ONBOARDING AGREEMENT (MAIN TERMS)

EFFECTIVE DATE:

PARTIES:

a) Williams Lea Limited, a company incorporated in England and whose company number is 02119266 and registered address is Darwin house, Leeds valley park, Savannah way, Leeds, LS10 1AB, England (the "**Company**)

b) a company incorporated and registered in whose company number is and having its registered address

, (the **"Supplier"**) Each a **Party**, together the **Parties.**

TERMS AND CONDITIONS
("Terms")

MAIN TERMS

1. Background

1.1. These Terms govern the relationship between the Company and the Supplier as it relates to the procurement by the Company from the Supplier of goods and/or services.

1.2. The Agreement comprises these Main Terms together with any Appendices applicable to the goods and/or services being delivered by the Supplier. The Appendices are attached to this Agreement and are incorporated by reference into its terms and conditions. The Supplier's appointment is strictly on a non-exclusive basis and subject to the Supplier passing the Company's Vetting Process (in accordance with Appendix 7) unless the Company states otherwise in writing.

2. Definitions

2.1. The following terms have the meanings set out alongside them:

"**Agreement**"	means this onboarding agreement including all Appendices together with the contents of the Purchase Order;
"**Applicable Law**"	means laws, rules, regulations, regulatory guidance, regulatory requirements and any form of secondary legislation, resolution, policy, guideline, concession or case law of the relevant jurisdiction from time to time and relevant to the provision, receipt or use of the Goods and/or Services or relevant to the business of the Company or a member of the Company's Group;
"Applicable Software"	means the software "Colour Lab" or any other applicable colour quality and management software provided by the Company from time to time;
"**Approved Subcontractor**"	means a subcontractor of the Supplier (if any) that has been approved in writing by the Company, at the Company's sole and unfettered discretion;
"**Authorised Users**"	means those employees, agents, clients and customers, suppliers and independent contractors of the Company and of the Client and/or other person nominated by the Company or the Client who are authorised to use the Software through the Services under these Terms;
"**Business Activities**"	the Supplier's supply to the Company of the Goods and/or Services;

"**Business Day**"	means a day other than a Saturday, Sunday or public holiday in England when banks in the city identified in the Particulars are open for business;
"**Business Hours**"	means 09:00hrs – 18:00hrs or the times during which the Supplier is otherwise open for business as notified to the Company in writing ;
"**Client**"	means a customer of the Company from time to time that has a requirement for the Goods and/or Services as part of its business operations;
"Company"	means and includes Williams Lea's, parent, group, affiliate, associated and or subsidiary companies that may also enjoy the benefit of this Agreement in their individual capacities.
"**Confidential Information**"	means all information of whatever nature (including any copies made of that information) however disclosed whether directly or indirectly including, any Intellectual Property Rights, documents, artwork, data, ideas, flowcharts, computer programs, specifications, plans, drawings, pricing, usage information and includes without limitation all and any financial, technical, commercial, marketing or product information of the Company, any member of its Group, any of the Company's Group's partners, clients, prospective clients, suppliers, prospective suppliers, data processes, specifications; drawings; designs; computer software; know-how; trade secrets; customer lists and prospective customer lists, supplier lists, prospective supplier lists; pricing and sales policies; manuals; business plans, forecasts and business opportunities or ventures being considered or pursued; intellectual property details including but without limitation artwork and brands; plans, designs, computer files, software and formulae; research that is being carried on into any products; network sensitive information; and any other material bearing or incorporating Confidential Information and whether disclosed visually, orally, or in the form of drawings, recordings, written material, or computer software, information relating to marketing or clients and customers or suppliers, or information relating to market opportunities and business affairs, the Company and its Group's Data, Personal Data; the Company's policies; Work Product; or other information marked as or which by implication is confidential or information of a competitive nature relating to a Party, the Company's Group, clients and suppliers;
"**Colour Quality Programme**"	the Company's colour quality assurance program containing modules, which includes the Applicable Software;
"**Commencement Date**"	means the date specified in the Purchase Order upon which the Supplier begins to provide the Services;
"**Company Data**"	means the data inputted by the Company, Authorised Users, or the Supplier on the Company's behalf for the purpose of using the Services or facilitating the Company's use of the Services;
"**Company System**"	means computer hardware, firmware, middleware, protocols and software and other hardware, peripheral equipment, networks, communications systems and other equipment of whatever nature belonging to or under the control of the Company, a Client or a Company customer or supplier;
"**Documentation**"	means the document(s) made available to the Company by the Supplier which sets out a description of the Services along with any user instructions (where relevant);
"**Fees**"	means the fees set out in the any Purchase Order;

"**Force Majeure**"	has the meaning set forth in Clause 7.1;
"**Goods**"	means the goods/items set out in any Purchase Order issued under this Agreement;
"**Good Industry Practice**"	means the use of the standards, practices, methods and procedures the exercise of the skill, care, diligence, prudence, foresight and judgment which would be expected from a skilled, qualified and experienced person or body engaged in a similar undertaking under similar circumstances seeking in good faith to comply with their obligations;
"Group Company"	means any subsidiary or holding company from time to time of the Company, and any subsidiary from time to time of a holding company of the Company (and for the purposes of these Terms the phrases "subsidiary" and "holding company" shall be construed in accordance with section 1159 of the Companies Act 2006);
"**Intellectual Property**" or "**Intellectual Property Rights**"	means patents, rights to Inventions and Works, current and future copyright and related rights, trade-marks, trade names and domain names, rights in get-up, rights in goodwill or to sue for passing off, rights in designs, rights in computer software, database rights, rights in Confidential Information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications (or rights to apply) for, and renewals or extensions of, such rights and all similar or equivalent rights or forms of protections which may now or in the future subsist in any part of the world;
"**Inventions**"	means inventions, ideas and improvements, whether or not capable of being registered as an Intellectual Property Right, and whether or not recorded in any medium;
"**Late Payment Fee**"	means the fee equal to 1% of the overdue fee owed by the Company to the Supplier;
"**Maintenance Window**"	means the period of time during which the Supplier shall carry out planned maintenance services;
"**Material Adverse Event**"	means any event outside of either party's control which results in: (i) a substantial adverse impact on a party's ability to perform the agreement in accordance with its terms and the law; and/or (ii) an increase in the costs incurred by a party in performing the Agreement of at least + or -5% since the price for the Services was last agreed;
"**Open Source Software**"	means software licensed under terms which require, as a condition of use, modification or distribution of such software or other software incorporated into, derived from or distributed with such software, the granting of a royalty-free licence to any person or the making available of the source code for such software to any person;
"**Poor Service**"	means an inadequate level of Services that entitles the Company to terminate the Agreement;
"**Purchase Order**"	means any document governed by and issued pursuant to this Agreement which serves as a requisition for Services from the Supplier;
"**Service Credits**"	means service credits payable in accordance with a Purchase Order;
"**Service Failure**"	means any failure by the Supplier to deliver any Services in accordance with the Service Levels;
"**Service Levels**"	means the service levels applicable to the delivery of the Services;
"**Services**"	means the services described in a Purchase Order;
"**Software**"	means the solution and online software applications provided by the Supplier as part of the Services as described in Appendix 2 and/or the applicable Purchase Order;

"**Software Services**"	means the software support and/or maintenance services as described in the Purchase Order;
"**Supplier Account Manager**"	means the member of Supplier Personnel identified by the Supplier to the Company as such in writing;
"**Supplier Permitted Locations**"	means the locations (if any) specified in the relevant Purchase Order for providing the Services and Software Services (as applicable);
"**Supplier Personnel**"	means all employees, staff, other workers, agents and consultants of the Supplier and of any Approved Subcontractors who are engaged by the Supplier from time to time to meet its obligations under these Terms;
"**User Subscriptions**"	means the user subscriptions purchased by the Company pursuant to these Terms which entitle Authorised Users to access and use the Software Services and the Documentation in accordance with these Terms;
"**Virus**"	means any form of computer code whether known or unknown, including "electronic possession", "logic bombs" "viruses", "Trojan horses", "worms", "spyware", "malware", and "adware" (such expressions shall have meanings as they are generally understood within the computing industry), which could, in any way, disable, disrupt, harm, impede or modify the performance or functionality of all or any part of any system, program, equipment, network or data;
"**Company**"	means (i) with respect to these Terms, the legal entity entering into these Terms as stated in the Particulars; and (ii) with respect to a Purchase Order, any Group Company which enters into that Purchase Order;
"**Work Product**"	means an output or deliverable of the Services arising from the Company's or its Authorised Users' use of the Services; and
"**Works**"	means all records, reports, documents, papers, drawings, designs, transparencies, photos, graphics, logos, typographical arrangements, software, and all other materials in whatever form, including but not limited to hard copy and electronic form.

3. Interpretation

3.1 In these Terms, references to Clauses, Schedules, Annexes and Purchase Orders are to the clauses, schedules, of these Terms; references to paragraphs are to paragraphs of the relevant schedule to these Terms; a person includes an individual, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors or permitted assigns; a reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established; unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular; unless the context otherwise requires a reference to one gender shall include a reference to the other genders; a reference to writing shall not include email, unless otherwise stated; a reference to a statute or statutory provision is a reference to it as it is in force as at the date of these Terms; a reference to an obligation on the Supplier shall also be construed to mean an obligation to procure the Supplier Personnel's compliance with such obligation and a reference to a "third party" means a person that is not a Party or a Group Company.

3.2 In the event of any conflict between the provisions contained in these Terms and the Appendices, the following order of precedence shall apply:

3.2.1 these Main Terms, together with Appendices 5, 6,6A and, 7;

3.2.2 any other selected Appendix.

4. Services and Fees

4.1 Subject to the Supplier's provision of the Goods and/or Services (as applicable) in accordance with these Terms, the Company shall pay the undisputed part of any Fees to the Supplier **within sixty (60) days** after receipt of a correct and valid invoice. Where the Company identifies reasons to dispute an invoice or specific amounts therein, the Company shall notify Supplier promptly in writing, setting out such reasons. In the event that the invoices remain disputed for a period of 60 days from the date that the Company first raised the applicable dispute, the Parties shall refer such dispute to the Escalation Procedure set out in Clause 26.

4.2 The Supplier's invoices must be complete and include the correct details, in accordance with Appendix 8 otherwise they will be returned, and payment will be delayed.

4.3 If any undisputed Fees remain unpaid 60 days after the due date pursuant to Clause 4.1 and the Escalation Procedure described in Clause 26 has been completed, the Supplier may suspend the provision of the Services in respect of the Purchase Order to which the outstanding Fees relate. The Supplier's remedies under this Clause 4.3 are the Supplier's sole and exclusive remedy for delayed payment.

4.4 The Company reserves the right to refuse payment of any invoices which are submitted more than six months after the specific provision of the Software, the Services or Software Services that the applicable invoice relates to were performed, or that were otherwise submitted in non-compliance with Clause 4.2.

4.5 If, upon examination at any time, the Company determines that any charges, prices, costs or expenses exceed the amounts properly chargeable to, or recoverable from, the Supplier shall, within 7 days refund to the Company the amount over-charged plus interest at the applicable statutory rate.

4.6 Subject to Appendix 1 if incorporated, the Fees shall remain fixed during the Term. The Fees are inclusive of all travel, subsistence and other incidental expenses incurred by the Supplier and the Supplier Personnel in respect of the provision of the Services. The Supplier shall only be permitted to charge for expenses if expressly authorised to do so in the applicable Purchase Order and provided that the Company's prior written consent has been obtained by the Supplier prior to the relevant expenses being incurred.

4.7 If Value Added Tax (VAT) is applicable:

4.7.1 the Supplier's invoice shall comply with all the requirements of Article 226 of the European Union Council Directive 2006/112/EC. the Company shall not be required to pay any invoice which fails to meet the requirements of Article 226 referred to above; and

4.7.2 the Services provided by the Supplier shall be taxable where the Company is established, according to the terms of Article 56.1 (c) of the European Union Council Directive 2006/112/EC.

4.8 If any Service Credits have been issued by the Supplier between invoices rendered by the Supplier, the Supplier shall reduce the Fees charged in the later invoice by an amount equal to the value of the Service Credits.

4.9 The Company may set off sums due to the Supplier. The Supplier may not set off sums due from the Company to it under these Terms against sums due from it to the Company.

5. Confidentiality

5.1. Where the Company is required to disclose Confidential Information to the Supplier, such disclosure shall be in accordance with the provisions of this Clause 5.

5.2. The parties agree that the Company shall disclose such Confidential Information as it deems necessary or useful in furtherance of the Business Activities.

5.3. The Supplier undertakes for a period of five (5) years from the date of disclosure or such other period as specified by the Company to:

5.3.1. not, without prior written consent of the Company, disclose any such Confidential Information to any person or body other than its employees, agents, professional advisors or sub-contractors ("**Representatives**") on a need to know basis relating to the Business Activities, to treat such Confidential Information as confidential, secret, take all necessary precautions to effect and maintain, to the highest standards, security measures to safeguard such Confidential Information from unauthorised use and prevent its unauthorised, negligent or inadvertent disclosure and not use, copy, reproduce or reverse-assemble such Confidential Information only for the Business Activities provided if specified by the Company in writing, and never for his/her/its personal gain;

5.3.2. bring to the immediate attention of the Company any known or suspected breaches of its obligations under these Terms; and

5.3.3. execute such documents or agreements that the Company may require from time to time in respect of the Confidential Information.

5.4. The Confidential Information shall remain the property of the Company at all times and no licence in the Intellectual Property is either granted or implied, nor any trade mark, patent, copyright or other intellectual property right by the conveying of Confidential Information to the Supplier. No Confidential Information disclosed shall constitute any representation, warranty, assurance, guarantee or inducement by the Company, in particular with respect to its accuracy, completeness nor the non-infringement of trademarks, patents, copyrights or other intellectual property right, or other rights of third parties.

5.5. In terms of any Intellectual Property Rights in any Works and/or Inventions created by the Supplier in the provision of the Services to the Company, the Supplier:

5.5.1. shall promptly disclose to the Company or its group companies all works including, without limitation, all inventions and/or works embodying Intellectual Property Rights originated, conceived, developed, written or made by the Supplier whether alone or with others during the Supplier's engagement with the Company which relate, or could relate, to the business of the Company or its group companies (as applicable) and shall (to the extent that they do not automatically vest in the Company or its group companies (as applicable) by operation of law) hold them in trust for the Company or group companies until such rights have been fully and absolutely vested in the Company or its group companies (as applicable);

5.5.2. agrees to waive any moral rights in the Inventions and Works to which it (or any of its staff) is now or may at any future time be entitled under Chapter IV of the Copyright Designs and Patents Act 1988 or any similar provisions of law in any jurisdiction, including (but without limitation) the right to be identified, the right of integrity and the right against false attribution, and agrees not to institute, support, maintain or permit any action or claim to the effect that any treatment, exploitation or use of such Works or Inventions or other materials, infringes the Individual's moral rights;

5.5.3. agrees that the Company shall (without limitation) be entitled to make such additions to, deletions from or alternatives to or adaptations of any of the Inventions and Works;

5.5.4. acknowledges that, except as provided by law, no further remuneration or compensation other than that provided for in these Terms is or may become due to the Supplier (or any of its employees) in respect of the performance of the obligations under this Clause;

5.5.5. agrees to (at any time during or after the provision of such services) do all acts necessary to confirm that absolute title in all Intellectual Property Rights in the Inventions and Works has passed, or will pass, to the Company including but not limited to executing all documents, making all applications and do all acts and things as may, in the opinion of the Company be necessary or desirable to vest the Intellectual Property Rights in, and to register them in, the name of the Company and to defend the Company against claims that works embodying Intellectual Property Rights or Inventions and Works infringe third party rights, and otherwise to protect and maintain the Intellectual Property Rights in the Inventions; and

5.5.6. grants an irrevocable power of attorney to the Company to be the Supplier's attorney in the Supplier's name and on his/her/its behalf to execute, sign all such deeds or instruments and do all things and to generally use his/her/its name for the purpose of giving to the Company or his/her/its nominee the full benefit of the provisions of this Clause 5, and the Supplier acknowledges in favour of a third party that a certificate in writing signed by any authorised signatory of the Company that any instrument or act falls within the authority conferred by this Clause 5 shall be conclusive evidence that such is the case.

5.6. The Supplier shall not:

5.6.1. make or permit others to make any reference to the disclosing or receiving of the Confidential Information or use the name or branding of the Company or any Client in any public announcements, promotional, marketing or sales materials without the prior written consent of the Company; and

5.6.2. from the date of these Terms and for a period of six (6) months after the date upon which these Terms expires, without the prior written agreement of the Company, offer employment to, enter into a contract for the services of, or attempt to entice away from the Company any individual who is at the time of the offer and was during the Supplier's engagement, an employee, or an officer of the Company, or procure or facilitate the making of any such offer or attempt by any other person (other than by means of an advertising campaign for genuine vacancies open to all comers and not specifically targeted at such employees or officers of the Company).

5.7. Unless the Company has agreed otherwise in writing, upon completion of the purpose for which Confidential Information has been disclosed, the Supplier shall either return or destroy (as the Company may elect) any Confidential Information and all copies made of it within fourteen (14) days of a request for the same by the Company. If the Company asks the Supplier to destroy the Confidential Information, the Supplier at its own cost must provide a confirmation declaration, signed by one of its directors, confirming that such destruction has been completed in accordance with these Terms.

5.8. The Supplier acknowledges and understands that the Confidential Information is of great value and importance to the success of Company business. Any unauthorised use or disclosure of the Confidential Information would cause serious and irreparable injury to the Company. Money damages may not be a sufficient remedy for a breach of these Terms and the Company is entitled to specific performance and/or injunctive or other equitable relief and remedies for such breach, without the necessity of showing any irreparable injury or special damages.

6. Termination

6.1. The Company may terminate these Terms and/or any Purchase Order in whole or in part at any time and for convenience without penalty upon serving thirty (30) days' written notice to the Supplier.

6.2. All individual Purchase Orders shall terminate immediately upon termination or expiry of these Terms, unless otherwise agreed in writing between the Parties. In the event of agreement between the Parties that a particular Purchase Order shall survive these Terms, they shall continue in full effect to govern that Purchase Order for the remainder of the Term of that Purchase Order.

6.3. If the Company determines that the Supplier has committed a Relevant Breach (as defined below), the Company may immediately upon giving written notice to the Supplier (at its option) and without liability:

6.3.1. terminate these Terms; and/or

6.3.2. terminate only the Purchase Order in respect of which the Relevant Breach has occurred.

6.4. For these purposes below a "**Relevant Breach**" is one or more of the following. The Supplier has:

6.4.1. committed a material breach of these Terms (if such material breach has not been remedied within a period of ten (10) Business Days of a request from the Company to remedy it);

6.4.2. committed material breach of these Terms, which is not capable of remedy;

6.4.3. not complied with any remediation plan agreed in writing between the Parties;

6.4.4. provided Poor Service;

6.4.5. contravened Clause 23.3; or

6.4.6. failed to comply with Clause 5 and or Appendix 5 and or Appendix 6 and or Appendix 6A.

6.5. Either Party may terminate these Terms upon giving written notice to the other:

6.5.1. upon the other Party passing a resolution for winding up (save for the purposes of amalgamation or reconstruction where the successor to the Party agrees to adhere to these Terms) or suffering a winding-up order being made against it; or

6.5.2. if the other Party is generally unable to pay its debts or ceases or threatens to cease to carry on its business; or

6.5.3. within six (6) months of distress or execution being levied against any property of the other Party; or

6.5.4. if the other Party claims Force Majeure and the period of the Force Majeure has lasted longer than thirty (30) days.

6.6. On termination of these Terms and/or any Purchase Order for any reason:
6.6.1. all licences granted under these Terms or the applicable Purchase Order shall immediately terminate unless expressly agreed otherwise;
6.6.2. each Party shall return and make no further use of any equipment, property, Documentation and other items (and all copies of them) belonging to the other Party;
6.6.3. the Supplier shall,
6.6.3.1. in respect of the terminated Purchase Orders, immediately deliver up to the Company the Company Data and all other relevant data in its most recent form (whether or not backed up) and all other property of the Company then in its possession at no additional cost; and
6.6.3.2. return any amounts pre-paid by the Company to the Supplier for the future provision of the Services which would have been provided but for the termination of these Terms or the applicable Purchase Orders; and
6.6.4. any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of these Terms which existed at or before the date of termination shall not be affected or prejudiced.
6.7. If a Material Adverse Event occurs, the impacted party may:
6.7.1. require the other party to negotiate in good faith an amendment to the Agreement to alleviate the Material Adverse Event; and
6.7.2. if no such amendment is made to the Agreement within 30 days, terminate the Agreement by giving the other party not less than 30 written notice. On termination under this clause, clause 6.6 shall apply.

7. Force Majeure

7.1. Without prejudice to Clause 11, neither Party will be liable for delay or failure in performing obligations if the delay or failure resulted from circumstances beyond its reasonable control (such circumstances hereinafter referred to as "**Force Majeure**"), including but not limited to: acts of God, governmental acts (other than the exiting of a European Union member state from the European Union), flood, fire, explosion, accident, civil commotion, and impossibility of obtaining materials. For the avoidance of doubt, the Company shall not be required to pay for any non-provision of Services as a result of the Force Majeure and any Fees charged in connection for such non- provided services shall either be waived, reimbursed or credited to the Company (at the Company's direction).
7.2. The Party whose performance is affected by Force Majeure shall:
7.2.1. upon becoming aware of same give notice forthwith in writing to the other Party, together with documentary evidence; and
7.2.2. use all reasonable endeavours to resolve the condition or to provide temporary workarounds or alternative solutions.
7.3. Force Majeure shall not be deemed to include any failure by a third party to perform its obligations to one of the Parties, unless agreed otherwise or unless the relevant Party shows that the non-performance of that third party was due to Force Majeure.

8. Relationship between the Parties

8.1 The relationship of the Supplier (and the Supplier Personnel) to the Company shall be that of independent contractor and nothing in these Terms shall render it (nor the Supplier Personnel) an employee, worker, agent or partner of the Company and the Supplier shall not hold itself out as such and shall procure that the Supplier Personnel do not hold themselves out as such. The Supplier shall have no right, power or authority to act as agent for the Company for any purpose and shall not enter into any contract or make any warranty or representation as to any matter or create any obligation, express or implied, or make any representation on behalf of the Company or any Client; or any authority to incur any expenditure in the name of or for the account of the Company.

9. Vetting

9.1. Where appropriate to the services the Company shall conduct vetting on the Supplier in accordance with Appendix 7. The Supplier acknowledges and warrants that its personnel consent to the Company (and its suppliers) processing their Personal Data solely for the purposes of the delivery of any Goods and/or Services pursuant to this Agreement.

10. Audit of Supplier's Performance

10.1. The Supplier shall forthwith following receipt of written notice from the Company, allow and/or procure the Company and any auditors of, or other advisers to the Company, to access the Supplier's premises or business premises of any Supplier Personnel at which the Supplier or Supplier Personnel holds any the Company Data or the Company's Confidential Information relating to the Services and to access such personnel and relevant records specifically relating to the Services provided herein, as may be reasonably required in order to:
10.1.1 fulfil any request from any regulatory authority or made by virtue of any Applicable Law; and
10.1.1.1. verify that:
10.1.1.1.1. any amounts payable pursuant to these Terms are accurate or identify suspected fraud;
10.1.1.1.2. the Services are being provided in accordance with these Terms (including any Appendices or Addenda);
10.1.1.1.3. the Supplier's systems protect the integrity, operational availability, confidentiality and security of the Company's Confidential Information and data; and
10.1.1.2. ensure compliance with the Supplier's obligations under Clause 5, Appendix 5 and or Appendix 6 and or Appendix 6A, and or Appendix 7
10.1.1.3. where the Services include Software or IT related Services, ISO 20000; and subject to the Company's

obligations of confidentiality, provide the Company (and its auditors and other advisers) with all reasonable co-operation, access and assistance in relation to each audit.

10.2. The Company shall use reasonable endeavours to ensure that the conduct of each audit does not disrupt the Supplier or delay the provision of the Services by the Supplier and provide at least ten (10) Business Days' notice of its intention to conduct an audit unless such audit is conducted in respect of a suspected fraud, in which event no such notice shall be required.

10.3. The Parties shall bear their own costs and expenses incurred in respect of compliance with their obligations under this Clause 10, unless the audit identifies a material default by the Supplier in complying with its obligations under these Terms, in which case the Supplier shall reimburse the Company for all reasonable costs and expenses incurred in the course of the audit.

10.4. If an audit identifies that the Supplier is failing to comply with any of its obligations under these Terms then, without prejudice to the other rights and remedies of the Company, the Supplier shall take the necessary steps to comply with its obligations at no additional cost to the Company within ten (10) Business Days of written notice from the Company, or the Company has overpaid any Fees payable under these Terms, the Supplier shall pay to the Company the amount overpaid within ten (10) Business Days from the date of receipt of an invoice or notice to do so.

10.5. Notwithstanding Clause 5 (Confidential Information), the Supplier hereby agrees that in respect of documents relating to the audit including audit results ("**Audit Documentation**") the Company has the right to share any such Audit Documentation with its relevant Clients subject always to the Client complying with confidentiality obligations substantially similar to those set out in these Terms.

10.6. This Clause shall survive termination of these Terms, however arising, for a period of up to six (6) years following the date of termination of these Terms.

11. Disaster Recovery and Business Continuity

11.1. The Supplier undertakes that it has and shall continue to have in place and keep up-to-date disaster recovery plans and business continuity plans and processes in accordance with the minimum standards prescribed from time to time by Applicable Law and without limiting the generality of the foregoing, in accordance with Good Industry Practice.

12. Liability

12.1. The following provisions set out the entire financial liability of the Parties (including liability for the acts or omissions of their employees, agents and sub-contractors) in respect of any breach of these Terms and any representations, statements or tortious acts or omissions including negligence arising under or in connection with these Terms.

12.2. The Supplier does not limit its liability (if any) in respect of any of the following:

12.2.1. fraud or fraudulent misrepresentation;

12.2.2. the death of, or personal injury to, any person caused by negligence;

12.2.3. any losses caused by the Supplier's wilful misconduct or intentional default;

12.2.4. any loss of the Company Data; and

12.2.5. causes of action brought under Clause 23 (Infringement of Third Party Rights),

12.3. Subject to Clause 12.2 above:

12.3.1. the total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation or otherwise for either Party arising in connection with the performance or contemplated performance of the Services shall be limited to 125 per cent of the total value of the sums paid or payable under these Terms or £1,000,000 (one million pounds sterling) whichever is the greater; and

12.3.2. neither Party shall be liable to the other for any indirect or consequential loss or damage (including loss of business, loss of profit, or loss or depletion of goodwill (howsoever caused)) which arise out of or in connection with these Terms. The Parties agree that the following losses are deemed as direct losses:

12.3.2.1. loss of profits, loss of reputation, loss of goodwill, loss of contracts, loss of business opportunity or loss of revenue;

12.3.2.2. the cost of selecting, procuring, implementing and operating any alternative or replacement systems or services whether internally or through or with a third party;

12.3.2.3. reasonable administrative costs (including but not limited to postage) and management time incurred by the Company; and

12.3.2.4. the cost of additional checks relating to security breaches.

12.4. For the avoidance of doubt, the Company entity that is party to the applicable Purchase Order is solely responsible for its acts and/or omissions under such Purchase Order and no Group Company shall otherwise be liable to the Supplier in connection with such Purchase Order.

13. Insurance

13.1. The Supplier shall:

13.1.1. at all times be insured on an each and every claim basis (but without limiting its obligations and responsibilities under these Terms), with a reputable insurer, against all liabilities for which it is able to insure under these Terms, including without prejudice to the foregoing:

13.1.1.1. public liability insurance for a minimum amount of cover of £5 million (five million pounds sterling);

13.1.1.2. products liability insurance for a minimum amount of cover of £5 million (five million pounds sterling);

13.1.1.3. employers' liability insurance for a minimum amount of cover of £5 million (five million pounds sterling);

13.1.1.4. property insurance for a minimum amount of cover of £2 million (two million pounds sterling); and

13.1.1.5. professional indemnity liability insurance for a minimum amount of cover of £5 million (five million pounds sterling);

13.1.2. provide all facilities, assistance and advice required by the Company or its insurers for the purpose of contesting or dealing with any action, claim or matter arising out of the Supplier's performance, or purported performance of, or failure to perform, these Terms;

13.1.3. maintain such insurance whilst these Terms is in force and for a period of twelve (12) months after termination or expiry of these Terms (howsoever arising) and shall do nothing to vitiate such insurance; and

13.1.4. upon request furnish the Company with proof of cover of the above insurance, through the provision of valid certificates of insurance.

14. Severability

If any provision of these Terms is held invalid, illegal, or unenforceable for any reason, such provision shall be severed and the remainder of the provisions hereof shall continue in full force and effect as if these Terms has been executed with the invalid provision eliminated.

15. Waiver

No single or partial exercise of, or failure or delay by a Party to exercise any right or remedy provided under these Terms or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy.

16. Cumulation of Remedies

Subject to the specific limitations set out in these Terms, no remedy conferred by any provision of these Terms is intended to be exclusive of any other remedy except as expressly provided for in these Terms and each and every remedy shall be cumulative and shall be in addition to every other remedy given hereunder or existing at law or in equity by statute or otherwise.

17. Whole Agreement

These Terms (including all Appendices and any document specifically referred to herein) form the entire agreement between the Parties and any other terms and conditions included in or specified by any other document exchanged between the Parties are fully excluded.

18. Amendment

These Terms may only be amended by written agreement of the Parties.

19. Notices

19.1. Notices hereunder shall be validly given if delivered by hand or post (recorded delivery) to the address identified in the Parties Clause and deemed to have been served if delivered by hand at the time of delivery and if posted: before 5 pm, on the next Business Day. or after 5 pm, on the second Business Day afterwards.

20. Publicity

20.1. Except with the prior written consent of the Company, which the Company may withhold in its absolute discretion, the Supplier shall not:

20.1.1. make any press announcements regarding the arrangements agreed between the Parties, or any Client; or

20.1.2. otherwise publicise these Terms or any part hereof in any way; or

20.1.3. refer to its role hereunder in any market material or presentations whatsoever, whether as a site reference or otherwise.

20.2. The Company shall be entitled to recover from the Supplier any expenses it has incurred arising from or incurred by it enforcing the compliance by the Supplier of Clause 20.1.

21. Assignment and Subcontracting

21.1. Subject to Clause 21.3, neither Party may assign or transfer these Terms in whole or in part without the other Party's prior written consent.

21.2. The Supplier shall not subcontract these Terms in whole or in part to any third party unless prior written authorisation is provided by the Company and it remain responsible for the acts and omissions of any Approved Subcontractor as if such acts and omissions were deemed to be those of the Supplier.

21.3. The Company may assign or novate its rights and obligations under these Terms to a Group Company or a legal entity established or authorised to take over and operate on a continuing basis all or the relevant parts of its business and Supplier shall enter into such documents as are reasonably necessary for this purpose.

21.4. These Terms are binding on and shall vest to the benefit of the Parties, their successors in title and permitted assigns.

22. Third Party Rights

These Terms do not confer any rights on any person or party (other than the Parties to these Terms and, where applicable, their successors and permitted assigns) pursuant to the Contracts (Rights of Third Parties) Act 1999 other than in respect of any Group Company.

23. Infringement of Third-Party Rights

23.1. The Supplier shall fully indemnify and keep indemnified the Company (and for the avoidance of doubt any Group Company) against all actions, proceedings, damages, costs, claims, charges and expenses arising from or incurred by reason of any (i) breach of this Clause 23 by the Supplier and or (ii) arising from any infringement or alleged infringement of any Intellectual Property Rights arising from the provision of the Goods and/or Services provided by the Supplier directly on directly under this agreement. Any infringement, threatened, actual and or alleged of this Clause will be notified by the Supplier to the Company immediately and in writing and the Supplier will make no admission of liability without the Customer's prior written consent.

23.2. The Company shall if the Supplier so reasonably requests, allow the Supplier to conduct any negotiations or litigation and/or settle any claim and give the Supplier all reasonable assistance (at the Supplier's cost).

23.3. If at any time an allegation of infringement of Intellectual Property Rights is made in respect of the Software, Services and or Documentation or if in the Company's reasonable opinion such an allegation is likely to be made, the Supplier may, at its own expense, modify or replace the Goods and/or Services so as to avoid the infringement without detracting from the overall performance the Supplier making good to the Company and any applicable member of the Company's Group any loss of productivity or use during modification or refund to the Company and any applicable member of the Company's Group all sums paid in respect of the infringing item.

23.4. If the above remedies fail after all reasonable efforts by the Supplier within a reasonable period, without prejudice to any other remedies available to the Company the Company may, at the expense of the Supplier, procure an alternative solution from a third party to satisfy its requirements relating to the Services and/or the Supplier shall refund the Fees paid for Goods and/or Services found to be or alleged to be infringing as well as any payment made for any related Goods and/or Services which have not been delivered or performed.

23.5. AI Usage Disclosure: It is a condition of this Agreement that during the term of this Agreement, the Supplier is obligated to immediately disclose to the Company, in writing, any use by the Vendor (including by any agents, third parties and/or subcontractors used by the Vendor) of any AI Technologies, including by reference the specific tools and systems used by it and the purposes for which they are used; and

23.6. Data Usage Restrictions: The Supplier undertakes, warrants, and agrees to use the data provided by the Company under the Agreement only for the agreed-upon purposes and will not use any data to train any AI Technologies outside of the scope of the Agreement without the prior written consent of the Company.

24. Counterparts

These Terms may be entered into in any number of counterparts and by the Parties to it on separate counterparts each of which when so executed and delivered shall be an original, but all these counterparts together shall constitute one and the same instrument.

25. Waiver

No failure or delay in exercising any right, power or privilege hereunder shall operate as a waiver thereof, nor shall any single or partial exercise preclude any other or future exercise thereof. Waivers are only binding if in writing and signed by an authorised representative of the Party giving the waiver.

26. Escalation and Dispute Resolution Process

26.1. The Parties shall meet and use their reasonable endeavours to resolve any dispute in accordance with the Dispute Resolution Procedure set out in this Clause 26 before escalating the dispute to court proceedings.

26.2. The Parties may relax the timescales referred to in this Clause 26 by mutual agreement (such agreement not to be unreasonably withheld or delayed).

26.3. The Parties' representatives to resolve the dispute shall be a director or senior manager within either Party who is authorised to make decisions on behalf of the Party and contractually bind the Party (including the settlement of any disputes) or the persons holding the relevant title, its equivalent or any successor title from time to time. If any of the representatives are unable to attend a meeting, a substitute may attend provided that such substitute has at least the same seniority or reasonably comparable managerial or directorial responsibility and is authorised to settle the unresolved matter.

26.4. As soon as either Party becomes aware of a disputed matter it shall refer the dispute to the representative best placed to deal with the dispute (taking into account the nature of the dispute). If the dispute cannot be resolved by good faith negotiations between the Parties within 10 Working Days of a written request from either Parties ("**Dispute Notice**"), the Dispute shall be further escalated in accordance with the escalation process set out in Clause 26.3.

26.5. If the Dispute is not resolved within a further thirty (30) days from the date of the Dispute Notice, the Parties shall mutually agree to resolve the Dispute by mediation in accordance with Clause 27.

27. Mediation

27.1. The following provisions shall apply to any such reference to mediation:

27.1.1. it shall be a reference under the Model Mediation Procedure ("MMP") of the Centre of Dispute Resolution ("**CEDR**") for the time being in force;

27.1.2. both Parties shall, immediately on such referral, co-operate fully, promptly and in good faith with CEDR and the mediator and do all such acts and sign all such documents as CEDR or the mediator may reasonably require to give effect to such mediation, including an agreement in, or substantially in, the form of CEDR's Model Mediation Agreement for the time being in force; and

27.1.3. to the extent not provided for by such agreement of the MMP the mediation shall:

i. commence by either Party serving on the other written notice setting out, in summary form, the issues in dispute and calling on that other Party to agree the appointment of a mediator; and

ii. be conducted by a sole mediator (which shall not exclude the presence of a pupil mediator) agreed between the Parties or, in default of Agreement, appointed by CEDR.

28. Applicable Law and Jurisdiction

28.1. Unless specified to the contrary between the Parties in writing, these Terms and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be

governed by and construed in accordance with the law of England.

28.2. Unless specified to the contrary between the Parties in writing, each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with these Terms or its subject matter or formation (including non-contractual disputes or claims).

29. Incorporation

Whether or not signed by both parties, the Supplier shall be deemed to accept the provisions of this Agreement if, following receipt of this Agreement, it supplies any Goods and/or Services to the Company.

For the avoidance of doubt, this Agreement (formed of the Terms, any applicable Appendices and any subsequent Purchase Orders) shall govern the Supplier's supply of Goods and/or Services to the Company and shall take precedence over any other terms and conditions issued on subsequent documentation, quotes or invoices unless explicitly agreed by the Parties (within in such documents) to supersede and replace this Agreement or any part of it.

IN WITNESS WHEREOF THIS AGREEMENT, has been entered into the day and year first before written by the Parties named below

SIGNED for and on behalf of WILLIAMS LEA LIMITED by:	**SIGNED for and on behalf of the SUPPLIER by:**
Signature: _____	***Signature:*** _____
Position: _____	***Position:*** _____
Name: _____	***Name:*** _____
Date: _____	***Date:***

APPENDIX 1

IF YOU SUPPLY GOODS (INCLUDING PRINT) TO THE COMPANY, THE FOLLOWING TERMS WILL APPLY

These terms are supplementary to the Main Terms. All capitalised terms shall have the definitions set out in the Main Terms.

1 Goods

1.1 The Supplier shall be responsible for the cost of packaging, loading, carriage and delivery of the Goods unless otherwise specifically stipulated by the Company in writing or as part of the Purchase Order.

1.2 The Goods shall be packaged by the Supplier in a safe and sufficient manner so as to avoid loss or damage to the Goods prior to acceptance by the Company, and the packaging shall comply with all applicable statutory requirements and codes of practice for the time being in force.

1.3 Unless otherwise agreed in writing by the Company, the Company shall not be obliged to return any packaging materials to the Supplier but shall be at liberty to dispose of or require the Supplier (at the Supplier's cost) to remove and take away packaging from the delivery location and lawfully and properly dispose of the same as it sees fit at the Supplier's expense and risk.

1.4 The Goods shall be accurately described, classified, packaged, marked and labelled all in strict accordance with applicable statutory and other legal requirements. On delivery, appropriate handling instructions and the Company identification information (including but not limited to a delivery note quoting the number of the Purchase Order and the quantity and weight of the Goods supplied) must accompany each delivery of the Goods and must be displayed prominently and be readily accessible.

1.5 Any acknowledgement given by any employee or agent of the Company purporting to be a receipt for Goods referred to in a delivery note shall be a non-binding estimate only of the identity or quantity of the Goods delivered. the Company reserves all of its rights in the event that subsequent investigation reveals that the Goods delivered were not as stated.

1.6 If and to the extent that the Supplier is or is deemed to be a producer as defined in The Producer Responsibility Obligations (Packaging Waste) Regulations 1997 as amended and the Packaging (Essential Requirements) Regulations 2003 ("**Producer Regulations**") or any such analogous legislation in a country other than the UK, the Supplier warrants and undertakes that it shall comply with the terms of the Producer Regulations.

1.7 If and to the extent that the Company is or is deemed to be a producer under the Producer Regulations, the Supplier further warrants and undertakes that it will assist the Company (and any third-party producer working on behalf of the Company) in fulfilling its obligations under the Producer Regulations. For the avoidance of doubt this shall include but shall not be limited to providing the Company (and its Clients) with all relevant information regarding the packaging used in the Goods, (and specifically providing a breakdown of materials, the quality of the materials and the origin of the materials used in the packaging).

2 Order and Acceptance

2.1 The Purchase Order constitutes an offer by the Company to purchase the Goods from the Supplier subject to these this Appendix 1.

2.2 The Purchase Order shall be accepted by the Supplier:

2.2.1 expressly by phone, e-mail, post, electronic means (including 'e-print'); or,

2.2.2 impliedly by fulfilling the Purchase Order.

2.3 Dispatch or delivery of the Goods by the Supplier to the Company shall be deemed conclusive evidence of acceptance of terms within this Appendix 1.

2.4 Once the Supplier accepts the Purchase Order in accordance with Clause 2.2, any document and artwork referred to in and supplied with the Purchase Order shall become a binding condition on the Supplier.

2.5 The Supplier expressly acknowledges that the terms within this Appendix 1 do not constitute any representation, promise or guarantee that the Company will request any particular volume of Goods from the Supplier.

2.6 the Company and the Supplier agree that the Company may at its sole discretion obtain in whole or part similar or equivalent Goods from a party other than the Supplier.

2.7 Unless otherwise agreed by way of an executed legal agreement signed by the Parties, this Agreement comprises the only terms and conditions on which the Company shall do business with the Supplier, (which replace any previous variations of the Agreement signed between the Company and the Supplier) and shall apply to the Agreement to the exclusion of any other terms and conditions generally used by the Supplier, proffered by the Supplier or otherwise brought to the Company's notice by the Supplier (whether or not such terms and conditions have been printed on any quotation, estimate or other document, electronically or otherwise given to the Company or subject to which the Purchase Order is accepted or purported to be accepted by the Supplier).

3 Quality and Description

3.1 Goods shall:

3.1.1 be free from all defects and shall conform and be rendered to meet all particulars and details as specified in the Purchase Order, where applicable;

3.1.2 comply with all statutory requirements and all applicable regulations relating to the Goods;

3.1.3 conform with any sample provided by the Company to the Supplier;

3.1.4 be and shall remain free from liens and encumbrances of any kind; and

3.1.5 be fit for any purpose for which they are supplied pursuant to the Purchase Order and any purpose held out by the Supplier.

3.2 The Supplier shall:

3.2.1 not accept an order request from the Company without being provided with a Purchase Order number;

3.2.2 and shall continue to have for the duration of the Agreement and for such time after the expiry or termination of the Agreement as is necessary for the proper performance of its obligations under the Agreement, full capacity and authority and all necessary governmental, administrative and regulatory authorisations, licences, permits and consents to enter into and to perform the Agreement and to supply the Goods and/or Services and the Supplier undertakes to inform the Company forthwith if any are withdrawn, limited or restricted in any way or are not renewed for any reason whether or not such withdrawal, limitation, restriction or non-renewal is a result of the fault or negligence of the Supplier;

3.2.3 comply with its obligations in accordance with Applicable Law;

3.2.4 promptly provide to the Company all information, materials, ancillary services reasonably required in relation to the Goods;

3.2.5 provide to the Company such access to personnel and/or premises as is reasonably required in relation to the Goods;

3.2.6 maintain adequate procedures in accordance with Good Industry Practice to maintain the security of data in relation to the Agreement;

3.2.7 maintain adequate Business Continuity and Disaster Recovery Procedures in accordance with Good Industry Practice;

3.2.8 ensure that any employees or agents of the Supplier, who are required to enter any the Company premises, comply with the security and health and safety regulations and other policies in force at such premises from time to time and obey the reasonable instructions of the Company while on such premises;

3.2.9 ensure that spare and/or replacement parts with respect to the Goods shall be available from the Supplier for a reasonable period of time following delivery of the Goods;

3.2.10 comply with ISO 12647-2 (at its own cost) as a recognised colour management standard or as specified by the Colour Connect Centre of Excellence, download any data requirements to achieve such standards from the Company server and upload relevant data to the Company's server for the Company to report on such compliance.

3.3 The Company has the right to inspect and/or test the Goods at any time prior to delivery and Supplier agrees to provide the Company with reasonable assistance to facilitate any such inspection and/or testing. If such inspection and/or testing cause the Company to be of the opinion that the Goods do not conform with the Agreement (and notwithstanding any other rights it may have at law or pursuant to the Agreement), the Company shall inform the Supplier and the Supplier shall at its own cost immediately take any action as is necessary to ensure conformity. If the Supplier fails to take any action reasonably requested by the Company, without prejudice to any other rights that the Company may have, the Company may treat such failure as a repudiatory breach of the Agreement by the Supplier and shall have the right to terminate it forthwith.

3.4 The Supplier hereby covenants that, where requested by the Company, the Supplier shall become a member of the Colour Connect Programme, and license the Applicable Software from the Company or any independent contractor or agent in order to perform the Services according to certain quality standards. Usage of the Applicable Software shall be strictly governed by the licence provisions of the *Colour Connect Onboarding Agreement – Addendum*, or (where granted directly by an independent contractor or agent) such other licence presented at the relevant time.

4 Guarantee

4.1 The Supplier guarantees the Goods against defects in design, materials equipment and workmanship, for a period of twelve (12) months following receipt of the Goods by the Company or such period of time specified in the Purchase Order.

4.2 In the event that following receipt of the Goods by the Company such Goods are not defect free (at the Company's sole discretion), then in such an event the Supplier shall at the request of the Company either replace or repair any defective Goods at the Suppliers own cost and within the agreed Service Levels to conform to the Agreement. In the event that the Supplier does not repair defective Goods within the agreed Service Levels then the Company may do so itself or authorise others to do the same and, in that event, the Company shall recover all costs arising therefrom from the Supplier.

5 Packaging and Labelling

5.1 The Supplier shall be responsible for the cost of packaging, loading, carriage and delivery of the Goods unless otherwise specifically stipulated by the Company in writing or as part of the Purchase Order.

5.2 The Goods shall be packaged by the Supplier in a safe and sufficient manner so as to avoid loss or damage to the Goods prior to acceptance by the Company, and the packaging shall comply with all applicable statutory requirements and codes of practice for the time being in force.

5.3 Unless otherwise agreed in writing by the Company, the Company shall not be obliged to return any packaging materials to the Supplier but shall be at liberty to dispose of or require the Supplier (at the Supplier's cost) to remove and take away packaging from the delivery location and lawfully and properly dispose of the same as it sees fit at the Supplier's expense and risk.

5.4 On delivery, the Goods are accurately described, classified, packaged, marked and labelled all in strict accordance with applicable

statutory and other legal requirements. On delivery, appropriate handling instructions and the Company identification information (including but not limited to a delivery note quoting the number of the Purchase Order and the quantity and weight of the Goods supplied) must accompany each delivery of the Goods and must be displayed prominently and be readily accessible.

5.5 Any acknowledgement given by any employee or agent of the Company purporting to be a receipt for Goods referred to in a delivery note shall be a non-binding estimate only of the identity or quantity of the Goods delivered. the Company reserves all of its rights in the event that subsequent investigation reveals that the Goods delivered were not as stated.

6 Title

6.1 Unless otherwise agreed by the Parties in writing, full legal title and beneficial interest in the Goods shall be transferred to the Company when the Company accepts the delivery of such Goods.

6.2 If any further action is required such as, but not limited to, installation of the Goods, the Suppler shall notify in writing to the Company providing the specifications to be carried out free of charge and pursuant this Agreement.

6.3 The Supplier warrants and represents that:

6.3.1 the Supplier will be the sole owner and responsible of such Goods until the delivery was accepted by the Company;

6.3.2 no other person and/or entity has a legal or other interest which could mean that the Company is unable to own the Goods;

6.3.3 at the time of the delivery the Goods shall fit for purpose and shall meet the description and standards described on the PO and/or agreed in writing by the Parties as applicable;

6.3.4 it has all unexpired manufacturer warranties related to the Goods for the benefit of the Company;

6.3.5 the Goods shall comply with the all relevant applicable legislation and Good Industry Practice;

6.3.6 it has all necessary licenses, consent and authorisations required to supply the Goods; and

6.3.7 the Supplier has paid any royalties due to Third Parties, if required.

6.4 Without prejudice to any other rights or remedies provided in these Agreement or by law if some or all of the Goods are faulty and/or the Supplier is in breach of any of the warranties or representations provided herein, the Company will be entitled to reject the Goods in whole or in part, and the Supplier shall within five (5) Business Days refund to the Company any charges paid by the Company in respect of such Goods and at the Company's sole discretion cancel any PO and/or terminate the Agreement pursuant to Clause 6 of the Agreement (termination) and/or, at the Supplier's cost, replace the Goods from the day the Supplier is notified to that effect.

7 REACH Regulation

7.1 Where applicable to the Goods, the Supplier will ensure for the duration of the Agreement, that:

7.1.1 the Goods conform with the legal requirements of the REACH Regulation before they are supplied to the Company; and

7.1.2 in the event of a change to the REACH Candidate List of Substances of Very High Concern, the Supplier will confirm to the Company that it has fulfilled all its obligations and provide the Company with the required information in accordance with Article 33 of the REACH Regulation.

8 Delivery

8.1 The Supplier shall deliver the Goods at the delivery point or points specified in the Purchase Order or elsewhere as the Company may direct, at the Supplier's expense, not earlier than the date and time specified in the Purchase Order. The Company may at its discretion request the Supplier to make delivery outside Working Hours but unless the Company notifies the Supplier in writing it shall not be obliged to accept deliveries outside of Working Hours.

8.2 In making delivery the Supplier shall comply fully (and shall procure that its carriers comply fully) with any delivery requirements/procedures at the delivery point or points which have been brought to the Supplier's attention.

8.3 Whenever a time of and/or date for delivery of Goods is stated on the Purchase Order, the time of and/or date for delivery of Goods shall be of the essence of the Agreement.

8.4 The Supplier shall give the Company immediate notice of any potential delay in delivery of the Goods.

8.5 If the Supplier fails to deliver the Goods and/or perform the Services by the time and/or date specified in the Purchase Order (if any) the Company may without prejudice to its other rights reject the Goods and cancel the Agreement.

8.6 Physical delivery of the Goods and acknowledgement or receipt thereof by the Company shall not be deemed to be any acceptance of a variation in the Purchase Order or the Agreement.

8.7 Even if the Goods are to be delivered by instalments, the Agreement shall be treated as a single contract and not severable. Failure to deliver one instalment of the Goods by the time and/or date specified in the Purchase Order (if any) shall allow the Company, without prejudice to its other rights to reject the Goods and cancel the Agreement.

9 Print Materials

9.1 Where the Goods supplied include printed materials, the Supplier will on request:

9.1.1 achieve and maintain ISO 14001: 2004 certification;

9.1.2 maintain Forest Stewardship Council chain of custody certification;

9.1.3 ensure that they comply with ISO 12647-2 as a recognised colour management standard or such other standard as specified by the Colour Connect Centre of Excellence;

9.1.4 submit an EcoVadis[1] scorecard and share with the Company.

9.2 From time to time the Company undertakes environmental initiatives with its vendor base. The Supplier shall participate in such initiatives on request from the Company.

9.3 The Supplier will comply with Waste Electrical and Electronic Equipment (Amendment) Regulations 2010 (SI 2010/1155) (as amended from time to time) or applicable analogous legislation in a country outside the EU.

9.4 The Supplier undertakes, on the Company's request, to become a member of the Supplier Ethical Data Exchange ("**Sedex**") and maintain its membership with Sedex when supplying any Goods to or performing any Services for the Company or any of its Clients. For the avoidance of doubt, as part of the membership requirement, the Supplier is required to keep up to date Sedex Self-Assessment Questionnaire information and upload any new audit data onto Sedex platform. The Supplier shall allow the Company access to any such information available on Sedex platform.

9.5 The Price shall be as specified in the Purchase Order and, unless otherwise stated, shall be inclusive of insurance charges and any other charges for delivery (including packaging and freight in[2] accordance with Clause 5.1) and any duties, imposts and levies (in respect of which all required documentation shall accompany the Goods), other than VAT which shall be payable by the Company subject to receipt of a VAT invoice in accordance with Clause 4 of the Terms.

9.6 No increase in the Price may be made (whether on account of increased material, labour or transport costs, fluctuation in rates of exchange or otherwise) without the prior written consent of the Company.

10 Free Issue Materials

10.1 All materials, including any artwork or documents (together with any modifications, alterations, adaptations or changes to the artwork and the documents) ("**Materials**") made available by the Company to the Supplier in connection with the Agreement shall be and remain the property of the Company but shall be at the risk of the Supplier until delivery and acceptance of the Goods or the return of the Materials whichever shall be the later.

10.2 The Supplier shall:

10.3 keep the Materials in good order and condition and be responsible for any loss thereof or damage thereto;

10.4 use the Materials only for the purpose of the Agreement;

10.5 return the Materials not required for use "carriage paid", to the Company at the Company's request or, if no request is made, upon completion of the Agreement.

11 Termination

11.1 The Supplier shall, on completion of the Agreement, deliver to the Company all artwork and documents whether supplied by the Company or prepared by or on behalf of the Supplier in connection with the Agreement.

12 Quotes and Instant Pricing

12.1 A Quote shall be valid for the period of time specified by the Supplier in the Quote.

12.2 If the Company wishes to purchase Goods on the basis of the Supplier's Quote, the Company shall issue a Purchase Order to the Supplier.

12.3 Should the Supplier's Quote be accepted, the Quote, the Purchase Order together with these Terms and any changes specifically agreed in signed writing will form a binding contract between the Supplier and the Company. There will be no provision for the price(s) submitted in the Quote to be subsequently reviewed by the Supplier.

12.4 The Company is not obliged to accept any Quote submitted by the Supplier.

12.5 If a Supplier uses Instant Pricing to submit a Quote, the remaining provisions of this Clause 12 shall apply:

12.6 The Supplier is solely responsible for inputting the Supplier Data into Instant Pricing, and the Company shall not be liable for any losses, damages, costs, expenses or liabilities arising from the Supplier incorrectly inputting the Supplier Data into Instant Pricing to submit a Quote, including but not limited to where:

12.6.1 the Supplier is not awarded a contract for Goods; or

12.6.2 the Supplier is bound to deliver Goods under a contract on the basis of the Supplier Data inputted by the Supplier.

12.7 The Supplier agrees that any Supplier Data inputted by the Supplier into Instant Pricing shall become the Company's property and the Company shall have full access rights in respect of such Supplier Data.

12.8 The Supplier warrants that:

12.8.1 it is the sole unencumbered absolute legal and beneficial owner or the licensee of all Intellectual Property Rights in

[1] EcoVadis is a global provider of business sustainability ratings, creating a global network of more than 65,000 rated companies: https://ecovadis.com/

the Supplier Data;

12.8.2 the Supplier Data does not and shall not infringe any Intellectual Property Rights or any other rights whatsoever of any person; and

12.8.3 the Supplier Data will be true, accurate and complete in all respects.

12.9 The Supplier shall comply with any additional terms of use of Instant Pricing required by any licensor of Instant Pricing (or any component thereof), as notified to the Supplier from time to time.

APPENDIX 2

IF YOU PROVIDE SOFTWARE SERVICES TO THE COMPANY THE FOLLOWING TERMS SHALL APPLY

These terms are supplementary to the Main Terms. All capitalised terms shall have the definitions set out in the Main Terms.

1. SERVICES AND LICENCE

1.1 The Supplier shall provide the Software Services specified in the Purchase Order or other agreed documents. The Software Services will be governed by the Agreement more generally and the special terms in this Appendix 2.

1.2 Supplier hereby grants the Company a worldwide, non-exclusive, non-transferrable (except in respect of any Group Company), sublicensable right to permit the Authorised Users to access the Software, the Services and the Documentation, during the applicable Subscription Term as specified in each Purchase Order entered into from time to time by the Company.

1.3 the Company shall ensure that:

1.3.1 only Authorised Users shall have access to the Software;

1.3.2 each Authorised User keeps a secure password for his use of the Software and that each Authorised User keeps his password confidential; and

1.3.3 it shall not store, distribute or transmit any Virus, or any material through the Services that is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive; facilitates illegal activity; depicts sexually explicit images; or promotes unlawful violence, discrimination based on race, gender, colour, religious belief, sexual orientation, disability, or any other illegal activities.

1.4 Supplier shall facilitate upon request of the Company, the transfer of User Subscriptions between Authorised Users provided that it does not exceed the number of User Subscriptions granted pursuant to the applicable Purchase Order.

1.5 Where the number of Authorised Users exceeds the number of User Subscriptions purchased by the Company under this Agreement, the Supplier's sole and exclusive remedy will be the applicable Fees for the period of such excess usage.

1.6 The Supplier shall perform the Services exclusively at the Supplier Permitted Locations.

1.7 The Supplier shall on a monthly basis provide the Company with reports and information to enable the Company to effectively monitor the Supplier's performance against the Service Levels. Without prejudice to the foregoing, the Supplier promptly upon request provide the Company with such reports and information as the Company may reasonably require in relation to the provision of the Services.

1.8 The Supplier agrees that the provision of the Services shall be subject to continuous improvement and shall provide to the Company upon reasonable request a detailed report setting out how it will improve the provision of the Services to the Company. The Supplier shall notify and make available to the Company any upgrades, updates and releases it makes generally available to its clients and customers.

1.9 The Supplier shall procure the attendance of sufficiently senior members of the Supplier Personnel to attend meetings with the Company from time to time upon the Company's reasonable request.

1.10 The Supplier and the Company shall agree in writing a member of the Supplier Personnel to be the Supplier Account Manager. The Supplier shall arrange that the Supplier Account Manager is responsible for the day to day activities relating to the Services and is the Company's first point of contact regarding the Services. The Supplier shall use all reasonable endeavours retain the Supplier Account Manager's engagement on the Services.

1.11 The Supplier shall:

1.11.1 promptly provide to the Company all information, materials, ancillary services reasonably required in relation to the Services; and

1.11.2 ensure that the Supplier Personnel, who are required to enter any the Company premises, comply with the security and health and safety regulations and other policies in force at such premises from time to time, obey the reasonable instructions of the Company while on such premises and otherwise not cause any disruption, spoilage, disturbance or damage to such premises.

2. ACCESS TO THE SERVICES

2.1 Supplier grants the Company a right to receive the Services under a Purchase Order during the applicable Subscription Term.

2.2 Supplier recognises that the Company may have legitimate business reasons for not upgrading to a new version of the Software as soon as the version becomes available. In the event of cessation of support of old versions which have reached their end-of-life, Supplier shall serve the Company a minimum of twelve (12) month's written notice of its intention to cease support such product version, Supplier may remove the Company's access to that version and upgrade the Company to a new version at no extra cost to the Company.

2.3 The Supplier shall ensure that any upgrade, update or release of the Software shall conform to the requirements of these Terms and shall not result in a material degradation or change in functionality of the Services.

3. SUPPLIER'S WARRANTIES

3.1 Supplier warrants, represents and undertakes that the Services will be delivered in accordance with:

3.1.1 the Services Description set out in the Purchase Order;

3.1.2 the Service Levels;

3.1.3 the Documentation;

3.1.4 Good Industry Practice;

3.1.5 Applicable Law; and

3.1.6 Appendices 4, 5, 6, 7 and 8 and any other of the Company's policies.

3.2 Supplier warrants, represents and undertakes that it:

3.2.1 shall not introduce any software into the Company System other than the Software without the Company's prior written consent;

3.2.2 has and shall maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under these Terms (including but not limited to its provision of the Software, Services and Documentation) and that the performance of its obligations shall not infringe the rights of any Third Party;

3.2.3 has full authority to enter into this Agreement to provide the Services and that doing so will not amount to a breach by the Supplier of any contract or binding agreement (whether written or oral) to which it is a party;

3.2.4 all information which the Supplier or any of its representatives has furnished to the Company or any of its representatives prior to the Commencement Date of this Agreement and, in respect of each Order, Service Commencement Date, in connection with or for the purposes of the transaction evidenced by this Agreement or Purchase Order is true, complete and correct in all material respects (except to the extent based on incorrect information provided by the Company to the Supplier); and

3.2.5 the Supplier has carried out due diligence in accordance with Good Industry Practice with the objective of satisfying itself as to all risks, contingencies and circumstances to do with the performance of this Agreement and any Purchase Order.

3.3 Supplier warrants, represents and undertakes that Supplier's hosting environment meets the following requirements:

3.3.1 preservation of the confidentiality of all of the Company's Confidential Information, which includes any back up media produced which incorporates in any way the Company Data;

3.3.2 provision of adequate security measures is in place at all times and are fully documented and made available to the Company upon request including but not limited to the provision of firewalls, virus detection and intrusion monitoring;

3.3.3 Supplier shall maintain daily backups of the Company Data for disaster recovery purposes in accordance with Clause 11 of the Main Terms and Appendix 6;

3.3.4 all the Company Data is encrypted for any transmission; and

3.3.5 Supplier shall ensure that it fully supports and maintains the hosting environment including putting in place, disaster recover planning and performance and capacity monitoring in accordance with Clause 11 of the Main Terms.

3.4 The Supplier warrants that:

3.4.1 the Software is free from any Virus; and

3.4.2 the Software is free from Open Source Software;

and the Supplier undertakes to use Software tools in accordance with Good Industry Practice to detect the presence of any Virus and/or Open Source Software.

3.5 Without prejudice to Clause 23 of the Main Terms and/or Clauses 3.2, 6.1 and 6.2 of this Appendix 2, in the event that the Supplier is non-compliant with any warranty in this Agreement relating to the provision of Software, the Supplier shall, at the Supplier's option, promptly repair, replace or remedy (as appropriate) the non-compliant Software.

3.6 If none of the options in Clause 23 of the Main Terms are reasonably practicable, the Company may (but is not obligated to) terminate the Agreement, in which case Supplier shall refund to the Company all Fees pre-paid to Supplier for unused Services (without prejudice to any other remedy available to the Company).

3.7 In the event that the Supplier becomes aware of its non-compliance with any of the warranties in Clauses 3.1 to 3.4 of this Appendix 2, it will notify the Company immediately and will provide full co-operation to the Company in its investigation of any such non-compliance.

3.8 The warranties, representations and undertakings in Clauses 3.1 to 3.4 of this Appendix 2 shall be repeated by the Supplier as at the date of providing any new Software or Software Services.

4. SERVICE LEVELS

4.1 The Supplier shall use make the Services available twenty-four (24) hours a day, seven days a week, except for:

4.1.1 planned Maintenance and Support carried out during the Maintenance Window; and

4.1.2 unscheduled Maintenance and Support performed outside Maintenance Window but during Business Hours, provided that the Supplier has used reasonable endeavours to give the Company at least six (6) Business Hours' notice in advance.

4.2 If there is a Service Failure, (without limiting any other obligations the Supplier may have and without limiting any other rights or remedies of the Company) the Supplier shall:

4.2.1 notify the Company immediately of the Service Failure; and

4.2.2 carry out promptly in accordance with Good Industry Practice and at its own cost resolution of the Service Failure; and

4.2.3 shall provide an incident report relating to the Service Failure which shall identify the cause of the Service Failure and will propose measures that the Supplier shall take in order to minimise the recurrence of such Service Failure.

4.3 The Supplier shall provide the Company with a monthly report detailing its performance in respect of each of the Service Levels in such format as is acceptable to the Company (acting reasonably).

4.4 The Supplier shall calculate any applicable Service Credits in accordance with the provisions set out in the Purchase Order Details and shall make payment of the Services Credits to the Company in accordance with the provisions of Clause 4.9 of the Main Terms.

4.5 The Parties agree that the Service Credits are not a penalty and are a genuine pre-estimate of the loss likely to be suffered by the Company in respect of a failure by the Supplier to comply with the relevant Service Level.

4.6 The Supplier acknowledges that Service Credits are in addition to (and not a substitute for) any other rights or actions the Company may have against Supplier arising from the Supplier's failure to provide the Services in accordance with this Agreement.

5. THE COMPANY OBLIGATIONS AND RELATED PROVISIONS

5.1 The Company shall provide to the Supplier and shall procure the provision of its personnel to the Supplier, information and cooperation that is reasonably required by the Supplier to provide the Software Services, including the provision of access and functioning of the Company System to effectively interface with the Software. The Supplier shall be relieved of any failure to provide the Software Services as a direct result of the Company's failure to perform such obligations provided that the Supplier has notified to the Company in writing of such failure of the Company as soon as reasonably practicable.

6. PROPRIETARY RIGHTS

6.1 The Company acknowledges and agrees that the Supplier and/or its licensors own all Intellectual Property Rights in the Software or the Documentation and this Agreement does not grant the Company any rights to, or in, the Intellectual Property Rights, or any other rights or licences in respect of the Software or any Documentation subject to Clauses 6.2 and 6.3 of this Appendix 2.

6.2 Where any Intellectual Property in the Work Products is created under this Agreement, such Intellectual Property belongs to and shall irrevocably belong to the Company and the Supplier hereby assigns to the Company all such Intellectual Property and hereby agrees that any Intellectual Property therein that come into existence after the date hereof shall vest absolutely in the Company immediately upon such rights coming into existence and to that end the Supplier hereby assigns with full title guarantee for all purposes, applications and fields of use (including by way of present assignment of future rights in relation to rights not yet created) and free from all third party rights, all right, title and interest in and to the foregoing to the Company absolutely. The Supplier agrees to do all acts and execute all documents necessary to give effect to the provisions of this Clause 6 of Appendix 2. The Supplier hereby unconditionally and irrevocably waives all moral rights in relation to such Intellectual Property. For the avoidance of doubt, all Intellectual Property Rights in the Company Data shall remain the property of the Company and the Supplier is not granted any rights under this Agreement in the Company Data except to the extent strictly necessary for the purposes of providing the Services.

6.3 Supplier hereby grants the Company a worldwide, non-exclusive, perpetual, non-transferrable (except in respect of the Company Companies which shall be transferrable), sublicensable right to use any Intellectual Property Rights incorporated into the Work Products (including, for the avoidance of doubt, any Intellectual Property Rights prior to their assignment to the Company pursuant to this Clause 6 of Appendix 2 and any Supplier Software incorporated in the Software).

6.4 The Supplier will execute, and procure the execution of, all necessary contractual documentation with Supplier Personnel to give effect to its obligations under this Clause 6 of Appendix 2.

APPENDIX 5 DATA PROTECTION

IF YOU PROCESS PERSONAL DATA ON BEHALF OF THE COMPANY THE FOLLOWING TERMS SHALL APPLY

These terms are supplementary to the Main Terms and Condition (the "Main Terms"). All capitalized terms that are not defined in this Appendix shall have the definitions set out in the Main Terms. The particulars of Processing under Schedule 1 below and its Annexes should be downloaded and modified as appropriate to the Processing.

1 **Definitions**

In this Appendix 5, the following definitions apply:

"**Contract**" means this Onboarding Agreement including all Appendices together with the contents of the any Purchase Order.

"**Data**" means all Personal Data collected, generated or otherwise Processed by Supplier as a result of, or in connection with, the provision of the Goods and/or Services.

"Data Processing Form" means a data Processing form in the format set out in the Annex hereto which shall be completed, agreed and signed by both Parties in the event that there is a change to the nature, extent, scope or purpose of the Processing of Personal Data under this Appendix 5 or where there is a change to the Technical and Organizational Security Measures taken by the Supplier.

"**Data Protection Laws**" means:

(a) the General Data Protection Regulation (EU 2016/679) ("**GDPR**") and any legislation which amends, re- enacts or replaces it in an EEA member state or in England and Wales from such time as the United Kingdom ceases to be an EEA member state and unless and until the GDPR is no longer directly applicable in the UK and any national implementing laws, regulations and secondary legislation as amended and updated from time to time in the UK and any successor legislation to the GDPR or the Data Protection Act 2018;

(b) at all times, any other Data Protection laws and regulations applicable in an EEA member state or in England and Wales from such time as the United Kingdom ceases to be an EEA member state.

"Data Exporter" means an entity transferring Personal Data to an entity situated in a Third Country.

"Data Importer" means an entity situated within a Third Country who receives and Processes Personal Data from and on behalf of a Data Exporter.

"Data Protection Officer" has the meaning given to it under Article 37 of the GDPR.

"**Data Subject**" means an individual who is the subject of Personal Data.

"**Data Subject Request**" means any request from a Data Subject concerning his or her rights of access to, rectification, erasure, objection to or restriction of Processing of Data under the Data Protection Laws.

"**Data Transfer Agreement**" means these Standard Contractual Clauses.

"**EEA**" means the European Economic Area.

"**Personal Data**" means any data relating to an identified or identifiable individual that are within the scope of protection as "Personal Data" under the applicable Data Protection Laws and that are Processed by Supplier in connection with the Goods and/or Services provided under the Contract.

"**Processing Agreement**" means this Appendix 5.

"**Standard Contractual Clauses**"

- When processing EU Personal Data as a Processor where Williams Lea is the Controller means Module 2 of the EU Standard Contractual Clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the relevant EU Privacy Law,
- When Processing EU personal Data as a Sub-Processor where Williams Lea is a Processor means Module 3 of the EU Standard Contractual Clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the relevant EU Privacy Law
- When processing UK Personal Data as a Processor or Sub processor also includes the addendum issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 and is set out in full here. .

"**Sub-Processor**" has the meaning set out in Schedule 1.

"Supervisory Authority" means any regulatory, supervisory, governmental, or other competent authority with jurisdiction or oversight over the Data Protection Laws.

"**Third Country(ies)**" means a country or countries outside the EEA.

2 **Data Processing**

(a) Supplier acknowledges that for the purposes of the Data Protection Laws the Company is the Controller and Supplier is the Processor of any Personal Data and that this Appendix 5 (***Data Protection***) constitutes a Data Processing Agreement where required by the Data Protection Laws. A Data Processing Form agreed and signed by the Parties will set out the scope, nature, purpose of Processing, duration of Processing and type of Personal Data to be Processed by the Supplier under this Appendix 5. Data Processing Forms may be updated from time to time between the Parties.

(b) The Parties acknowledge that the Company is located in a Third Country, thereby potentially acting as a Data Importer, where it transfers to the Supplier, Personal Data that originates from any Customers within the EEA. In such cases the GDPR requires that Standard Contractual Clauses must govern the Processing of such Personal Data (including where the Company transfers the Personal Data to a Supplier (a Sub-Processor).

(c) The Parties acknowledge and agree that the Standard Contractual Clauses are effective and offer the same or greater protective requirements with regards to the Processing of Personal Data between Data Controller and Data Processor within the EEA as it does on the Processing of Personal Data between Data Exporters and Data Importers. Therefore, whether or not the origin of Personal Data Processed under this Agreement is the EEA, they shall comply with the provisions of the Standard Contractual Clauses as they would apply to Importers.

(d) Supplier shall comply with the requirements of the Data Protection Laws in respect of the activities which are the subject of the Agreement and shall not knowingly do anything or permit anything to be done which might lead to a breach by Supplier or the Company of the Data Protection Laws.

(e) Supplier warrants, represents and covenants that it will only Process Personal Data, when applicable, to the extent it relates to:

(i) the types of Personal Data;

(ii) the categories of Data Subject;

(iii) the duration, nature and purpose of Processing,

(iv) the Technical and Organisational Security Measures that must apply to any Processing, set

out in a Data Processing Form and only for the duration specified in a Data Processing Form.

SCHEDULE 1

Cross Border Transfer

PART 1 – EU RESTRICTED TRANSFERS

1. The parties agree (under Clause 4 of the Agreement), that the terms of Module 2 or 3 (As applicable) of the Standard Contractual Clauses are hereby incorporated into this agreement as if they had been set out in full and shall apply to any EU Restricted Transfer.
2. Module 2 (EU Controller to Processor Model Clauses) of the EU Model Clauses shall apply where the EEA Transfer of Personal Data is data controller to data processor.
3. Module 3 (EU Processor to Processor Model Clauses) of the EU Model Clauses shall apply where the EU Restricted Transfer of Personal Data is data processor to data processor.
4. Clause 7 of the EU Model Clauses (Docking Clause) shall apply.
5. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the EU Model Clauses shall apply, and the method for appointing and time period for prior notice of sub-processor changes shall be 30 calendar days.
6. In Clause 11 of the EU Model Clauses, the optional language will not apply.
7. In Clause 17 of the EU Model Clauses, Option 1 shall apply, and the Parties agree that the EU Model Clauses shall be governed by the laws of the Ireland
8. In Clause 18(b) of the EU Model Clauses, disputes will be resolved before the courts of Ireland.
9. Annexes of the EU Model Clauses are completed:
    a. Annex IA of the EU Model Clauses: List of Parties are the Parties to this Agreement;
    b. Annex IB of the EU Model Clauses: Description of Transfer is at Annex 1 of this Agreement;
    c. Annex IC of the EU Model Clauses: Competent Supervisory Authority will be the Irish Data Protection Commissioner.;
    d. Annex II of the EU Model Clauses: Technical and Organisational Measures are defined Annex 2 of this Agreement; and
    e. Annex III of the EU Model Clauses: List of sub-processors is at Annex 3 of this Agreement.
10. To the extent there is any conflict between the EU Model Clauses and any other terms in this Agreement, the provisions of the EU Model Clauses will prevail.

Signature and Date: By entering into the Agreement, the Data Exporter and the Data Importer are deemed to have signed these EU Model Clauses, incorporated here as if they have been set out in full, including their Annexes, as of the Effective Date of the Agreement.

PART 2 – UK RESTRICTED TRANSFERS

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making UK and EU Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

AGREED TERMS

Table 1: Parties

The Parties	Williams Lea (who sends the Restricted Transfer)	The Supplier (who receives the Restricted Transfer)
Parties' details	The parties to this Agreement	The parties to this Agreement
Key contacts	As detailed in the MSA	As detailed in the MSA
Signature (if required for the purposes of Section 2)	As detailed in the MSA	As detailed in the MSA

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	Yes	Yes	No	-	-	-
2	Yes	Yes	No	General	30 days	-
3	Yes	Yes	No	General	30 days	-
4	Yes	Yes	No	-	-	Yes

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: The parties to this Agreement
Annex 1B: Description of Transfer: Annex 1
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex 2
Annex III: List of Sub processors (Modules 2 and 3 only): Annex 3

Table 4: Ending this Addendum when the Approved Addendum changes.

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☒ Exporter ☐ Neither Party

Alternative Part 2 Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. These can be found here.

PART 3 – ADDITIONAL SAFEGUARDS

1. In the event of a Restricted Transfer, the Parties agree to supplement the Agreement with the following safeguards and representations, where appropriate:

   (a) The Data Importer shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from Data Exporter to Data Importer and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.

   (b) The Data Importer will make commercially reasonable efforts to resist, subject to Applicable Privacy Laws, any request for bulk surveillance relating to the Personal Data protected under EU GDPR and/or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Court ("FISA");

   (c) If the Data Importer becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:

      (i) The Data Importer shall inform the relevant government authority that the Data Importer is a processor of the Personal Data and that the Data Exporter has not authorized the Data Importer to disclose the Personal Data to the government authority; and

      (ii) inform the relevant government authority that any and all requests or demands for access to the Personal Data should therefore be notified to or served upon the Data Exporter in writing.

ANNEX 1

Duration of Processing

Customer Personal Data shall be Processed for no longer than is necessary for compliance with the Processing Agreement, or as is required by any law to which the Data Importer is subject.

Nature and Purpose

- The accessing of and storage on the Data Importer's systems/network servers.
- Provision of services to the Customer pursuant to the Processing Agreement.
- Operation and maintenance of systems.
- Management and management reporting.
- Financial reporting and audit reports, including invoicing activities on behalf of the Customer.
- Risk management, compliance, legal and audit functions.

Data subjects

The Personal Data transferred concern the following categories of Data Subjects (please specify):

- End users and/or consumers of products and services provided by the Customer.
- End users and/or consumers of products and services provided by Company Entities
- Employees of the Customer.
- Employees of suppliers to the Customer.
- Employees of suppliers to Company entities.
- Employees of Company Entities.

Categories of data

The Personal Data transferred concern the following categories of data:

- Personal details: Name, address, email address, telephone number and other contact information, next of kin, family and social details.
- Financial details: Tax status, transaction records, payment method records.
- Employment details: Company, job title, cost centre, fee rates.
- Other Personal Data which has been provided by end users or consumers in the course of using the services provided by the Customer

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

- Health / Medical including Disabilities
- Ethic origin
- Genetic Data
- Sexual Orientation
- Religious / Philosophical Beliefs
- Trade Union Memberships
- Political Opinion

Processing operations

The Personal Data transferred will be subject to the following basic Processing activities (please specify):

- Processing as part of a contracted service
- Processing for Company activities (Employment, Purchases, Sales, Marketing, Operational, HR)

Minimum Security measures

List of approved Sub Processors

Company name	Company address	Transfer mechanism	Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized)

APPENDIX 6

DATA SECURITY SCHEDULE

INFORMATION SECURITY, PHYSICAL SECURITY & BUSINESS CONTINUITY MANAGEMENT

These terms are supplementary to the Main Terms. All capitalised terms that are not defined in this Appendix shall have the definitions set out in the Main Terms.

Applicable Security Law Requirements	means any applicable requirements arising out of law, statute, byelaw, regulation, order, regulatory policy, guidance or industry code, rule of court or directives relating to information security.
Business Continuity Incident	means any event as a result of which the Business Continuity Plan is invoked.
Business Continuity Management Programme	means a proactive process to identify key operations and recovery requirements from which Business Continuity Plans may be developed.
Business Continuity Plan	means a plan produced by the Supplier invoked upon the occurrence of a Business Continuity Incident which provides step by step guidance around the recovery of services to an agreed recovery point.
Business Impact Analysis	means a process that identifies and evaluates the potential effects of natural and man-made events on business operations.
Company Assets	means the Company personnel, the Company Data or relevant infrastructure.
Company Customer Data	means information relating to the Company's clients and customers (or those of any Group Company).
Company Data	means all data (including but not limited to the Company Customer Data), tables, information, text, drawings, codes, diagrams, images or sounds which are embodied in any electronic or tangible medium, including compilations of any of the foregoing, and which are: (a) processed by, or a product of, the Services; (b) generated by the Supplier or a Supplier Company or a sub-contractor of the Supplier in carrying out the Supplier's obligations under this Agreement; or generated by or on behalf of the Company or a Group Company.
Company Systems	means systems of the Company or a Group Company.
Development Environment	means the environment made available for the creation and development of programs or software products prior to being released into a Testing Environment.
GDPR Regulation	means General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).
Information Commissioner's Office	means ICO is the UK's independent body responsible for upholding information rights and data privacy for individuals.
Information Security Controls	means controls to protect the confidentiality, integrity or availability of data.
Minimum Business Continuity Objective	means the minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during an incident, emergency or disaster.
Personally Identifiable Information (PII)	means information that can be used to identify an individual person e.g. name, date of birth, address.
Physical Security Controls	means controls to prevent unauthorised physical access to Supplier or Supplier company premises.

Physical Security Incident	means any event where there is, or potentially could be, unauthorised access to, or use of, or interface with Company Assets under the Supplier's or a Supplier Company's or any of the supplier's (or, as the case may be, a Supplier Company's) sub-contractors' control.
Production Environment	means an environment where the real-time staging of programs that run an organisation are executed, and includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Public Cloud Services	means any data hosting, processing or storage service which is provided to the Supplier by a Third Party, where the service is provided on infrastructure owned and located at the third party's premises, and the service is made available over the internet using infrastructure shared amongst clients and customers.
Recovery Point Objective	means the point in time to which work needs to be restored following a Business Continuity Incident.
Recovery Time Objective	means the time objective for restoration of Business as Usual in the event of Business Continuity Incident.
Relevant Systems	means systems that host Company Data, either the Company Systems or Supplier Systems.
Security Incident Management Process	means monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events.
SMEs	means Subject Matter Experts.
Supplier Company	means a member of the group of companies of which the primary Supplier is the parent company, or where the supplier company is considered an affiliate of a group of companies.
Supplier Personnel	means any employee, officer, agent or other person whatsoever acting for the Supplier or otherwise under the control and direction of the Supplier, a Supplier Company or of any of the Supplier's Approved Sub-Contractors.
Supplier Network	means technology network or system of computers operated by the supplier or a Supplier Company or any of the Supplier's sub-contractor which are joined together so that they can exchange information in a segregated environment.
Supplier Systems	means system or systems that host Company Data whether they are under the ownership of the Supplier or a Supplier Company or any affiliated sub-contractors.
Supplier's Key Security Contact	means supplier contact with responsibility for the information security of the services, physical security of assets and notification and update on business continuity invocation in the event of a business continuity incident.
Testing Environment	means environment made available for the testing of recently developed programs or software products prior to being released into a Production Environment.

1. INTRODUCTION

1.1. Subject to the provisions set out below, the Supplier shall be responsible for all aspects of the security of the Services and shall take action to safeguard the Services against:

1.1.1. breach of confidentiality (e.g. unauthorised observation, acquisition or transmission of paper or electronic data including voice);

1.1.2. loss of integrity of information either in storage or in transit (e.g. loss, corruption, contamination or obliteration of data including voice);

1.1.3. loss of availability of information due to failure or compromise of the Services;

1.1.4. unauthorised access to, use of, or interface with the Services by any person;

1.1.5. unauthorised breaches of physical security, including network elements, buildings and tools used by the supplier in the provision of the Services; and

1.1.6. use of the Services by any Third Party (including, but not limited to, a sub-contractor) in order to gain access to any computer resource of an authorised user unless the Company has explicitly permitted this in writing.

1.2. The Supplier must ensure that its Information Security Controls where applicable to the Services provided to the Company:

1.2.1. are contained within an up-to-date information security policy which is approved by the Supplier's management, published and communicated to all personnel;

1.2.2. meet all local and Applicable Security Law Requirements;

1.2.3. are substantially aligned with the information security requirements documented within the international ISO27001 standard; and

1.2.4. are compliant with this Schedule and accept that the requirements within it are subject to change to ensure continued protection of any Group Company and their respective clients and customers.

1.3. The Supplier will appoint an appropriate individual to act as the Supplier's Key Security Contact to:

1.3.1. act as the first point of contact for all the Company information security, physical security and BCM related questions, requests, issues and incidents;

1.3.2. attend all relevant meetings;

1.3.3. have or have access to Subject Matter Expertise in information security; and

1.3.4. either have authority to approve any technical or procedural changes required to maintain the security of the services or access to appropriate escalation routes within the Supplier's organisation to obtain prompt approval.

2. INFORMATION SECURITY RIGHT OF AUDIT

2.1. The adequacy of the Supplier's Information Security Controls will be periodically assessed (save in the case of a reasonably suspected breach by the Supplier of its obligations under this Appendix 6 or following any significant security breach) either by:

2.1.1. a direct on-site or remote assessment by the Company information security SMEs or an independent sub-contractor under the Company's general rights of audit under the Agreement; no more than once annually or

2.1.2. an ISAE3402, SSAE16, ISO/IEC27001:2013, PCI DSS v3.0 or other appropriate audit of Information Security Controls ordered by the Supplier and conducted by an independent party, but only where:

2.1.2.1. the date of such independent assessment, certification or audit is no more than twelve (12) months prior to the Company's request to assess the Supplier's Information Security Controls;

2.1.2.2. the Company accepts the scope as being adequate to prove Information Security Control standards for all Services; and

2.1.2.3. such output can be shared with the Company (allowing for reasonable redaction and/or appropriate non-disclosure agreements should this raise any issues of confidentiality); and

2.1.2.4. a regular or frequent cyber ratings report conducted and published by a reputable cyber ratings agency, where such output can be shared with the Company or the Company's client upon request.

2.2. The output of any direct on-site, remote or independent assessment must enable the Company to compare the adequacy of the Supplier's Information Security Controls against the standards of security required in the Agreement;

2.3. Where the Supplier's Information Security Controls (as assessed either by the Company or by an independent audit) are deemed to be inadequate, the Company and the Supplier shall agree on a remedial plan and a timetable for achievement of improvements. The Supplier shall notify the Company of remediation completion and shall allow the Company to conduct a further assessment if requested;

2.4. All expenses incurred associated with such an assessment by the Supplier, sub-contractors employed by the Supplier (or as the case may be, a Supplier Company) including all staff expenses of those organisations shall be the responsibility of the Supplier; and

2.5. The Company shall accept responsibility for all expenses incurred by its staff including expenses associated with the use of an independent sub-contractor only.

3. INCIDENT MANAGEMENT

3.1. The Supplier will:

3.1.1. implement a process for the management and reporting of security related incidents or suspected security incidents (including, but not limited to: (i) losses of data storage devices; (ii) destruction of, damage to, theft of, or unauthorised access to any store of the Company Data; and (iii) exploitation of any vulnerability in the Supplier's hosted networks, connections, applications, websites, or servers if such exploitation may impact the security of any the Company Data or otherwise damage the Company's reputation);

3.1.2. provide immediate communication of the actual or suspected security incident to the Company and to all persons accessing the Services in order for the Company to fulfil its obligations of timely notification to the ICO in accordance with GDPR Regulation;

3.1.3. promptly provide the Company with such assistance and co-operation as the Company may request in relation to the conduct of investigations into any confirmed incident which includes the preserving of any evidence if required for forensic analysis; and

3.1.4. test its Security Incident Management Process no less frequently than once in every twelve (12) month period.

4. INFORMATION ASSET MANAGEMENT

4.1. The Supplier shall implement and maintain an asset register which records all hardware, software and data assets, this register includes:

4.1.1. a Supplier owner for each asset; and

4.1.2. a record for each asset which defines its purpose, location and acceptable use in accordance with its information classification.

4.2. Any assets used for the Company Data shall manage information privacy appropriately and have established security controls for handling Personally Identifiable Information.

5. SUB-CONTRACTORS

5.1. Without prejudice to any other provision of the Agreement relating to sub-contracting, inform the Company of any functionality that is sub-contracted and to whom and ensure that:

5.1.1. each sub-contractor complies with all applicable requirements of this Appendix 6;

5.1.2. background verification checks of all Sub-Processors are carried out in accordance with relevant laws, regulations and ethics;

5.1.3. the Information Security Controls of each sub-contractor are regularly checked to confirm that they are adequate and are being operated effectively and that evidence of such checks is retained; and

5.1.4. where requested by the Company, provide the Company with evidence of the Information Security Controls of each sub-contractor to support any assessment, remediation, governance or incident investigation activity conducted pursuant to this Appendix 6.

6. ACCESS CONTROL

6.1. The Supplier will:

6.1.1. maintain and implement appropriate security systems, controls, policies and procedures to ensure the secure use of the Relevant Systems and any the Company Data held therein;

6.1.2. ensure that access to the Relevant Systems is only granted to those Supplier Personnel who reasonably need it for the purposes of delivering the Services;

6.1.3. ensure that access to the Relevant Systems by Supplier Personnel is restricted in accordance with the role or function of the individual and that access is added, modified, deleted and reviewed in a timely manner and in accordance with current policies;

6.1.4. ensure that background verification checks on all candidates for employment are conducted in accordance with relevant laws, regulations and ethics; and

6.1.5. ensure all users are authenticated by using an identifier (e.g., a User ID) and an authenticator (e.g., a password).

7. REMOTE ACCESS SECURITY

7.1. The Supplier shall ensure that controls are in place to prevent unauthorised remote access to the Relevant Systems. Such controls shall include, without limitation:

7.1.1. any remote access to Relevant Systems shall use industry approved remote access tools and strong authentication;

7.1.2. all data travelling across a remote access mechanism shall be encrypted from the end-point (e.g. laptop) to the network;

7.1.3. all attempts to connect to the Relevant Systems using an unauthorised remote access mechanism shall be rejected and logged; and

7.1.4. all such remote access logs shall be reviewed, and any suspicious activity investigated.

8. CUSTOMER ACCESS TO THIRD PARTY SYSTEMS

8.1. The Supplier will ensure that all aspects of individual customer access to the organisation's business applications meet security requirements by:

8.1.1. maintaining a documented standard or procedure for the provision of customer access to the organisation's business applications;

8.1.2. controlling the means of authentication to ensure each customer is uniquely identified, type of access is appropriate and maintain a record of all authentication activity; and

8.1.3. installing a single point of contact or call centre for handling customer access queries or security issues.

9. THIRD PARTY ACCESS & SYSTEM MAINTENANCE TO COMPANY SYSTEMS

9.1. The Supplier shall ensure that any and all access to any Company Systems by any sub-contractor or the Supplier (or, as the case may be, of a Supplier Company) including to perform maintenance, either on site or remotely will:

9.1.1. be covered by an active contract between the Supplier (or the applicable Supplier Company) and applicable Sub-contractor which contains non-disclosure provisions no less robust than the non-disclosure provisions set out in this Agreement before access is provided;

9.1.2. is approved in advance in writing by the Company and managed in tandem with an assigned Company or Company employee and is restricted to specified individuals only;

9.1.3. has defined objectives and scope agreed with appropriate Company supplier relationship personnel prior to the commencement of any planned Maintenance and Support activities;

9.1.4. restricts access rights to the minimum level required to perform the Maintenance and Support activities and disables access rights immediately following completion of those activities; and

9.1.5. is reviewed and revalidated on a regular basis to ensure that, inter alia, any access no longer required is removed in a timely manner.

10. STAFF SECURITY, TRAINING AND AWARENESS

10.1. The Supplier shall ensure that all persons accessing the Relevant Systems are screened prior to employment, trained in and aware of the provisions of this Appendix 6 and their responsibilities by:

10.1.1. ensuring that robust background verification checks on all candidates for employment are conducted in accordance with relevant laws, regulations and ethics;

10.1.2. documenting information security responsibilities for all employees throughout the organisation which include security responsibilities in job descriptions and terms and conditions of employment; and

10.1.3. providing induction training for all new employees and ongoing training for all staff with specific coverage of information security.

11. MEDIA AND MOBILE DEVICE SECURITY

11.1. The Supplier will:

11.1.1. not store Company Data on unencrypted portable storage devices such as external hard drives, USB sticks, laptops or portable backup media;

11.1.2. not store Company Data on any personally owned mobile or smartphone devices;

11.1.3. ensure that any corporately owned mobile or smartphones devices are appropriately approved, password protected, encrypted and configured to prevent unauthorised access; and

11.1.4. ensure that all Company Data held on removable media (disks, memory sticks, etc) is encrypted using at least AES 128bit.

12. DATA TRANSFER SECURITY

12.1. The Supplier will ensure that:

12.1.1. all Company Data sent over any email system has appropriate Transport Layer Security (TLS) in place;

12.1.2. all Company Data sent over the internet using any known internet protocols (e.g. FTP, SMTP) is encrypted using a minimum AES 128bit encryption mechanism whilst in transit; and

12.1.3. instant messaging over external networks and text messaging is not used to communicate Company Data.

13. CRYPTOGRAPHIC CONTROLS

13.1. The Supplier shall implement appropriate cryptographic controls to ensure that:

13.1.1. the confidentiality of all Company Data is protected using industry recognised appropriate encryption strength and algorithms, both in transit and at rest; and

13.1.2. only trusted keys and certificates are accepted, and that the protocol in use only supports secure versions, with approved length and with appropriate generation and management of those keys.

14. DATA STORAGE & DISPOSAL

14.1. The Supplier shall ensure that:

14.1.1. all information is secured under lock and key if left unattended by Supplier Personnel and its access is appropriately restricted;

14.1.2. any IT assets and electronic media that are being used to store only Company Data but which are no longer required are destroyed by incineration or damaged beyond repair by an industry recognised method;

14.1.3. all electronic Company Data is erased using data erasure technology that confirms it is not recoverable; and

14.1.4. any paper documents containing Company Data which are no longer required are disposed of by shredding, using a third-party data disposal organisation or appropriate internal disposal means.

15. SYSTEM DEVELOPMENT LIFECYCLE (SDLC) SECURITY

15.1. The Supplier will operate a robust System Development Lifecycle (SDLC) which includes information security requirements that must be implemented on all software elements supporting the Service, ensuring that:

15.1.1. there is clear segregation of environments between all environments, including but not limited to, Development Environments, Testing Environments and Production Environments;

15.1.2. developers have no access to any Production Environments and are not able to promote code to any Production Environments;

15.1.3. all system changes affecting project and support environments are reviewed to ensure that they do not compromise the security of those environments;

15.1.4. all system changes and associated code is approved by the appropriate Supplier manager prior to the deployment of any such change to the Production Environment;

15.1.5. secure coding standards are documented, followed and appropriately reviewed prior to deployment;

15.1.6. source code, including all software under development, is appropriately controlled including being securely stored, version controlled, protected from unauthorised access and fully tested in a lesser environment prior to deployment to any Production Environment; and

15.1.7. no Company Data classified as 'RESTRICTED' or 'CONFIDENTIAL' is stored or used at any time in any Development or Test Environment.

16. THIRD PARTY NETWORK MANAGEMENT

16.1. The Supplier will take all steps necessary to safeguard the security of their network through:

16.1.1. restricting access to the network to only Supplier Personnel approved in advance by an appropriate manager within the Supplier's organisation to access any Supplier Network;

16.1.2. implementing controls which ensure that any Supplier Network is used only for its intended business purpose;

16.1.3. configuring network devices (including routers, switches and firewalls) to ensure they do not compromise the security of the network;

16.1.4. creating specific firewall rules that control and limit the level and type of network activity which are routinely reviewed and changed only via change request including approval by an appropriate network manager;

16.1.5. implementing network logging and monitoring capability which includes, but is not limited to, logging of all unauthorised authentication attempts; and

16.1.6. limiting remote maintenance of Supplier Systems and Networks to only essential maintenance by authorised individuals confined to individual sessions.

17. THIRD PARTY APPLICATIONS

17.1. The Supplier shall ensure that any and all Supplier Systems used by the Supplier or any sub-contractor for the purposes of providing Services to the Company will:

17.1.1. be appropriately segregated from other internal or untrusted networks;

17.1.2. have appropriate, and up to date, security controls such as patches, encryption, firewall protection and Anti-Virus where relevant;

17.1.3. limit access to a least privilege principle for all internal and external employees;

17.1.4. follows appropriate password configuration and management guidelines, including but not limited to instructing employees to:

17.1.4.1. keep passwords or memorable words confidential by not sharing with any other person, writing passwords down or storing them in any IT function or facility;

17.1.4.2. change passwords immediately if there is an actual or suspected breach of password security;

17.1.4.3. regularly change passwords as required by the Company Systems to maintain security; and

17.1.5. not access, use or attempt to access or use the Company Systems using any other person's credentials.

17.2. Passwords will be automatically revoked after five (5) consecutive unsuccessful log-on attempts. Resetting of passwords where revoked or forgotten will be carried out as determined by the Company from time to time.

18. THIRD PARTY INFRASTRUCTURE

18.1. The Supplier will have appropriate operating procedures for the management and operation of all information processing facilities, including e-commerce environments by:

18.1.1. maintaining policies and procedures for system maintenance;

18.1.2. standardised system builds for all Supplier Systems and Supplier Network devices;

18.1.3. conducting regular logging and monitoring of all information security events and user activity on Supplier Systems which detects any unauthorised access, modification or deletion of data;

18.1.4. implementing a secure wireless solution which ensures that all requirements are authorised, authenticated, restricted appropriately and protected from unauthorised access; and

18.1.5. implementing appropriate encryption for all wireless traffic.

19. PATCHING AND ANTI-MALWARE

19.1. The Supplier will have a centrally managed anti-malware solution. Anti-malware protection will be in place on all devices used at any time to store or process Company Data and malware signatures on any network connected device will include latest updates from the anti-malware supplier at all times.

19.2. The Supplier will have a process for dealing with actual or suspected malware infections to ensure that any potential or actual security breaches linked to infections are promptly investigated and notified to the Company.

19.3. The Supplier will have a process for:

identifying and risk-assessing all new patches made available for systems storing or processing Company Data;

the timely testing and implementation of patches in non-Production Environments;

authorising implementation of patches before they are applied to production systems;

rolling back implemented patches without operational impact on Services if required; and

maintaining records of all patching activities.

20. INTRUSION DETECTION

20.1. The Supplier will operate appropriate Intrusion Detection mechanisms for all and any Supplier Systems and Supplier Networks to identify predetermined and new types of attack.

20.2. Intrusion Detection methods should be supported by documented standards or procedures;

20.3. Intrusion Detection mechanisms should identify activity typically associated with malware or traffic originating from known malicious IP addresses or network domains, known attack characteristics or unusual or anomalous behaviour; and

20.4. Intrusion Detection mechanisms should be configured to incorporate new or updated attack characteristics, provide alerts when suspicious activity is detected, and allow for suspected intrusions to be analysed and potential business impact assessed.

21. WEB SERVICES SECURITY

21.1. The Supplier will:

21.1.1. conduct penetration testing of any interfaces to be used by the Company, the clients and customers of the Company or of any Group Company. In respect of such penetration testing, the Supplier will:

21.1.1.1. ensure that the scope is agreed with the Company;

21.1.1.2. ensure that the penetration testing supplier is agreed with the Company;

21.1.1.3. where a penetration test is conducted by the Supplier, provide the Company with a copy of the report which confirms the penetration testing company used, date of the test, scope and key findings; or

21.1.1.4. allow the Company to perform its own penetration testing where the Supplier either does not perform its own testing or does not perform it to a level acceptable to the Company.

21.1.2. conduct regular vulnerability scans of all:

21.1.2.1. internet-facing interfaces;

21.1.2.2. internal systems that store or process Company Data; and

21.1.2.3. network components (including, but not limited to, firewalls) that protect systems storing or processing Company Data;

21.1.3. ensure that any output of the vulnerability scans is made available to the Company for scrutiny upon request;

21.1.4. ensure that any vulnerabilities identified are remediated and that any associated risks are properly articulated and effectively managed; and ensure that any vulnerabilities identified that cannot or will not be remediated are communicated to the Company with appropriate explanation.

22. PUBLIC CLOUD SERVICES

22.1. The Supplier will:

22.1.1. not store, host, or process any Company 'RESTRICTED' or 'CONFIDENTIAL' information in any Public Cloud Service without the prior written consent of the Company;

22.1.2. provide adequate assurance of the Public Cloud Services provider's security controls by allowing the Company access to any or all of the following:

22.1.2.1. documentation relating to the Supplier's due diligence activity in respect of the Public Cloud Services provider;

22.1.2.2. ISAE 3000, ISAE 3402, SSAE16 or any similar independent SOC II audit of the Public Cloud Services provider; and

22.1.2.3. where applicable, details of the scope and certification status of ISO/IEC 27001:2013.

23. PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS

23.1. Where end user initial or full payment for Goods and/or Services is made using a debit or credit card, the Supplier will ensure (and will procure that any sub-contractor ensures) that the Services (and any component thereof) are compliant with the latest Payment Card Industry Data Security Standard version and will, upon request, provide to the Company evidence demonstrating compliance with this Clause 23.

24. CONTRACT EXPIRY

24.1. Without prejudice to any other provisions of this Agreement regarding the consequences of termination and/or exit (and in addition to those provisions), upon the expiry or termination of this Agreement, the Supplier shall:

24.1.1. assist the Company in performing a termination review detailing the nature, type and classification of Company Data held within the Supplier, Supplier Company (or, as the case may be, of a Supplier Company's) sub-contractors network and the requirement to retain any the Company Data following Agreement expiry or termination;

24.1.2. assist the Company in the system extraction, packaging and return (in a format mutually agreed) and/or destruction of all the Company Data from all sources, networks and devices;

24.1.3. ensure that all physical or logical assets, intellectual property and licences are returned, and physical and logical system access to the Company Data or the Company Systems is revoked within timescales agreed with the Company;

24.1.4. confirm in writing to the Company that the Company retains the right to perform a periodic assessment of the Supplier to confirm the adequacy of the Supplier's Information Security Controls, where Company Data is retained post contract expiry no more than once annually (pursuant to Clause 3.1 of this Appendix 6); and

24.1.5. provide appropriate notification and assistance to the Company should a data breach occur where Company Data is directly or indirectly impacted (pursuant to Clause 3 of this Data Security Appendix).

25. PHYSICAL SECURITY MANAGEMENT

25.1. The Supplier shall be responsible for all aspects of the physical security in relation to the Services provided, Company Assets whether they reside with the Suppliers operating facility, Supplier Company's (or as the case may be, of a Supplier Company's) sub-contractor logical or physical premises and shall ensure that:

25.1.1. appropriate Physical Security Controls will be implemented in order to protect all Company Assets whilst in their possession, custody or control and shall take action to safeguard them;

25.1.2. its Physical Security Controls are aligned with the physical security requirements in international standard ISO/IEC27001:2013 as a minimum; and

25.1.3. the Company are informed promptly upon identification of any Physical Security Incident which could cause an exploitable vulnerability to the physical security profile of the Company or any other company within the Company's Group, and will provide the Company with such assistance and co-operation as the Company may reasonably request in relation to the conduct of any investigation into any Physical Security Incidents.

26. BUSINESS CONTINUITY MANAGEMENT

26.1. The Supplier shall have a documented Business Continuity Management Programme and associated Business Continuity Plans enabling it to restore Goods and/or Services to an acceptable predefined level should a Business Continuity Incident occur and shall ensure that:

26.1.1. each Business Continuity Plan is reviewed and approved by the Supplier's senior management at least annually;

26.1.2. both the Business Continuity Management Programme and associated Business Continuity Plans reflect relevant regulations and guidance issued by the appropriate regulatory authority and shall be managed to a standard no lower than ISO22301;

26.1.3. all Business Continuity Plans shall have clearly documented Business Impact Analysis, Recovery Time Objectives, Recovery Point Objectives and Minimum Business Continuity Objective;

26.1.4. all Business Continuity Plans are exercised at least annually, the Company informed of the dates of planned exercises and the results and corrective action plans made available to the Company upon request;

26.1.5. all relevant staff are appropriately trained to recognise what a Business Continuity Incident is, and are familiar with the conditions on which a Plan will be invoked, and suitably trained in the steps required to enable the recovery solution; and

26.2. the Supplier shall notify the Company immediately of any potential invocation of the Business Continuity Plan, provide ongoing updates to the Company in line with the agreed escalation process and provide a post incident report within forty-eight (48) hours of the Services being resumed outlining all steps undertaken during invocation.

Data Security Schedule – Short form

Information Security, Physical Security & Business Continuity Management

Business Continuity Plan	a plan produced by the supplier invoked upon the occurrence of a business continuity event which provides step by step guidance around the recovery of services to an agreed recovery point.
Industry Standard	Alignment to ISO/IEC27001: information security international standard
Information Security Controls	controls to protect the confidentiality, integrity, or availability of data
Physical Security Controls	controls to prevent unauthorised physical access to supplier or sub-contractors premises.
Public Cloud Services	any data hosting, processing or storage service which is provided to the Supplier by a third party, where the service is provided on infrastructure owned and located at the third party's premises, and the service is made available over the internet using infrastructure shared amongst customers
Williams Lea Data	all data (including but not limited to Williams Lea (WL) customer data), tables, information, text, drawings, codes, diagrams, images, or sounds which are embodied in any electronic or tangible medium, including compilations of any of the foregoing, and which are: (a) processed by, or a product of, the services. (b) generated by the supplier or a sub-contractor of the supplier in carrying out the Supplier's obligations under this Agreement; or (c) generated by or on behalf of WL or a WL Company
Williams Lea Systems	systems of WL or any WL Company

1. **Introduction**

The supplier shall be responsible for all aspects of the security of the services provided by them, or any third party engaged in the performance of any element of the services, including the requirements around Confidentiality, Integrity, and Availability.

Any continued failure to remediate an identified deficiency or material breach of this Schedule by the supplier shall entitle WL to terminate this Agreement immediately on written notice to the supplier.

2. **Information Security Requirements**

The supplier must ensure that its Information Security Controls are contained within an up-to-date information security policy and are substantially aligned to the industry best practice ISO27001 standard.

The supplier will allow its Information Security Controls to be periodically assessed via an on-site or remote assessment by a WL or independent assessor or via a regular and frequent cyber rating review and report undertaken by a reputable cyber ratings agency under WL's general right of audit. Where the output of such an assessment identifies potential security control failings, the supplier shall agree on a remedial plan and a timetable for achievement of improvements.

3. **Incident Management**

The supplier will implement a process for the management and reporting of security related incidents or suspected security incidents and will provide WL immediate notification upon discovery of any actual or suspected incident.

If the incident is confirmed the supplier will provide WL with such assistance and co-operation as WL may request in relation to the conduct of investigations which includes the preserving of any evidence if required for forensic analysis.

4. **Sub-Contractors**

The supplier shall seek approval from WL of any sub-contractor used in the servicing of the Agreement. The supplier will attest as to the security maturity of each of its sub-contractors, will provide WL evidence of recent

third-party assurance it has undertaken on each of them and accepts that it is legally liable for the compliance of those third parties' operations with this schedule.

5. **Staff Security, Training and Awareness**

The Supplier shall ensure that all employees are screened prior to employment, trained in and aware of the provisions of this Schedule. All employees must have security responsibilities detailed within their job descriptions and terms and conditions of employment and regular security training is undertaken throughout their employment.

6. **Data Storage & Disposal**

The supplier shall ensure that all WL Data held either logically or physically by them is secured appropriately and destroyed when no longer required either through shredding or incineration for paper-based asset or through WEEE regulation aligned methods for electronic information.

7. **Access Management to WL Systems**

The supplier shall ensure that any access to WL Systems is strictly controlled only to supplier or sub-contractor employees approved in writing by WL and is managed in conjunction with a WL employee. All access is based on least privilege and is regularly reviewed and removed immediately when no longer required.

8. **Access Management to Third Party Systems**

The supplier shall ensure that appropriate access is provided to all employees based on a principle of least privilege, restricted to authorised users only, subject to regular recertification and revalidation and is added, modified, and deleted in a timely manner.

The Supplier shall ensure that all access, including remote access, will require strong authentication controls, in particular clear password configuration aligned to Industry Standard.

9. **Application Security to Third Party Systems**

The supplier shall ensure that all systems used by the supplier, or any sub-contractors are appropriately configured in order to logically segregate WL data from other clients and have current security controls in place such as patches, encryption, and anti-virus protection.

10. **Data Transfer Security**

The Supplier shall ensure that all WL data sent via email or through any recognised internet protocol is appropriately encrypted to a minimum AES 128bit mechanism using an industry recognised tool. Where relevant trusted keys and certificates are to be used and must have appropriate management procedures in place.

11. **Third Party Network Management**

The supplier must restrict access to its network to only approved supplier or sub-contractor personnel. Network security controls must be implemented including firewalls, device hardening, secure wireless, and the recording of all activity undertaken and stored within logs for scrutiny.

Intrusion detection systems must be configured to incorporate new or updated attack characteristics, provide alerts when suspicious activity is detected and allow for suspected intrusions to be analysed and potential business impact assessed.

Anti-malware protection must be in place on all devices used at any time to store or process WL Data and a process for dealing with actual or suspected malware infections must be in place.

A process for managing patching activity should include risk-assessing of all new patches, testing of all patches, approval of deployment within a system of record and processes for deployment.

12. **Web Services Security**

The supplier must conduct penetration testing of any externally facing system to be used in support of WL business. The supplier must allow WL access to the scope of the test, output of any test and sight of remediation plans, with timelines, where findings have been identified.

The supplier must conduct regular vulnerability scans of all internal systems that store or process WL Data and all network components that protect those systems. The supplier must, where required by WL, make available those scan results or provide a regular report which details the vulnerabilities identified and remediation plans, with timelines, to fix.

13. **Public Cloud Services**

The supplier will not store, host, or process any WL information in any Public Cloud Service without the prior written consent of WL and will provide assurance of the Public Cloud Services provider's security controls prior to engagement.

14. **Contract Expiry**

The supplier will in good time, upon notification of contract termination or expiry, assist WL in performing a termination review, identifying all data to be extracted, packaged, and returned and execute the return of all data or delete where return is not possible.

15. **Physical Security Management**

The supplier shall be responsible for the physical security of all supplier or WL owned devices stored within their premises. The supplier will ensure that appropriate Physical Security Controls will be implemented which are aligned with the physical security requirements in international standard ISO/IEC27001 as a minimum.

16. **Business Continuity Management**

The supplier shall have documented Business Continuity Plans enabling it to restore products and services to a predefined level. Each Business Continuity Plan shall be reviewed, tested at least annually, and compiled to reflect the industry best practice standard ISO22301. The supplier shall notify WL immediately of any potential invocation of the Business Continuity Plan, provide ongoing updates to WL in line with the agreed escalation process and provide a post incident report within 48 hours of the services being resumed outlining all steps undertaken during invocation.

Supplier Signature	Role	Date
_____	_____	_____

APPENDIX 7

VETTING

Introduction

The Company works with a range of clients and industry sectors across the EMEA Region. The Company's employees are often responsible for the creation, production and/or distribution of client Documentation, which may contain confidential and business critical information. The Company's screening processes for all temporary workers and permanent employees have therefore been developed to ensure:

- The integrity and quality of all the Company's personnel
- 100% compliance to the Company's contractual requirements
- Support the Company's Risk Mitigation Strategy

The Company's screening processes are regularly reviewed in line with increasing legislation and industry regulation to ensure they meet requirements of both the law and clients in each country in which the Company operates.

Please note failure to comply or pass the security screening in a timely manner may result in withdrawing from any contractual relationship with the Supplier.

Policy Statement

The Company is committed to carrying out pre-employment screening on any potential employee prior to confirmation of permanent or temporary appointment. We will ensure existing employees or those joining us through TUPE transfers meet the same requirements unless indemnification is provided in the client agreement.

Eligibility

This policy applies to all Supplier Personnel.

Countries in Scope

The following countries are considered in scope under this policy:

UK, Belgium, Czech Republic, Finland, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Poland, Romania, Russia, Spain, Ukraine

General Principles

The Company requires all workers to comply with either Standard Level or High-Level security screening. The level of screening is determined by the client site or the role of the employee and is influenced by the level of exposure an employee has to confidential and secure information.

All checks should be carried out in each country as outlined in the policy unless prohibited under specific in-country data privacy or employment law.

The checks at each level currently encompass the following:

Standard level (level 1)

- Proof of Identity
- Proof of Eligibility to Work in Country
- 2 years address verification (provided on a recent utility bill, bank statement or Government issued correspondence)
- 2 years employment referencing via HR departments, previous managers, work books or job certificates and/or education history where applicable, with gap analysis

High level (level 2)

- Proof of Identity
- Proof of Eligibility to work in-country
- 5 years Address Verification (provided on a recent utility bill or bank statement or Government issued correspondence)
- 5 years Employment Referencing via HR departments, previous managers, work books or job certificates and/or education history where applicable, with gap analysis
- Verification of Highest Education
- Criminal Records Check (Disclosure Scotland, Certificate of Good Conduct, Criminal Extract, Police Certificate as applicable)
- Credit Check to highlight any County Court Judgement's, Individual Voluntary Arrangements or bankruptcies (where available)
- Global Sanctions Check to reference international financial enforcement and sanctions bodies

In addition to these checks, there may be additional forms to be completed at either level which are client specific such as a confidentiality agreement or other security documentation. These forms will be administered and completed locally.

The requirements per country can be identified in the country matrix on page 8 of this policy. The Company reserves the right to request further relevant information if required.

Returning to the Company employment

If an individual has previously been employed by the Company and is returning to the Company's employment, they will always be required to participate through the screening process again. This applies regardless of whether the employee previously worked on a temporary and/or permanent basis.

The only exception to this is if the employee has a gap of less than three months in their employment with the Company. In this instance no further screening will be required as their screening details will still be on file. If the gap in their employment with the Company is greater than six months, the gap will be investigated and re-screening will take place.

Moving internally within the Company

If a recruiting manager offers a secondment or permanent position to an existing employee and therefore instigates an internal transfer, both managers are responsible for ensuring the screening of that employee is sufficient for the new role they are moving into.

Dispensation

Individuals are not permitted to commence work without a full clearance completion certificate being issued. If the site requires the individual to commence prior to the completion certificate being issued, a Dispensation Form must be signed off by the Client Services Director and sent to Resourcing prior to the individual commencing employment or internal transfer. The request will then be sent to the relevant HR Director for final sign off.

What checks will be carried out?

Proof of Identity

The Company requires verification and confirmation of the individual's identity. This will usually be original documents, either:

- Passport or Travel Document (must provide a copy of front cover and photo page, **plus** any pages relating to a visa, entry clearance, or right to work scheme etc), or
- Full Birth Certificate identifying the individual as a country national (must detail at least one parents details including place of birth)
- National Identity card
- All pages of the chosen form of ID must be signed and verified in the following way:

- Printed name of person verifying the documents
- Signature of person verifying the documents
- Date the documents are verified
- And using the words of “True and certified copy" – please note that no other alternative words are permitted
- All ID must be signed on the same date and by a manager and can be emailed to Resourcing

Eligibility to work in-country

The Company requires verification and confirmation of the individual’s eligibility to work in the country in which they are working. Any restrictions are highlighted by our external provider.

- Passport identifying the individual as an EU or EEA National
- National Identity card
- Biometric Identity Card for Migrant Worker (UK Only)
- Official Birth Certificate (long version if UK) **plus** proof of National Insurance or Social Security Number
- Residence Permit demonstrating the individual is eligible to work in-country (limited or indefinite)
- Visa documents identifying eligibility to work in-country issued by relevant Immigration Directorate or Embassy
- Accession Worker Registration Certificate (Croatia only) Croatia is the only EU/EEA Country where there are any restrictions on employing nationals in the UK. Croatian nationals require Home Office authorization to work in the UK. Once a Croatian has completed 12 months continuous employment they become exempt from the workers registration requirement and are allowed the same rights as any other EU/EEA National.
- Official Documentation from country Immigration Directorate indicating eligibility to work
- All pages of the chosen form of Eligibility to Work documents must be signed and verified in the following way:
- Printed name of person verifying the documents
- Signature of person verifying the documents
- Date the documents are verified
- And using the words of “True and certified copy" – please note that no other alternative words are permitted

(Further guidance can be found in the Identity and Right to Work Check Guidance)

Proof of address

The individual’s current address will be confirmed by the individual providing proof of one of the documents below. This must be dated within the last three months and can be any of the following original documents (further guidance can be found in the Proof of Address Reference Guide):

- Utility bill (gas, electricity, water, state social security tax documents)
- Bank, building society or credit card statement
- Tenancy / mortgage agreement or statement
- Insurance document (must be a current insurance)
- Payslip (containing the individual’s address)
- A search of publicly available UK Electoral Roll at the individual’s current and previous addresses will be carried out

Please note that a mobile phone bill will not be accepted as a proof of address document.

All pages of the chosen form of proof of address must be signed and verified in the following way:

- Printed name of person verifying the document
- Signature of person verifying the document
- Date the document is verified
- And using the words of “true and certified copy" – please note that no other alternative words are permitted

All documentation must be signed on the same date (if more than 1 copy) and by a manager and can be emailed to Resourcing.

Employment History

This will seek to confirm a 2 years history for standard screening and 5 years history for high level screening. Confirmation of full employment history will be from the appropriate HR Department and/or Line Managers (from previous employers) - in writing. If references cannot be collected or are culturally not issued the following proof may be considered:

- Job Certificates
- Official Work Books
- Wages/pay slips, State Taxation Documents
- Employment Contract and Communications
- For Pensioner - proof of receipt of pension payments

If employment history is not available, then the requirement is to check for the highest educational references available.

Any periods of self-employment will need to be confirmed by the individual's accountant, solicitors or by State Social Security communication, e.g. tax return and bank statements.

Employment Gaps

The Company will check any gaps in employment history above three months, or following a period of redundancy or when the individual was in full time education. The evidence that may be requested is outlined as follows:

Redundancy - evidence of a period of redundancy should be provided by formal documentation relating to the terms of redundancy or evidence of the payment (this doesn't have to be in the period being referenced), taxation and wage documentation.

Unemployment – individuals should contact the state unemployment office to provide a letter from the country's relevant Social Security Department confirming payment of benefits to the individual or confirming non-employment status, or, a Bank Statement evidencing receipt of benefits. Individuals who were searching for employment should be able to provide confirmation emails or letters from direct employers or employment agencies, confirming receipt of CV / application forms, interview details, or refusals.

Voluntary work - written evidence of voluntary work during the period on the headed paper of the institution concerned.

Travelling abroad - individuals that have been travelling should be able to provide stamps in their passport. Individuals may have to show old passports and the Company must ensure ALL visa stamps from a passport are copied and date certified. If passport stamps are not available the following proof may be collected; hotel, car hire & card receipts, sole bank statement evidencing overseas transactions during the period, inoculation records, formal documentation from a recognised travel company/airline for booking or travel during the period in question (including flight confirmations, train, boat tickets or car hire), bank account statement showing transactions in relevant currency if combined with additional verification which supports.

Sabbaticals - formal documentation from the employer confirming the sabbatical and outlining the terms.

Maternity / Paternity / Carer - individuals caring for children should provide a child's birth certificate within the period, up to 16 years maximum, Notice of Award of child benefit payments during the period or formal confirmation of award of child tax credit in respect of the birth of the child. If not the parent, a link to relationship must be established with documentary evidence. Individuals with other caring responsibilities should provide evidence of allowances received, death certificate, power of attorney or doctor's note/communication.

Medical illness - individuals should be able to provide a medical certificate covering the period or documentation from a medical practitioner or establishment that verifies that the individual was undergoing treatment during that period.

Character References - the Company will only accept character references if no other evidence relating to the gap can be

provided. Please note that under Level 3 requirements, character references are not accepted and other client terms may vary.

Academic Qualifications

The requirement is to provide the highest academic qualification attained at degree or higher diploma level. Secondary education or in-country equivalent will only be confirmed if attained in the last 6 years.

- The following can be accepted as proof of full-time education (at least 20 hours per week) for Graduates, University Leavers and Mature Students
- University/College letter of acceptance, which must be on headed paper, be issued by a recognised University/College (i.e. Government funded) and not a language school (unless an international student) and must confirm acceptance of student onto course and address must match POA (or dated in period of previous address)
- Student Loan Company/LEA/SAAS Award letter (UK only), which must match that on POA (or dated in period of previous address)
- Educational Certificates
- Confirmation of withdrawal from University including relevant dates
- Introduction from a recognised University/College (as above), which must be addressed to the individual or the bank, must be on headed paper or carry an appropriate stamp and must confirm the individuals name date of birth & course, be current or dated within the period of the previous address

Where existing employees are being screened for client site requirements, academic qualification checks may not be required.

Criminal Record Check (CRC)

Criminal checks will be conducted to cover the last 7 years, unless otherwise restricted. This check will identify any criminal activity recorded against the individual. For most EMEA countries the Company utilise jurisdictional court records to ascertain an individual's criminal history (Standard and High-Level Country Matrix outlines where this is not permissible). In the UK a Basic Criminality Disclosure Certificate is obtained from Disclosure Scotland verifying all unspent convictions under the Rehabilitation of Offenders Act 1974. For all countries results are compared to candidate's self-declaration and any adverse findings are advised to the client for a decision.

Please note it is a contractual requirement for the Company employees to declare any criminal convictions during employment either via their line manager or to HR.

Financial Probity Check

Identify any adverse financial information recorded against the individual. This check covers adverse credit history, registered debts, including Bankruptcy, Court judgments, Scottish Decrees and Creditor Voluntary Arrangements. Only credible Credit Reference Agencies should be used to perform such checks. Credit information is limited across the EMEA region and the nature of the information reported is not uniform (Standard and High-Level Country Matrix outlines where this is not permissible). All adverse findings will be validated through current address verification procedures and advised to the client for a decision.

Please note it is a contractual requirement for the Company employees to declare any financial sanctions during employment either via their line manager or to HR.

Global Sanctions Check

Requirement to check for sanctions and enforcements imposed by a financial regulator for regulatory misdemeanours, debarment lists and any other information. A cross reference check is carried out against the world's leading financial sanction and enforcement bodies, which includes international warrants issued by law enforcement bodies.

International checks

When recruiting in-country, individuals may have previously lived and worked in other countries during the time period which is being verified. In such cases Individuals will need screening checks carried out in the specific countries in which they have worked or lived within the time period (where permissible and available) which will be charged at an additional cost.

Standard and High-Level Country Matrix

Individuals who have worked or lived abroad will need screening checks carried out from that specific country which will be determined by their residency and employment history and their availability governed by in-country legislation and privacy laws as outlined below.

Country	ID Checks	Proof of Right to Work	Address Checks	Highest Education Check	Professional Qualifications	Employment Referencing	Financial Probity Checks	Criminal Records Check	International Sanctions List Check
Belgium	Yes	Yes	Yes	Yes	Yes				
Czech Republic			Yes	Yes	Yes				
Finland			Yes	Yes	Yes				
France			Yes	Yes	Yes				
Germany			Yes	Yes	Yes				
Ireland			Yes	Yes	Yes				
Italy			Yes						
Luxembourg			Yes	Yes	Yes				
Netherlands			Yes	Yes	Yes				
Poland			Yes	Yes	Yes				
Romania			Yes	Yes	Yes				
Russia			Yes	Yes	Yes				
Spain			current address only	Yes	Yes	Yes	Yes	Yes	Yes
Ukraine	Yes	Yes	Yes	Yes	Yes				

Third Parties and Sub-Contractors

It is both the Company policy and the expectations of our clients that all individuals engaged on client sites are appropriately screened to the same standard. It is the managers' responsibility to ensure that all individuals are security screened to the appropriate level for the site and that any third parties and subcontractor companies have fulfilled the requirement as outlined in this policy for their own employees.

Further guidance can be obtained from the Company Procurement on the contractual obligations for all known suppliers and sub-contracting companies.

APPENDIX 8
SUPPLIER INVOICING INSTRUCTION

The Williams Lea Group of Companies operate a strict process for payment of supplier invoices. Please ensure that you follow the guidelines provided in this document. Any invoice that does not follow these guidelines will be returned to you unpaid. These guidelines apply to all Global Williams Lea companies.

EMAIL INVOICE

Please send your invoices to the email address below.

Americas, Europe & Middle East, India & APAC (Except Below)	WL.AP@Williamslea.com
For Japan, Hong Kong, Korea, Taiwan, China	WL.GC-INV@williamslea.com
TSO Mailbox info	invoicescanning@tso.co.uk

Your invoice must be a correct and legal invoice. Invoice must be sent via PDF to the proper email address above without any restrictions, such as printing, editing or password protection. Payment terms are based upon the date of receipt to the email address above. Please ensure that the following details are correct otherwise your invoice will be returned:

Your invoice must include:

- WL Purchase Order (P.O.) number
- Invoice must be addressed to the proper WL entity per the P. O.
- Invoice must match the P. O. details for value, quantity, and price.
- Supplier's name, address, email address and contact telephone number.
- Invoice number, invoice date, quantity, amount (net and gross)
- PDF file name must be unique. Any duplicate file names will not be processed. PDF file can only contain one invoice however, you can send multiple PDFs on one email. You can include supporting documents in this PDF but only one invoice per PDF.
- Please do not send zipped files.
- A black and white invoice format is preferable.
- No Zipped files will be accepted.

Most of the above information is included in the Purchase Order (PO) we send to you. Please ensure you receive a copy of the PO from your WL contact before delivering goods/services and issuing your invoice. Invoices that do not match these requirements, will not be processed, and will be returned to you for correction.

STATEMENT & QUERIES & SUPPORT

Americas, Europe & Middle East, India & APAC (Except Below)	WL.Statements@williamslea.com
For Japan, Hong Kong, Korea, Taiwan, China	WL.GC-AP@williamslea.com
For TSO	invoicebooking@tso.co.uk

Please send queries and your Statements to the email address below based on your region of business.

Americas, Europe & Middle East, India & APAC (Except Below)	WL.SST@Williamslea.com
For Japan, Hong Kong, Korea, Taiwan, China	WL.GC-AP@williamslea.com