actual or suspected breaches of this Code to AG as soon as possible after becoming aware.

7 The Supplier shall carry out appropriate due diligence on its Representatives, including by assessing their ability to meet the requirements and principles that are covered in this Code.



B. PAYMENT, INVOICING AND EXPENSES

1 While the Supplier will interact with a variety of AG personnel, only certain individuals are authorised to commit AG to expenditure. Please contact the Central Procurement Team (centralprocurement@addleshawgoddard.com) for confirmation of such individuals. Any Supplier acting on requests from AG personnel who have not been properly authorised, or without a valid Purchase Order (PO) number, may not be paid for those goods or services, and therefore does so at its own risk.

2 The Supplier shall obtain a PO number prior to supplying any goods or services to AG, as any invoice without a valid PO number will not be digitally recognised by AG's Purchase to Pay system and cannot be approved for payment. PO numbers are provided in a PO Report, issued to the Supplier by email.

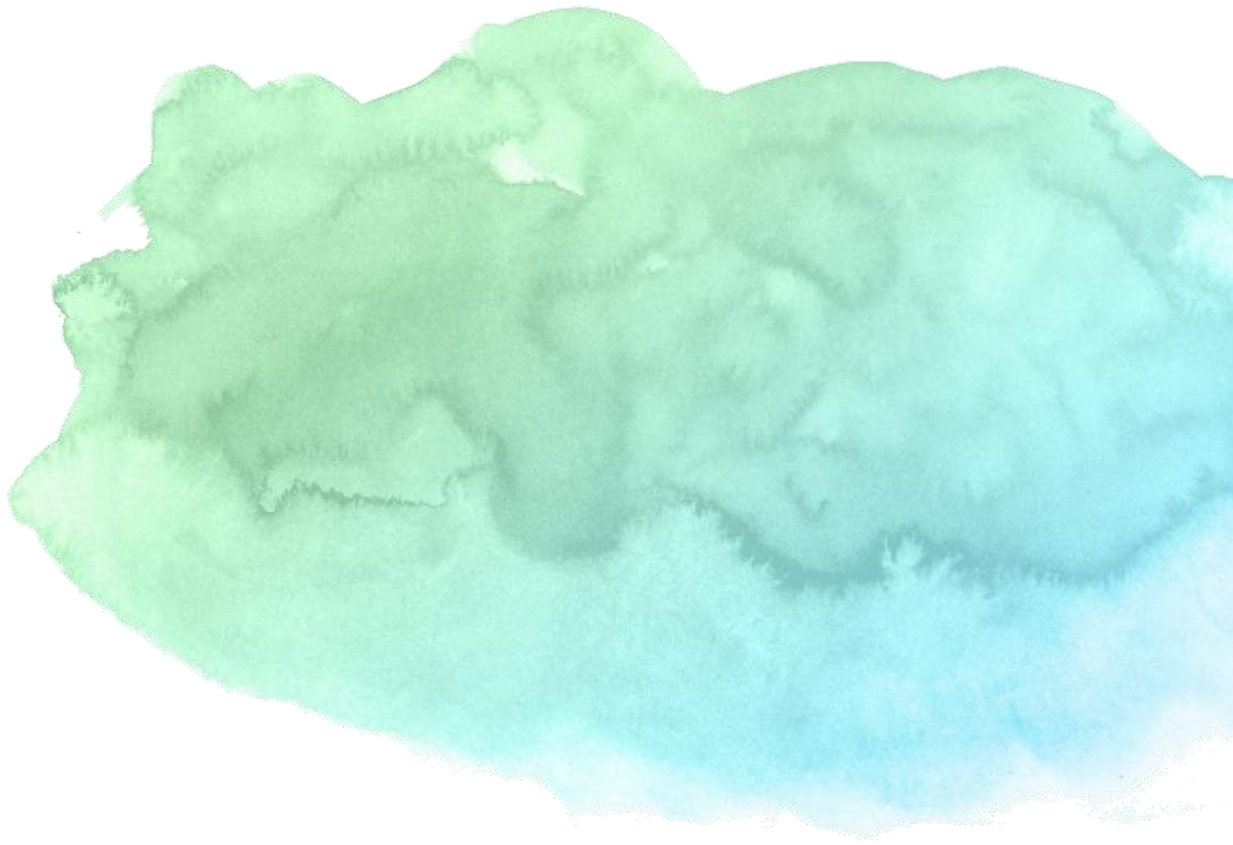
3 The Supplier is responsible for submitting accurate and valid invoices, which quote the correct PO, to AG via the Chrome River Purchase to Pay system at the following email address: *addleshawgoddard.com-vision@invoice.eu1.chromeriver.com*.

4 Statements and queries shall be sent to the following email address: *accountspayable@addleshawgoddard.com*.

5 Invoices shall not be backdated or password protected, and shall be addressed to the correct AG entity, as detailed on the PO Report.

6 All invoices will be paid in line with agreed invoice and payment terms. If none are agreed, our default is 30 days following the date of receipt of a valid, undisputed and properly due invoice. Any incorrectly submitted invoices may be returned to the Supplier for correction and resubmission.

7 Where the Supplier is entitled to recharge expenses under its contract with AG, it shall follow the AG expenses policy, and supply valid receipts to evidence these expenses.



C. ETHICAL PEOPLE PRACTICES

1 Human Rights

The Supplier shall respect the human rights of their employees, other personnel and local communities, and comply with all relevant Law related to human rights.

2 Modern Slavery

2.1 AG is determined to identify and eradicate any modern slavery in its business and supply chain, and to ensuring transparency in our approach to this, consistent with our disclosure obligations under the Modern Slavery Act 2015 (**MSA 15**). **Modern slavery** in this document means any activity which involves the exploitation of a person or deprivation of their liberty by another, in order to exploit them for personal or commercial gain, such as slavery, servitude, forced and compulsory labour and human trafficking, and any similar or related activity prohibited by Law.

2.2 The Supplier shall take all reasonable steps to ensure that modern slavery is not taking place in its business or supply chain, including by (a) putting in place, maintaining and enforcing appropriate policies and procedures to identify risks and actual instances of modern slavery in its business and supply chain, (b) implementing appropriate due diligence, risk analysis and mitigation measures, (c) providing appropriate training to personnel, including on MSA 15.

2.3 The Supplier shall document the steps taken to tackle modern slavery (as described above), and if AG requests, report to AG on the steps taken, risks identified and how they have been mitigated, and consequences for third parties of non-compliance. The Supplier shall promptly notify AG upon becoming aware of any actual or suspected instance of modern slavery.

2.4 The Supplier shall ensure that it, and all persons engaged by it or its supply chain to provide goods or services to AG in any part of the world, at all times comply with the provisions of the MSA 15, all Laws, made under or relating to it, and all equivalent Laws applicable across the world. The Supplier shall ensure that all relevant personnel do not engage in any activity, practice or conduct that would constitute an offence under the MSA 15 if carried out in the UK, and comply with any other policy relating to modern slavery reasonably required by AG.

3 Labour practices

3.1 AG is committed to a policy of equal opportunity and inclusiveness in our employment and working practices. AG expects its Suppliers to be committed to the same principles, therefore the Supplier shall not discriminate against any job applicant, employee or other individual, or treat them less fairly, because of gender identity, marital status, race (including nationality or ethnic origin), disability, health condition, religion, age, sexual orientation, union membership, political affiliation, being a member of a protected class under international human rights law or any other conditions not justified in Law or relevant to the performance of the job. The Supplier shall have policies in place to promote diversity and inclusion within their own organisations and supply chain, including workplace standards such as the UK Government's Disability Confident scheme (as may be updated or replaced from time to time) or equivalent.

3.2 The Supplier shall ensure that, within its own organisations and throughout its supply chain:

(a) child labour is not used and relevant Law relating to minimum working age legislation is strictly complied with;

(b) forced labour, in any form, is not used and workers are not required to lodge papers or deposits on starting work;

(c) physical abuse, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation or inhumane practice are prohibited and do not take place, whether as part of a disciplinary process or otherwise;

(d) all terms and conditions of employment are made clear to the workforce in a manner which is easily understood;

(e) employee wages comply with relevant minimum wage Laws, and minimum wages or the prevailing industry wage (whichever is higher) are paid to workers as a minimum;

(f) employees are provided with all benefits under Law and no non-statutory deductions are made from wages;

(g) the employment terms of young workers adhere to International Labour Organisation Standards, the OECD Guidelines for Multinational Enterprises and Law;

(h) Laws relating to working time and the maximum hours of work permitted to be undertaken by any employee in any period of time are complied with, with any overtime being on a voluntary basis and at manageable levels;

(i) all employees, local or migrant, have the right and ability to leave employment when they choose;

(j) obligations under Law arising from regular employment are not avoided through the use of labour-only contracting, sub-contracting, or home-working arrangements, or through apprenticeship schemes where there is no real intent to impart skills or provide regular employment, or through the excessive use of fixed-term contracts of employment;

(k) clear, fair and uniformly applied disciplinary practices and grievance procedures are implemented;

(l) the rights of workers to form or join trade unions, which are free to meet without hindrance and to bargain collectively, are recognised, and an open attitude towards the activities of trade unions is adopted;

(m) where it is not practicable for unions to operate, other means of association, such as Works Councils, are recognised; and

(n) all necessary training is provided to workers, including that required under Law and industry specific training (both mandatory and best practice).

4 Harassment.

AG does not tolerate any form of harassment in the workplace, including sexual harassment. The Supplier shall take appropriate measures to prevent harassment, including sexual harassment, occurring in any workplace (whether its own or AG's), while providing goods or services to AG.

5 Health and Safety

5.1 AG recognise our duty of care to foster practices that support operational excellence while ensuring compliance with relevant health and safety Law, industry standards and best practices.

5.2 It is the Supplier's responsibility to ensure that all Representatives are suitably trained and competent to perform their tasks safely.

5.3 The health and safety responsibilities of both the Supplier and AG must be clearly defined.

5.4 The Supplier shall implement a formal hazard management process to effectively minimise health and safety risk.

5.5 The Supplier is responsible for promoting health and safety standards, maintaining a healthy working environment to ensure the well-being of all individuals impacted by AG's operations, and complying with health and safety Laws wherever it operates.

5.6 Where the Supplier or its Representatives are performing activities at AG sites, they shall comply with the AG Site Health and Safety Rules set out in this Code.

D. ENVIRONMENTAL RESPONSIBILITY

1 The Supplier shall comply with all relevant Law relating to the environment and operate its business in an environmentally responsible way.

2 The Supplier shall take a proactive approach to working with AG in reducing our environmental impact. In the case of key suppliers to AG, this will involve working with AG and its third-party sustainability ratings provider, to evaluate sustainability performance to help identify opportunities for improvement and benchmark sustainability within our supply chain. It will also involve working with AG and its third-party carbon emissions monitoring provider to participate in carbon emissions assessment and monitoring and collaborating to explore mechanisms to reduce our and our suppliers' carbon footprint.

3 The Supplier shall ensure that:

(a) it monitors and takes action to reduce its and its supply chain's carbon emissions, ideally by implementing formal carbon reduction or net zero or similar targets;

(b) it adopts and uses practices and systems that minimise the use of resources e.g. water efficiency, energy efficiency;

(c) it and its suppliers use environmentally friendly working practices, tools and equipment, consumables and replacement parts, wherever possible;

(d) the goods it sells or manufactures (including the inputs and components incorporated into those goods) comply with all applicable environmental Laws;

(e) where practicable, all consumables originate from a sustainable or recycled source;

(f) there are facilities or arrangements in place, either directly or through its suppliers, to ensure AG can return used packaging for recycling or reuse or environmentally friendly disposal; and

(g) any hazardous or toxic waste that is produced is properly identified and disposed of by licensed and competent bodies via authorised and/or licensed means.

4 The Supplier shall have a written environmental / sustainability policy appropriate to the size and nature of its operation which addresses preventing, mitigating and controlling serious environmental and health impacts from its operations. The Supplier shall review this policy annually, have it signed and dated by senior management, and provide it to AG on request.

5 The Supplier shall carry out annual reviews and audits of its environmental performance and the environmental performance of its suppliers, and keep a record of all findings and any remedial action or improvements in processes or procedures that are made to reduce any negative environmental impact. The Supplier shall provide such records to AG on request.

6 The Supplier shall identify and make know to AG, a senior manager within its organisation who has overall responsibility for the Supplier's environmental performance.

7 The Supplier shall have an effective internal environmental management program, with adequately trained staff, which addresses environmental impact control, collation and communication of data on key environmental indicators, the continuous improvement of environmental performance, and the reduction of pollution, emissions and waste.

8 The Supplier shall possess ISO 14001 accreditation or be demonstrably working towards ISO 14001 accreditation throughout the contracting period with AG.

E. FINANCIAL CRIME

1 Introduction

AG is committed to providing the highest standards of care and service to our clients. As such, we take compliance with Law extremely seriously and expect our suppliers to do so too.

2 Anti bribery and corruption, AML and tax evasion

2.1 Supplier shall ensure that no benefit which would amount to a bribe under Law, is given or accepted on behalf of an AG Entity, and shall put in place, maintain and enforce an appropriate policy and procedures to prohibit Supplier personnel from:

(a) the offering, giving, soliciting or receiving of a bribe at any time (including the making of facilitation payments or the bribery of public officials) whether for the benefit of Supplier, any AG Entity, the worker, or a member of the worker's family, friends, associates or acquaintances;

(b) the use of a gift or hospitality to induce a fraud or other wrongdoing to secure a personal or business benefit (and Supplier shall keep proper and accurate records of all payments or other benefits made or received and expenses incurred in connection with its contract with AG);

(c) the use of sponsorship or advertising agreements to exercise undue influence; and

(d) unapproved or unauthorised charitable donations or political donations of any kind.

2.2 Supplier shall put in place, maintain and enforce an appropriate anti-money laundering and counter terrorist financing policy and procedures which:

(a) verify the legitimate origin of goods and services within their supply chain; and

(b) verify the identity and the legitimate nature of the businesses with which Supplier contracts.

2.3 Supplier shall maintain a tax strategy that demonstrates a willingness to pay the right amount of tax, in the right place at the right time. Supplier shall put in place, maintain and enforce an appropriate policy and procedures aimed at preventing tax evasion and the criminal facilitation of tax evasion, which:

(a) regularly assess the opportunity, motive and means within their business for the criminal facilitation of tax evasion;

(b) implement reasonable preventative measures by developing procedures that are appropriate to mitigate the identified risks; and

(c) effectively communicate the expectations of management, being that compliance with such policy and procedures is mandatory and that the business takes a zero-tolerance approach to any breach.

3 Prevention of fraud

3.1 Supplier shall ensure that it and its Associates shall not, by any act or omission, commit, cause, facilitate or contribute to the commission by any person, including any AG Entity, of a Fraud Offence or Failure to Prevent Offence, in each case in connection with the performance of services for any AG Entity.

3.2 Supplier shall not, and shall ensure that its Associates shall not, solicit or engage with or take steps to solicit or engage with any Associate of any AG Entity to commit, cause, facilitate or contribute to the commission of a Fraud Offence in connection with its contract with or the performance of services for any AG Entity.

3.3 Supplier shall ensure that it and all relevant Supplier Associates have in place such Prevention Procedures as it is reasonable in all the circumstances to expect Supplier and Supplier Associates to have in place to prevent any breach of these provisions.

4 Trade Sanctions

Supplier and AG shall comply with Law pertaining to international trade sanctions and shall notify the other promptly on becoming aware of any activity or suspected activity, connected to the business relationship between AG and Supplier, which contravenes any such economic, trade and/or territorial restrictions.

5 Financial Crime Generally

5.1 AG Group has a responsibility to detect and prevent Financial Crime, therefore Supplier shall co-operate with AG in relation to due diligence and the verification of the legitimate nature of (a) Supplier entities, (b) payment processes and funding arrangements, and (c) any other aspects of the goods and service provision by Supplier.

5.2 Supplier shall comply with Law relating to Financial Crime and shall not do or omit to do anything which would cause any AG Entity to be in breach of any such Law.

5.3 Supplier shall implement measures appropriate to Supplier's business in order to prevent and mitigate the risk of Financial Crime occurring and support its identification and detection, such as mandatory training for workers, oversight, regular risk assessments, due diligence, procedural audits, codes of conduct, whistleblowing procedures and internal and regulatory reporting and notification procedures.

5.4 Supplier shall keep sufficiently detailed records relating to the identification and prevention of Financial Crime and promptly notify AG upon becoming aware of any actual or suspected instance of Financial Crime, or any attempt or request to commit Financial Crime, connected to the business relationship between AG and Supplier or its Associates.

5.5 Supplier shall encourage workers to promptly report to an appropriate senior manager if they know or suspect that any business activity contravenes Supplier's Financial Crime policies and shall implement disciplinary action for any worker failing to comply with such procedures. Supplier shall ensure that workers do not suffer any adverse consequences for making a report under the Financial Crime policies or refusing to participate in Financial Crime.

5.6 Supplier shall ensure that all Supplier Associates involved in the performance of services for AG, in connection with its contract with AG have been vetted and that due diligence and monitoring has been and is undertaken on a continuing basis in respect of them to an appropriate standard in the relevant circumstances.

5.7 Supplier shall ensure that all Supplier Associates involved in the performance of services for or its contract with AG are subject to and at all times comply with obligations which are equivalent to Supplier’s obligations under these Financial Crime provisions. Supplier shall be liable to AG for any act or omission by any Supplier Associate in breach of any such obligation as if this was an act or omission of Supplier itself.

5.8 Supplier warrants and represents that it has not, and to the best of its knowledge, information and belief, no Supplier Associate:

(a) has been investigated in connection with, or charged with having committed, caused, facilitated, or contributed to the commission of any Financial Crime;

(b) has received any court orders, warrants, or oral or written notices from a government prosecuting authority concerning any actual or alleged violation by it of any Financial Crime; or

(c) has received any report (including from Supplier’s external auditors, any Supplier Associates or any other person) or discovered any evidence suggesting that Supplier or any Supplier Associate has committed, caused, facilitated or contributed to the commission of any Financial Crime.

5.9 Without affecting any right or remedy available to any AG Entity, a breach by Supplier of these Financial Crime provisions shall be deemed a material breach of its contract with AG.

6 Definitions

In these Financial Crime provisions the following terms have the meanings below.

Associate means any entity or person which is an employee, agent, group company or subsidiary undertaking of or service provider (of any tier) to a body, and any other entity or person "associated with" (as defined in ECCTA 2023) that body or any such entity or person

Financial Crime means bribery, corruption, money laundering, terrorist financing, failure to prevent the criminal facilitation of tax evasion, Fraud Offences and Failure to Prevent Offences

Failure to Prevent Offence means an offence under section 199 of ECCTA 2023 and any other applicable United Kingdom laws, legislation, statutory instruments and regulations in relation to failure to prevent fraud and any similar or equivalent laws in any other relevant jurisdiction

Fraud Offence and **Prevention Procedures** shall be construed in accordance with Part 5 of the Economic Crime and Corporate Transparency Act 2023 (**ECCTA 2023**) and guidance published under it;

F. CONFIDENTIALITY AND DATA PROTECTION

1 The confidentiality and security of AG's and its clients' information and data is paramount. As such, the Supplier shall:

(a) hold all information received from us confidentially and securely and in compliance with their contract with AG, and ensure that there is no unauthorised access to this information by third parties, including unauthorised Representatives;

(b) inform AG immediately if it becomes aware of any security breach or incident that affects or may affect the security of AG's or its clients' information or data, providing full details of the breach or incident, its impact, and the proposed mitigation and remediation steps, and fully co-operate with AG in securing and preserving all such information or data;

(c) comply with all relevant Law related to data protection and privacy, including the General Data Protection Regulations ((EU) 2016/679) and Laws implementing it, and not do or omit to do anything which would cause AG to be in breach of any such Law;

(d) to the extent that it processes personal data on behalf of AG, do so only in accordance with the terms set out in its contract with AG (and if no data processing terms are included, then in accordance with the Data Processing Terms set out in AG's Standard Terms and Conditions linked to above); and

(e) respect and protect the intellectual property rights of AG and its clients.

2 To the extent that the Supplier will be collecting personal data in respect of which AG will be a controller or joint controller with the Supplier, it shall provide each individual to whom the personal data relates with all such information required to be provided to the data subject pursuant to Law.

3 Prospective suppliers shall keep all pre-contract information (e.g. negotiations and tender progress) strictly confidential and, at AG's request, enter into a more detailed non-disclosure agreement.

4 The Supplier shall not publicise the existence or nature of its relationship with AG without AG's prior written consent. Where consent is given, The Supplier shall ensure that any publicity is limited to that which has been approved by AG, and that any use of AG's intellectual property rights or branding is in accordance with AG's branding guidelines.

G. RESPONSIBLE USE OF AI

1 Innovation and technology are firmly embedded in AG's DNA. We are committed to embracing artificial intelligence (AI) and harnessing technology to deliver tangible benefits for clients. In doing so, AG is committed to the following guiding principles:

(a) **Governance**: All new systems are robustly assessed before adoption, to ensure that they are deployed responsibly and in a way that is consistent with legal and ethical standards.

(b) **Data Integrity and security**: AG ensures that appropriate security measures are in place to protect the data and confidential information of clients and AG's data and confidential information.

(c) **People**: Technology does not replace people; it is a tool to be utilised by AG's Partners and employees in delivering for clients. Unless specifically agreed with a client, the output of any tool will be reviewed by people in AG, to ensure that clients continue to receive the benefit or their expertise.

(d) **Limited Use**: AG is committed to protecting client data and to ensuring that third party technology providers are not permitted to use any client data to train and develop their systems.

2 AG expects its suppliers to apply the above principles in their own use of AI and technology. The Supplier shall not act in a manner that would cause AG to fail to adhere to the above principles. Among other things, the Supplier shall:

(a) be transparent about when and how AI is used, and obtain AG's consent where it proposes to use an AI system to process AG's or its clients' data;

(b) in its use of any AI in the provision of services, comply fully with its contract with AG, and with all applicable Law, including the EU AI Act, and not infringe the intellectual property rights of others;

(c) ensure that any AI systems developed or used by the Supplier are robust, secure, and safe throughout their entire lifecycle;

(d) develop and use AI systems in a way that respects human rights and human-centric values, including fairness, equality, diversity, privacy and data protection, and avoiding discrimination and bias;

(e) ensure the explainability, auditability and traceability of any AI systems used or developed by the Supplier, including their outputs, and ensure, where appropriate, that decisions or outcomes from an AI system are contestable;

(f) establish and maintain appropriate governance, risk management, and policies and procedures that promote the responsible, accountable, ethical and environmentally responsible use of AI;

(g) not use or retain AG's or its clients' data or confidential information for the purposes of training, developing, testing, or improving any AI system or model or other technology, without AG's prior express written consent;

(h) minimise the duration and extent of processing of AG's or its clients' data or confidential information within any AI system, including by implementing zero data retention policies with third-party providers;

(i) ensure that AG's or its clients' data or confidential information is not exposed to human review, by virtue of its use within an AI system;

(j) implement appropriate risk management and supervision measures to ensure that third-party providers, who develop or provide some or all of an AI system, adhere to the above requirements; and

(k) ensure that its employees and any other persons who use or develop AI systems in connection with the services have a sufficient level of AI literacy, including the skills, knowledge and understanding to make an informed deployment of AI systems as well as an awareness about the opportunities and risks of AI and the possible harm it can cause.

H. INFORMATION SECURITY MINIMUM REQUIREMENTS

1 Definitions

In this Information Security Minimum Requirements document (**ISMR**), bracketed reference letters/numbers after a requirement relate to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire" or an ISO 27001:20132022 Annex A control and references to the following capitalised terms have the following meanings:

AG means AG Service Company Limited, a company registered in England and Wales (No. 7299444) whose registered office is at Milton Gate, 60 Chiswell Street, London, EC1Y 4AG

AG Data means all data disclosed or made available by AG or a member of the AG Group to the Supplier (including Confidential Information and Personal Data) and all materials to be created or created and data to be generated or generated by the Supplier pursuant to the Contract.

AG Group means AG LLP and (a) any entity owned or controlled by AG LLP including AG; and (b) any entity owned or controlled by an entity captured under part (a) of this definition

AG IT System means the hardware and software comprising the IT infrastructure which handles all electronic data necessary for the business of the members of the AG Group

AG LLP means Addleshaw Goddard LLP a limited liability partnership registered in England and Wales (No. OC 18149) whose registered office is at Milton Gate, 60 Chiswell Street, London EC1Y 4AG

Best Industry Practice means all relevant practices and professional standards relating to the protection of information resources and the maintenance of the confidentiality, integrity and availability of customer data that would be expected of a well-managed, expert service provider performing services substantially similar to the Services to customers of the same nature and size as AG Group

Client means any customer, prospective customer or former customer of AG Group

Cloud is defined by NIST as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (NIST SP 800-145)

Confidential Information means

(a) in the case of AG, any and all information whether recorded or not (and, if recorded in whatever media and by whosoever recorded) disclosed or made available by AG to the Supplier that is by its nature confidential and/or the other party knows or ought to know is confidential including

(i) details of the existing or proposed business carried on by any member of the AG Group including financial, technical, operational, administrative, contractual (including with clients or suppliers or the existence or details of this Contract), marketing and other information or data

(ii) information relating to any client, potential client or former client of any member of the AG Group including the confidential information of any such client, potential client of former client

(iii) AG Data

(iv) information in respect of which any member of the AG Group owes a duty of confidentiality to a third party

(v) information obtained by Supplier as a result of being present at any of the premises of any member of the AG Group

(vi) information disclosed prior to the date of and in connection with this Contract

(vii) any and all other information which is designated by AG as confidential

(viii) plans, analyses, compilations, studies and other documents (in whatever format) which contain or otherwise reflect or are generated from any of the information described above and

(ix) any copies of any of the above

(b) and in the case of the Supplier all information whether recorded or not (and, if recorded in whatever media and by whosoever recorded) disclosed by the Supplier to AG relating to the Contract and which is identified by the Supplier in writing to AG as being confidential

Contract means the contract in place between the Supplier and AG or another member of AG Group

GDPR means the General Data Protection Regulations ((EU) 2016/679)

Handle means to store, disclose, transfer, access or process data (and Handled shall be construed accordingly)

Infrastructure as a Service (IaaS) is defined by Microsoft as "computing infrastructure, provisioned and managed over the internet". IaaS is normally supplied as virtual servers hosted in the Supplier's (or Sub-contractor's) data centres that can be used for any purpose by the AG Group.

Personal Data means any data or information which relates to an individual and which is held by or is under the control of any member of the AG Group as defined in the GDPR

Physical Facilities means the physical premises where hardware comprising part of the Technical Solution is located

Platform as a Service (PaaS) means a computing environment (including servers, storage and operating system) provided and maintained by the Supplier or Sub-contractor, on which the AG Group can develop, run and manage their own applications

Processing means any operation or set of operations which is performed on data - such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

Relevant Law means

(a) any legislation, enactment, statute, regulation, by-law; ordinance or subordinate legislation in force from time to time to which any member of the AG Group, the Supplier or any third party connected with the Contract is subject

(b) the common law as applicable to any member of the AG Group, the Supplier or any third party connected with the Contract from time to time

(c) any binding court order, judgment or decree

(d) all applicable statutory, industry or other rules, codes, guidance, regulations, instruments and provisions in force from time to time; and

(e) in the case of the Supplier, requirements notified to the Supplier by AG in writing which are born out of the rules and codes of conduct stipulated by any Regulatory Authority or industry body to which any member of the AG Group is subject from time to time

Regulatory Authority means in relation to AG Group, any body (including the Solicitors Regulation Authority, any consumer protection body or the Information Commissioner's Office) which has the responsibility of supervising and/or regulating any member of the AG Group and/or any individual performing a role on behalf of any member of the AG Group

Serverless computing means a cloud computing model using servers supported by the Supplier or Sub-contractor but with machine resources dynamically allocated as required by the customer. This option is normally used to deploy code which runs when triggered by an event and can be integrated with other services.

Services means the services to be provided under the Contract

Software as a Service (SaaS) is defined by Microsoft as a service which "allows users to connect to and use cloud-based apps over the Internet. Common examples are email, calendaring and office tools". Hardware and software are managed by the Supplier or Sub-contractor and the service is usually purchased on a pay-as-you-go basis

Special Categories of Personal Data means any data or information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning

health or data concerning a natural person's sex life or sexual orientation which is held by or is under the control of any member of the AG Group

Sub-contractor means any third-party supplier from time to time providing goods and/or services directly or indirectly (via any tier of the Supplier's supply chain) to the Supplier in connection with the delivery of the Services. Any Supplier affiliate providing goods or services in connection with the performance of the Services shall be a third party for the purpose of this definition

Supplier's information security policy means the documented policy implemented within the Supplier's business which details the procedures, processes, roles and responsibilities, risk assessment tools and risk management tools which comprise the Supplier's information security arrangements and which enable the Supplier as a minimum to comply with the requirements of this ISMR

Supplier IT System means the hardware and software comprising the IT infrastructure under the direct control of the Supplier which handles all the electronic data necessary for the business of the Supplier

Technical Solution means the description of the hardware (including its location(s)) and the software utilised by the Supplier in the provision of the Services which shall comprise the Physical Facilities, the Supplier IT System and may also comprise hardware and software managed by one or more third parties which accordingly may be outside of the direct control of the Supplier

Supplier or **supplier** means the person supplying, or wishing to supply, goods or services to AG

2 Risk management

2.1 The Supplier shall:

(a) protect the confidentiality, integrity and availability of all AG Data and any other information relating to AG which is Handled by the Supplier or any of its Sub-contractors;

(b) ensure that such information is not lost, destroyed (including deletion), altered (including corruption), accessed by unauthorised personnel, transferred, mis-used or (without appropriate authorisation) disclosed while it is in the possession and/or under the control of Supplier or any of its Sub-contractors; and

(c) establish an information security risk assessment which includes:

(i) a risk assessment methodology

(ii) regularly analysing and evaluating the risks, at a minimum annually

(iii) awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure

(iv) compliance with defined retention periods and end-of-life disposal requirements

(v) data classification and protection from unauthorized use, access, loss, destruction, and falsification

(vi) risk acceptance criteria; and

(vii) risk treatment plans.

2.2 The Supplier shall at all times have in place such security arrangements as are necessary:

(a) to comply with the requirements of paragraph 2.1 of this ISMR;

(b) for the identification and management of operational security risks; and

(c) to mitigate risks to an acceptable level - based on risk criteria, which shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.

2.3 The Supplier shall at all times Handle AG Data in accordance with

(a) Best Industry Practice;

(b) the requirements of the ISO 27001 Standard or equivalent; and

(c) Relevant regulation and law.

2.4 The Supplier shall have in place and comply with a comprehensive information security policy, which is reviewed annually. The Supplier shall provide AG with an up-to-date copy of its information security policy on request.

2.5 The Supplier shall provide the services and handle the AG Data in accordance with the Technical Solution where applicable as approved in writing by AG.

2.6 The Supplier shall maintain points of contact for applicable regulatory or legal jurisdictional authorities, and national and local law enforcement., These shall be regularly updated (e.g. change in impacted scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established in order to be prepared for a forensic investigation as an example which would require rapid engagement with law enforcement.

3 Audit

3.1 The Supplier shall develop and maintain information security audit plans to meet the requirements of ISO27001. Auditing plans shall include reviewing the effectiveness of the implementation of security controls. All audit activities that involve AG or Client data must be agreed with AG prior to commencement.

3.2 The Supplier shall arrange independent audits of its information security arrangements at least annually to ensure:

(a) conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics; and

(b) that the organisation addresses nonconformities of established policies, standards, procedures, and compliance obligations.

3.3 Wherever risks are identified that can be more effectively managed or require better security controls, the Supplier shall update its information security policy accordingly and implement the changes as soon as reasonably practicable in accordance with paragraph 8 of this ISMR.

3.4 The Supplier shall carry out regular data protection impact assessments of its information security arrangements to ensure:

(a) appropriate technical and organisational measures, designed to implement data protection principles, have been implemented; and

(b) the necessary safeguards have been integrated into the processing of personal data in order to meet the requirements of the GDPR and protect the rights of data subjects.

3.5 The Supplier will, at all times and on reasonable notice, allow AG or its nominee access to:

(a) all Physical Facilities where AG Data is stored, processed or handled;

(b) all records of the Supplier or any of its Sub-contractors connected with the Services;

(c) any individual involved in the provision of the Services, or with access to any element of the Technical Solution or who has responsibility pursuant to the Supplier's information security policy; and

(d) the procedures, processes and tools utilised in connection with the Contract or in connection with the Supplier's information security policy

for the purpose of auditing compliance with this ISMR and assessing compliance with the Supplier's information security policy.

3.6 The Supplier shall co-operate fully with any right to audit request and will provide on request any records or other information connected with the delivery of the service or to validate if information security obligations contained within this ISMR are being met.

4 Implementation and management of information security measures

4.1 The Supplier shall ensure that appropriate roles and responsibilities are clearly defined and recorded in the Supplier's information security policy, appropriately allocated and properly fulfilled by individuals within the Supplier's organisation to ensure that:

(a) the Supplier's security obligations under the Contract, including this ISMR, are met;

(b) the Supplier's information security policy is fully and properly implemented;

(c) compliance with the Supplier's security obligations and the Supplier's information security policy are monitored, recorded and enforced;

(d) where information security issues are identified, reporting procedures to senior management are in place and are followed appropriately; and

(e) regular risk assessments are undertaken and the Supplier's information security policy and any other associated policies are updated to ensure that risk is effectively managed and reflected in policy amendments where required.

4.2 The Supplier shall implement appropriate technical and organisational measures to ensure that processing of Personal Data and Special Categories of Personal Data is performed in accordance with GDPR. This may include, pseudonymising and encrypting Personal Data, and ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the measures in place.

4.3 The Supplier shall implement data input and output validation to reduce potential for misuse, manual or systematic processing errors and data corruption.

4.4 The Supplier shall ensure that application programmable interfaces (APIs) comply with Relevant Law and contractual requirements, and the Supplier shall create, test and deploy any APIs which are required, in line with industry good practice.

4.5 The Supplier shall establish policies, procedures, and mutually agreed upon provisions and/or terms to satisfy AG's requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.

5 Sub-contractor and supplier management

5.1 The Supplier shall ensure that AG Data that is hosted within the Supplier IT System is not released to anyone outside the Supplier's organisation without the prior express written approval of AG.

5.2 The Supplier shall ensure that AG Data is only handled by its approved third-party suppliers or any of its Sub-Contractors in accordance with the agreed delivery model.

5.3 Where AG Data is handled by a third-party supplier or Sub-Contractor other than in accordance with the agreed delivery model, the Supplier shall provide AG with full details in writing of the request, clearly describing the business justification, and requesting a change to the delivery model. Where AG in its sole discretion, agrees to such change, it shall issue the Supplier with prior express written approval - in accordance with the procedure for change management detailed in section 7 of this ISMR.

5.4 The Supplier shall ensure that its third-party suppliers or Sub-Contractors shall handle AG Data in accordance with the Contract, including in particular this ISMR, such that the requirements placed on the third-party suppliers or Sub-Contractors shall as a minimum be equal to the obligations of Supplier pursuant to the Contract.

5.5 The Supplier shall design and implement controls to mitigate and contain data security risks through separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.

5.6 The Supplier shall manage third-party suppliers and Sub-contractors such that information security controls are not reduced by the introduction of Sub-contractor products or services.

5.7 The Supplier shall carry out audits on their third-party suppliers and Sub-contractors handling AG Data at least annually to ascertain their information security controls are maintained and are in accordance with the requirements of this ISMR. These audits shall include:

(a) all third-party suppliers and Sub-Contractors upon which their supply chain depends.

(b) the risk management and governance processes so that practices are consistent and aligned to account for risks inherited from other members of the supply chain.

5.8 An Exit Plan including relevant timescales should be agreed with third-party suppliers and Sub-contractors which should include the return and removal of AG data upon termination of the contract.

6 Human resources security

6.1 The Supplier shall document and communicate roles and responsibilities of contractors, employees, and third-party users as they relate to information assets and security.

6.2 The Supplier shall carry out the following background and reference checks:

(a) proof of identity;

(b) proof of address;

(c) proof of right to work;

(d) work references;

(e) proof of continuous employment history;

(f) criminal records check (equivalent to the Disclosure Scotland Checks);

(g) proof of qualifications;

(h) credit reference check;

(i) financial sanctions check; and

(j) any other check required by Relevant Law.

6.3 The Supplier shall establish a security awareness training program for all the Supplier's Sub-Contractors, third-party users, and employees and mandate completion of this. All individuals with access to organisational data shall receive appropriate awareness training and regular updates in organisational procedures, processes, and policies relating to their professional function relative to the organisation. This shall be on induction and annually thereafter.

6.4 The Supplier shall establish a formal disciplinary or sanction policy to cover violation of security policies and procedures by employees. Such employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.

6.5 The Supplier shall inform all workforce personnel to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to Relevant Law.

6.6 The Supplier shall create, update and maintain a record, for all individuals with access to AG Data, of the following information:

(a) full name;

(b) job role;

(c) start date; and

(d) leaving date.

6.7 The Supplier shall establish policies and procedures to ensure the principle of least privilege is followed, and data is accessible only by the minimum number of people necessary to support the service

6.8 Where access is given to AG Group's IT resources and systems, the Supplier shall ensure that by default access be configured with restrictive permissions.

7 Physical and environmental security

7.1 The Supplier shall ensure that adequate security measures are in place at all Physical Facilities to ensure that:

(a) security perimeters (barriers such as perimeter fencing, walls, card-controlled entry gates, or manned reception desks) shall be used to protect areas that contain AG Data and / or information processing facilities used to handle AG Data;

(b) hardware used to handle AG Data (e.g. servers; telecommunication cabling) and any other vital equipment or services (e.g. power supplies; security cameras or access devices) are protected from damage, unauthorised access and/or interruption;

(c) access to secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access, such as a proximity or swipe card system;

(d) reports on access to secure areas shall be produced and reviewed quarterly;

(e) Data centres shall be equipped with doors:

(i) which are resistant to fire and forcible entry;

(ii) that automatically close immediately after they have been opened; and

(iii) that set off an audible alarm when they have been kept open beyond a certain brief period of time.

7.2 The Supplier shall employ a CCTV system where appropriate, to monitor certain areas of their sites for the purpose of prevention and detection of crime, safety and good management.

(a) All entrances shall be monitored continuously.

(b) CCTV cameras, camcorders, webcams, and other video cameras used shall be placed so that they do not capture passwords, telephone, credit card numbers, encryption keys, or any other security parameters.

(c) CCTV footage shall be stored and available for thirty days.

7.3 Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises shall be controlled by the Supplier, and, if possible, isolated from information processing facilities to avoid unauthorised access.

(a) All deliveries and loading shall be supervised.

7.4 The Supplier shall obtain authorisation prior to relocation or transfer of AG Data, or hardware or software used to handle AG Data, to an offsite premises.

7.5 The Supplier shall have a clear desk policy for papers and removable media and a clear screen policy for IT systems.

7.6 The Supplier shall regularly test the security measures in place at the Physical Facilities to risk assess for any vulnerabilities and to enhance measures where security is shown to be inadequate.

8 Change management

8.1 The Supplier shall ensure that their sub-contractors and third-party suppliers adhere to robust and secure policies and procedures for change management, release, and testing.

8.2 The Supplier shall ensure that developers supporting the service review new and evolving threats, and ensure the service is improved in line with them.

8.3 If the Supplier wishes to implement a change to the Technical Solution or other operational or organisational change connected with the provision of the Services, it may only do so with prior written consent from AG, unless the change:

(a) does not have a detrimental effect on the provision of the Services or the effectiveness of the security measures in place; or

(b) is critical to the continuance of the Services and/or the security of the AG Data.

8.4 The Supplier may only implement a change to the Technical Solution or other operational or organisational change connected with the provision of the Services where the agreed change control procedure has been followed and, in the circumstance described in paragraph 8.3 of this ISMR, AG has, in its sole discretion, given prior written approval to the change.

8.5 The Supplier shall separate Production and non-production environments in line with segregation of duties so that accountability is enforced.

8.6 The Supplier shall ensure that AG Data is not replicated or used in non-production environments. Any use of AG data in non-production environment requires explicit, documented approval from AG.

8.7 The Supplier shall ensure that it has in place a robust configuration management process for the Supplier IT System and Technical Solution, which shall include:

(a) a comprehensive testing regime and approval process for all changes to hardware or its configuration or to software; and

(b) completion of regular comprehensive reviews of servers, firewalls, routers and monitoring platforms to assess optimal configuration and security.

8.8 The Supplier shall ensure that it has in place a robust development management process for the Supplier IT System and Technical Solution, which shall include:

(a) trace back to a living individual, for the development and testing of new software;

(b) removal of any special access paths prior to moving software into production, including any Trojan horses, trapdoors, back-doors, developer security shortcuts, developer universal privileges, in order to ensure that access may only be obtained via normal secured channels;

(c) ensuring that diagnostic test hardware and software, such as communications line monitors, are used only by authorised Individual and that access to such hardware and software is rigorously controlled and restricted; and

(d) the adoption, in accordance with Best Industry Practice, of other secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed or malformed software.

8.9 The Supplier shall ensure that the technical and organisational measures required for compliance with the data protection principles and all applicable requirements of GDPR are integral to the Supplier IT System and the Technical Solution.

8.10 The Supplier shall ensure that AG Data is not used to test, demonstrate or evidence any characteristics of the Services provided by the Supplier

9 Incident management

9.1 The Supplier shall establish policies and procedures and supporting business processes and implement technical measures, to triage security-related events and ensure timely and thorough incident management policies and procedures.

9.2 The Supplier shall establish mechanisms to monitor and quantify the types, volumes, and costs of information security incidents.

9.3 The Supplier shall report all actual or potential security violations, breaches or incidents which impact or could potentially impact the provision of the Services, the security of AG Data or the ability of AG to carry out its business in accordance

with the escalation processes agreed with AG, and as soon as reasonably practicable and in any event not more than twenty-four hours after the incident comes to the Supplier's attention (or in any shorter period required by the Contract).

10 Vulnerability management

10.1 The Supplier shall establish policies and procedures and supporting business processes and implement technical measures, for timely detection and remediation of vulnerabilities within applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. Critical rated vulnerabilities should be remediated as soon as possible and within 7 days and high rated vulnerabilities should be remediated within 30 days of detection.

10.2 The Supplier shall conduct annual independent penetration testing, including vulnerability assessment exercises on the Services and the Technical Solution and allow AG visibility of the findings where required.

10.3 The Supplier shall conduct vulnerability assessments on at least a monthly basis and shall ensure that security vulnerability assessment tools or services which are implemented can accommodate any virtualisation technologies which might be used (e.g. are virtualisation aware).

10.4 The Supplier shall establish policies and procedures, implement supporting business processes and ensure technical measures to:

(a) prevent the execution of malware on organisationally owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

(b) prevent the introduction of malicious software (including viruses and spyware) into the Technical Solution and/or into the AG IT System through the provision of the Services;

(c) promptly detect any malicious software and/or viruses attempting to access any element of the Technical Solution and/or into the AG IT System through the provision of the Services;

(d) implement regular updates of anti-malware software tools;

(e) report and escalate as appropriate any malicious software and/or viruses incidents in-line with agreed and documented AG incident management procedures; and

(f) ensure that incidents are immediately notified to AG if there is an actual or suspected Virus in:

(i) The AG IT System;

(ii) any part of Technical Solution to which the AG IT System interfaces; or

(iii) anything to be delivered by the Supplier or any sub-contractor to AG as part of the provision of the Services.

11 Network security management

11.1 The Supplier shall implement all appropriate security measures to protect the AG Data within the Supplier IT System and at all interfaces where AG Data enters or leaves the AG IT System or any third-party electronic environment (Network).

11.2 The Supplier shall carry out regular tests to check the security of the Network and make such changes as are necessary to remove any actual or suspected security weaknesses.

11.3 Where appropriate, the Supplier shall document a data flow map for AG Data which depicts accurately and comprehensively how AG Data flows and is stored across the AG IT System, the Supplier IT System and any Network or other permitted external destinations.

11.4 Where the Supplier uses APIs, supplier shall ensure that such APIs shall be open and published to ensure support for interoperability between components and to facilitate migrating applications.

11.5 The Supplier shall establish policies and procedures and supporting business processes and implement technical measures, for the use of encryption protocols for protection of data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) in accordance with Relevant Law, including:

(a) the Supplier shall encrypt AG Data in transit and at rest;

(b) the Supplier shall apply encryption using industry recognised technologies such as Virtual Private Network (VPN), Secure Sockets Layer (SSL) or Transport Layer Security (TLS 1.2 and higher)

(c) the Supplier shall protect all AG Data transmitted over third party public networks with strong encryption techniques of at least 256 bits, such as Secure Sockets Layer (SSL), or Internet Protocol Security (IPsec); and

(d) where the Supplier manages cryptographic keys, the Supplier shall ensure that these have identifiable owners (binding keys to identities) and that effective key management policies are established.

12 Cloud Security

12.1 Where the Supplier delivers a service using Cloud infrastructure or services, the Supplier shall:

(a) hold a Cloud Policy which sets out the management and governance of cloud platforms;

(b) Information Security roles and responsibilities for the cloud service provider shall be agreed, documented, and reviewed periodically to ensure responsibilities are transparent and defined.

(c) ensure that multi-factor authentication is in place for externally hosted cloud platforms;

(d) ensure that Cryptography is deployed within the cloud environment, using AES-256 block cipher algorithm and encryption of traffic and data applying TLS Cipher Suite (TLS 1.2 and higher). Key management process to be implemented and maintained;

(e) be aware of the cloud services used to provide services to the Firm which can be requested by the Firm in inventory form in line with due diligence requirements;

(f) instruct vulnerability scanning and penetration testing of the cloud environment and vulnerabilities found shall be prioritised and remediated depending on criticality;

(g) Distributed Denial of Service (DDoS) protection shall be in place to help safeguard all resources within the cloud.

(h) harden virtual machines within the cloud to maximise security;

(i) monitor the cloud environment to ensure performance, unauthorised access, tampering and data integrity;

(j) ensure that management of virtualisation platforms is restricted to AG Group's IT staff and service provider staff;

(k) ensure that if templates are used in the deployment of virtual resources they are reviewed at least annually for suitability and security issues;

(l) inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks, and inform AG of any changes to provision of such services;

(m) ensure that AG data is appropriately segmented in a multi-tenant environment from any other tenant users, based on the following considerations:

(i) established policies and procedures;

(ii) identity and access control mechanisms;

(iii) isolation of data, and sessions that mandate stronger internal controls and high levels of assurance; and

(iv) compliance with Relevant Law;

(n) ensure that Network environments and virtual instances are designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed by the Supplier at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls; and

(o) use secure (e.g., non-clear text and authenticated) standardised network protocols for the import and export of data and to manage the service and shall make available a document to AG detailing the controls involved.

(p) Changes to cloud services are required to be declared and reported so that risks can be flagged, and mitigating controls are deployed where required.

(q) For a supplier that is a cloud service provider there shall be a documented incident notification procedure in place with an agreed reporting timescale contained within the contract. A detailed description of the incident will be provided to the Firm by the supplier as part of the incident notification procedure.

13 Access control

13.1 The Supplier shall ensure that all access to the Technical Solution and AG Data is:

(a) strictly controlled - physically and logically, and that user access is audited on at least an annual basis;

(b) restricted to authorised Individuals only as per defined segregation of duties to address business risks associated with a user-role conflict of interest.;

(c) granted only when an Individual inputs authorised identity authentication information; and

(d) revoked as soon as no longer required or when the relevant individual is no longer engaged by the Supplier or assigned to the Services.

13.2 The Supplier shall establish procedures to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access.

13.3 The Supplier shall maintain, protect and retain user access logs for 365 days, so that all obligations under Relevant Law can be met and potentially suspicious network behaviours, file integrity anomalies and security breaches can be investigated.

13.4 The Supplier shall ensure that Passwords for the Supplier's IT Systems:

(a) are technically enforced;

(b) are at least nine characters;

(c) are different from their associated unique identifier;

(d) contain characters from at least three or more of the following:

(i) numbers;

(ii) upper-case letters;

(iii) lower-case letters;

(iv) symbols (e.g. &^%);

(e) are subject to change on first login, if provided by an administrator;

(f) are subject to change every 90 days;

(g) are different from the previous 24 passwords; and

(h) are supported by multi-factor authentication for all remote access and administrator access to AG Data.

13.5 The Supplier shall ensure that individual accounts on the Supplier IT System must be locked out after four invalid logon attempts.

14 Access logs and record keeping

14.1 The Supplier shall implement the following audit procedures:

(a) audit logging;

(b) monitoring; and

(c) alerting

to ensure that any action which takes place in the Technical Solution or which is effected by an individual or other person is logged and can be proven to have taken place.

15 Business continuity and disaster recovery

15.1 The Supplier shall back-up all AG Data in accordance with agreed service levels, to ensure security of the AG Data and the uninterrupted provision of the Services.

15.2 The Supplier shall implement and maintain appropriate and adequate business continuity arrangements that comply with:

(a) Best Industry Standards; and

(b) ISO22301 or equivalent

that detail agreed Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Incident response plans shall involve impacted clients and other critical business relationships.

15.3 The Supplier shall:

(a) test the business continuity measures on a regular basis and in any event not less than annually or upon significant organisational or environmental changes;

(b) record the test results; and

(c) make the test results available to AG upon request.

15.4 The Supplier shall develop and implement adequate disaster recovery arrangements that;

(a) ensure the agreed RTOs and RPOs can be achieved; and

(b) take account of the AG critical functions and processes supported by the Services; and

(c) take account of all interdependencies within the Technical Solution, both internal, within the Supplier IT System and external between the Supplier IT System and any third party electronic environment.

15.5 The Supplier shall:

(a) test the disaster recovery arrangements on a regular basis and in any event not less than annually;

(b) record the test results; and

(c) make the test results available to AG on request.

15.6 The Supplier shall ensure that availability, quality, and adequate capacity and resources are planned, prepared, and measured to deliver the required system performance in accordance with Relevant Law. The Supplier shall make projections of future capacity requirements to mitigate the risk of system overload.

16 Asset management

16.1 The Supplier shall ensure it has a clear complete understanding and a written record of the type of AG Data being Handled as part of the Services. Supplier shall keep a comprehensive record of the names of the AG IT Systems being used in the provision of the Services.

16.2 The Supplier shall classify and handle the AG Data in accordance with requirements set out by AG, including:

(a) establishing policies and procedures for the labelling, handling, and security of data and objects which contain data; and

(b) implementing mechanisms for label inheritance for objects that act as aggregate containers for data.

16.3 The Supplier shall ensure that, when no longer needed for bona fide business purposes, or as required by Relevant Law or pursuant to contractual obligations, or as requested by AG, AG Data within the Supplier IT System or otherwise in its possession or under its control (which shall include being under the control of Sub-contractors pursuant to the Technical Solution):

(a) that is stored electronically, is securely and permanently deleted/erased and/or destroyed so that such AG Data is not recoverable; and

(b) which comprises hardcopy materials, are cross-cut shredded, incinerated, or pulped.

16.4 The Supplier shall provide to AG, five (5) business days in advance of the termination or expiry of the Contract, a copy of all AG Data at no cost to AG. All structured and unstructured data shall be available to AG in an industry-standard format (e.g. doc, xls, pdf, logs, and flat files).

16.5 The Supplier shall, within five (5) business days of providing AG with a copy of all AG Data pursuant to paragraph 16.4 of this ISMR, dispose of all AG Data in accordance with paragraph 16.3 of this ISMR.

16.6 The Supplier shall establish policies and procedures with supporting business processes and implement technical measures for the secure disposal and complete removal of AG's data from all storage media, ensuring data is not recoverable by any computer forensic means.

16.7 The Supplier shall, upon request by AG, provide evidence acceptable to AG that AG Data has been permanently and securely destroyed in compliance with paragraph 16.3 of this ISMR.

I. AG SITE HEALTH AND SAFETY RULES

1 Introduction

1.1 The Supplier shall establish a baseline and adhere to Law and relevant standards and best practices.

2 Pre-Qualification and Selection

The Supplier shall provide:

(a) a copy of the Supplier's Health and Safety Policy, aligned with company values and legal requirements;

(b) copies of liability insurances (must include public liability);

(c) confirmation and certification of any health and safety accreditations e.g. ISO45001;

(d) copies of any competency qualifications e.g. CHAS, SafeContractor, BAFE etc; and

(e) risk assessments and method statements (RAMS) specific for the task being undertaken.

3 Before Work

(a) Implementation of safe systems of work by the Supplier.

The Supplier shall:

(i) fully assess the risk associated with the works;

(ii) provide all necessary tools and equipment to carry out the works; and

(iii) assign and provide competent persons and supervision to complete the works.

(b) Proper Use of Supplier Tools and Equipment

The Supplier shall ensure that:

(i) the correct tools and equipment are used, and that these are operated by appropriately licensed and trained operators; and

(ii) all equipment is properly maintained, with maintenance records kept.

(c) Personal Protective Equipment

The Supplier shall issue its personnel with appropriate PPE and ensure they are appropriately trained on its correct usage.

(d) Housekeeping

The Supplier shall ensure that the general work area is kept well maintained.

3.2 The Supplier shall ensure that AG and the Supplier have agreed and understand the applicable incident notification procedures and investigation process between AG and the Supplier.

3.3 The Supplier shall ensure that hazardous materials are either not used or, if required to be used, that their use is minimised and that they are stored, applied, and removed from the site in accordance with COSHH regulations.

4 During Work

4.1 Onsite, the Supplier shall comply with, address, and participate in the following:

(a) Compliance to AG's Health & Safety Management System.

(b) Compliance to site specific rules and local regulations.

(c) AG will meet the Supplier on arrival, at site, and sign them in.

(d) The Supplier shall conduct a site safety induction prior to commencing works .

(e) The Supplier shall Maintain good workplace conditions.

(f) The Supplier shall identify the responsible person onsite and ensure a daily brief is conducted and report concerns or unsafe conditions.

(g) When required, AG will issue a Permit to Work (PTW).

(h) The Supplier shall have a copy of their RAMS with them onsite.

(i) The Supplier shall ensure effective control of any dust or fumes generated.

(j) The Supplier shall ensure that noise is kept to a minimum.

(k) The Supplier shall implement all necessary measures to manage and mitigate any risks associated with asbestos exposure. If asbestos is suspected or identified, the Supplier shall immediately cease work and promptly notify the appropriate AG contact.

(l) AG may perform periodic inspections and audits of the Supplier to ensure compliance with contractual requirements.

(m) The Supplier shall participate in health and safety meetings.

(n) The Supplier shall respond to improvement action notifications.

(o) The Supplier shall comply with health and safety instruction.

5 Completion of Work

5.1 The Supplier shall coordinate the final inspection and approval of the works with the AG representative.

5.2 The AG representative may conduct a performance appraisal to assess whether the Supplier has complied with these requirements.

6 Disclaimer

6.1 These instructions and procedures are not intended to override any applicable legal requirements or Health and Safety Executive guidelines. Should any conflicts arise, please address them with AG's representative.

J. DEFINITIONS USED IN THIS DOCUMENT

Addleshaw Goddard, **AG**, **AG Entity**, **we** or **our** means any one or more of the entities comprising:

(a) Addleshaw Goddard LLP, a limited liability partnership registered in England and Wales (No. OC 318149) whose registered office is at Milton Gate, 60 Chiswell Street, London EC1Y 4AG (**AG LLP**)

(b) any entity owned or controlled by AG LLP or its members or any entity owned or controlled by any other AG entity,

(c) AG LLP's affiliated firms, and

(d) any other partnership, entity or practice authorised to use the name "Addleshaw Goddard"

Law means any legislation, enactment, statute, regulation, by-law, ordinance or subordinate legislation in force from time to time in any jurisdiction to which a party is subject, the common law as applicable to the parties from time to time, any binding court order, judgment or decree, and all applicable statutory, industry, regulatory, supervisory or other rules, codes, guidance, regulations, instruments and provisions in force from time to time

Representative means the Supplier's personnel, and its suppliers, agents, and subcontractors who form part of its supply chain, and their respective personnel

Supplier or **you** or **your** means the person supplying, or wishing to supply, goods or services to AG

The words, **includes**, **including**, **for example**, **such as**, **in particular** and similar phrases do not limit the generality of any words preceding them. Any words which follow them shall not be construed as being limited in scope to the same class as preceding words, where a wider construction is possible

Document Information	
Document owner:	Head of Procurement
Approved by:	Head of Procurement
Last updated:	21 July 2025
Next review date:	July 2026
You can find previous versions of this document here: https://www.addleshawgoddard.com/globalassets/policies/procurement-supplier-policy-previous-version.pdf