Accredited Assessment Services

Terms and Conditions

Customer identified in the Proposal Document agrees to acquire the Services described in in the Proposal Document in accordance with the provisions of this Agreement

1. Definitions

The following terms, whether in the singular or plural thereof, shall have the meanings ascribed to them below

.

"Affiliate"	means an entity directly or indirectly controlling, controlled by or under common control with a party, where control means the ownership or control, directly or indirectly, of fifty one percent (51%) or more of all of the voting shares; provided that an entity shall be considered an affiliate only for the time during which such control exists.
"Agreement"	means the Proposal Document together with these Accredited Assessment Services Terms and Conditions.
"Accredited"	means that the Services are provided in accordance with processes defined by an accreditation body.
"Auditor"	means SAI Global's employees, agents and contractors who perform the Services.
"Services"	means the accredited assessment services rendered by SAI Global or its agents and contractors to assess a Management System/ product/process/service and determine if the Management System/ product/process/service complies with an applicable Standard within the scope of accreditation of SAI Global, and if compliant, issuance of an Accredited Certificate.
"Accredited Certificate"	means the Certificate issued under a Standard included in the scope of accreditation of SAI Global with an accreditation body.
"Certified" or "Certification"	means a confirmation that in the opinion of SAI Global a Management System/ product/process/service complies with requirements of a Standard to which an Accredited Certificate has been issued by SAI Global.
"Certification Mark" or "Logo"	means a symbol, word(s) or other sign that signifies that a Management System/ product/process/service has been found to be in conformance with a Standard within the scope of accreditation of SAI Global.
"**Certification Scheme Procedures"**	means the procedures developed by SAI Global to complete an assessment to a Standard.
"Control"	means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" will be construed accordingly.
"Controller"	means an entity that, alone or jointly with others, determines the purposes and means of the processing of Personal Data as defined in EU Data Protection Law.
"Customer"	means the customer of SAI Global signing the Proposal Document.
"Customer Data"	means any Personal Data that SAI Global Processes on behalf of Customer in the course of providing Services.
"Customer Material"	means all Customer owned or licensed data, content, or other material provided by Customer to SAI Global pursuant to this Agreement, to be included in or used with a Product or Service (including without limitation customer data, logos, policies, procedures, organisation charts, and other proprietary text or graphics), and any other proprietary information collected by SAI Global from Customer or its Users in connection with the provision of a Product or Service pursuant to this Agreement.
"Proposal Document"	shall the document executed by the parties describing the Services to be provided by SAI Global to Customer pursuant to the Agreement. Each Proposal Document shall be subject to the terms of this Agreement and may contain additional terms. In case of conflict between this Agreement and a Proposal Document, the Proposal Document will prevail.
"Data Protection Laws"	means all effective data protection and privacy laws applicable to the Processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.
"Documentation"	means this Agreement; the Proposal Document; and any applicable statements of work, addenda, schedules or documents referenced therein.
"EU Data Protection Law"	means (i) prior to May 25, 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("Directive"); (ii) on and after May 25, 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation, or "GDPR").
"EEA"	means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.
"Management System"	means a set of interrelated or interacting elements of an organisation to establish policies and objectives and processes to achieve those objectives.
"Process"	means a set of interrelated or interacting activities that use inputs to deliver an intended result.
"Personal Data"	means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person as defined in EU Data Protection Law.
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
"Personally Identifiable Information"	means that information identifying a person or persons that is protected by data protection law or regulation within any jurisdiction pursuant to which the Products or Services are being provided under this Agreement.
"Processing"	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or

	destruction. "Process", "Processes" and "Processed" will be construed accordingly as defined in EU Data Protection Law.
"Processor"	means an entity that processes Personal Data on behalf of a Controller as defined in EU Data Protection Law
"Product(s)"	means any product(s) to be provided by SAI Global listed and described in the Documentation and all the components of the Product(s), including without limitation, computer software, data, audio, video, text, graphics, animation, etc.; and any materials that are ancillary to the Product (user manuals, instructor guides, etc.), but excluding Customer Materials.
"SAI Global"	means the SAI Global Company contracting party identified in the Proposal Document including its Affiliate.
"Significant Change"	means any material change that affects the activities and operation of a Management System/ product/process/service such as a change in ownership, management, organisation, policy, technology, personnel, product and services, facilities, equipment, procedures, change of address of any relevant sites or other premises, subcontracting or outsourcing of processes.
"Site"	means the location of the Customer's Management System/ product/process/service.
"Standard(s)"	means a document published by a third party setting forth a particular set of criteria applicable to a Management System/ product/process/service for which the Services have been requested by the Customer.
"Standards Body"	means a party that issues Standards.
"Internet Site(s)"	means the SAI Global controlled internet site(s) to which Customer may be provided access as specified in the Documentation.
"Model Clauses"	means the Standard Contractual Clauses for Processors as approved by the European Commission.
"Service(s)"	means any service(s) to be provided by SAI Global as listed and described in the Documentation.
"Sub-processor"	means a third party engaged by SAI Global to assist in fulfilling its obligations with respect to processing pursuant to the Agreement.

2. Services

2.1. SAI Global agrees to provide the Services identified in the Proposal Document as otherwise agreed by the Customer and SAI Global, subject to the provisions of these terms and conditions

2.2. This Agreement shall commence on the commencement date stipulated in the Proposal Document and shall continue for a minimum period of twelve (12) months.

2.3. Thereafter this Agreement shall continue unless and until terminated by either party giving to the other party not less than ninety (90) days' written notice.

2.4. The Customer agrees to provide SAI Global's employees, agents, contractors and partners with all information, co-operation and assistance required to perform the Services including reasonable access to the premises, facilities, documents and records of the Customer and the Customer's contractors and agents. Such access shall, upon request by SAI Global, include representatives of accreditation bodies, other organisations that provide oversight of the accredited Standard or regulators to witness SAI Global performing Services at Customer's site or to investigate, validate or resolve an external complaint. These audits can be on short-notice or unannounced. SAI Global may also need access to the Customer's suppliers if required by the Standard. SAI Global representatives shall not be obligated to sign any agreement as a condition of site entry and if signed the Customer agrees that such agreement shall be void and of no force and effect.

2.5. The Customer agrees to comply with the applicable SAI Global Certification or Certification Scheme Procedures provided to Customer.

2.6. Except as required by the applicable Standard, SAI Global will perform on the Customer's Site the Services during the Customer's normal business hours and in a manner so as not to interfere with the performance of any work by the Customer.

2.7. The Customer accepts responsibility for the safety of Auditors at Customer's Site and Customer shall provide to the Auditors all necessary safety or protective clothing and/or equipment and advise SAI Global, its employees, agents and contractors appropriately of any safety hazard or special training requirements. If specialised training is necessary for SAI Global staff to enter the site, all costs associated with such training are not included in the Proposal Document unless specifically noted and will be billed to the Customer separately.

3. Fees

3.1 The Customer agrees to pay the fees set out in the Proposal Document regardless of whether Customer's Management System/ product/process/service meets the requirements of the Standard and achieves Certification by SAI Global. SAI Global shall be under no obligation to refund fees paid by the Customer in the event of suspension or termination of Certification by SAI Global or the Customer. SAI Global reserves the right to increase the Fees as outlined in the Proposal Document or Statement of Work annually in the month of July by an amount not less than 2.5% or as otherwise detailed in the Proposal Document or Statement of Work.

3.2 SAI Global may charge a postponement or cancellation fee to the Customer which Customer agrees to pay for all confirmed audits that are postponed or cancelled by the Customer. Should the Customer provide between fifteen (15) – thirty (30) days' advance written notice of the postponement or cancellation of a confirmed audit, the Customer will be charged 50% of the applicable fees outlined in the Proposal Document. Should the Customer provide less than fifteen (15) days' advance written notice of the postponement or cancellation of a confirmed audit, the Customer will be charged 100% of the applicable fees outlined in the Proposal Document.

3.3 In addition to the postponement or cancellation fee, the Customer agrees to reimburse SAI Global for all non-refundable charges and expenses incurred by SAI Global prior to postponement or cancellation. Travel related expenses will be charged at cost plus a 10% administration fee or as described in the Proposal Document. The Customer may choose to handle all travel arrangements and travel related costs at their expense.

4. Certification

4.1. The Customer acknowledges that SAI Global will only issue an Accredited Certificate where the Customer's Management System/ product/process/service has successfully fulfilled the Certification Scheme Procedures and met the applicable Standard requirements, in the opinion of SAI Global. SAI Global and its Auditors assume no liability with respect to the Management System/ product/process/service, its operation, safety, Certification or otherwise. Customer will defend, indemnify and hold SAI Global, its Auditors and the applicable Standards Body harmless from and against all costs, damages, expenses and liability associated with any legal action or regulatory proceedings brought against or otherwise involving SAI Global, its Auditors or a Standards Body, or subpoenas brought by a third party compelling SAI Global, its Auditor or a Standards Body to testify.

4.2. In granting the Certification, SAI Global approves the use of the relevant Certification Mark solely in connection with a Management System/ product/process/service that is Certified.

4.3. The policies and procedure under which SAI Global operates and the administration of them shall be non-discriminatory. Procedures shall not be used to impede or inhibit access by applicants, other than as provided for in ISO/IEC 17065

4.4. SAI Global shall make its services accessible to all customers whose activities fall within the scope of its operations. For the avoidance of doubt; (i) access to the certification process shall not be conditional upon the size of the customer; or its membership of any association or group, or the number of Certifications already issued; and (ii) there shall be no influence of undue financial or other conditions, in granting the Certification by SAI Global. SAI Global shall confine its requirements, evaluation, review, decision and surveillance (if any) to matters specifically related to the scope of Certification.

4.5. Customer acknowledges and agrees that SAI GLOBAL can decline to accept an application or maintain a contract for Certification from a Customer on account of fundamental or demonstrated reasons such as the customer participating in illegal activities, or customers having a history of repeated non-compliances with certification/product requirements, or similar customer-related issues.

5. After Certification

5.1. After and during the period of Certification, the Customer acknowledges full responsibility to operate and maintain the Management System/ product/process/service at the Site (or Sites) in conformance with the requirements of the Certification Scheme Procedures under which Certification was granted. The Certification shall continue throughout the period identified by the Accredited Certificate expiry date or as terminated in accordance with the requirements of this Agreement.

5.2. The Customer must promptly inform SAI Global in writing of any Significant Change. These changes can include: legal, commercial, organisational status or ownership, organisation and management (e.g. key managerial, decision-making or technical changes, modification to the product or production method, contact address and production sites, major changes to the Management System)

5.3. The Customer must promptly implement appropriate changes communicated in writing by SAI Global, such as changes to the Standard or changes introduced in the certification scheme by a Standards Body; changes in SAI Global's certification process, changes in terms and conditions or fees. The Customer agrees that if the certification applies to ongoing production, the certified product continues to fulfil the certification requirements

5.4. After Certification, any request to modify the scope of Certification as it appears on the Accredited Certificate may require SAI Global to conduct an on-site accredited conformity assessment to validate the request. Such accredited conformity assessments may occur in conjunction with scheduled activities or as a separate activity with fees to be determined at the time of the request. Any request for change shall not result in a change to the expiry date of the Accredited Certificate.

5.5. After Certification, SAI Global may require the performance of a short notice accredited conformity assessment to evaluate the impact of Significant Changes of which it becomes aware or as a result or the receipt of an external complaint by a third party or as required by the Standards Body. Fees for such Services will be determined at the time of notification.

5.6. During and after Certification, the Customer shall:

5.6.1. maintain a written record of all complaints relating to compliance with Certification requirements and make these records available to SAI Global upon request;

5.6.2. Take appropriate action with respect to such complaints and any thereafter any deficiencies found in products/Management systems/processes that affect compliance with the requirements for Certification; and

5.6.3. document the actions taken pursuant to Section 5.6.2 which will be available upon request to SAI Global.

6. Advertisement of Certification

6.1. Subject to these terms and conditions, the Customer may publicize that Certification has been granted and use the certification documents as evidence of Certification including displaying the certificate at the Site listed on the certificate. In addition, the Customer may publicize the Certification in various communication documents such as brochures or advertising documents provided Customer complies with the requirements of the applicable Standards Body or as specified in the Certification Scheme. The Customer may copy the Accredited Certificate (and any other certification documents received from SAI Global), provided that each copy is clearly identified as a copy and reproduced in its entirety or as specified by the applicable Standard. Customer may not alter, modify, deface or destroy the certificate. The original and any permitted copies of any certification documents remain the property of SAI Global and must be returned immediately upon request by SAI Global.

6.2. Customer may refer to SAI Global's Certification of Customer in accordance with SAI Global's advertising guidelines which may be amended or supplemented by SAI Global from time to time.

6.3. SAI Global shall have the right to maintain in its public listings such information about the Customer and the consistent with SAI Global Certification Scheme Procedures.

6.4. The Customer may not engage in any conduct which might mislead, deceive or confuse any person in relation to or otherwise misrepresent the nature, status, scope or effect of its Certification by SAI Global. The Customer must promptly comply with any directions given by SAI Global to correct any misconduct or misrepresentation.

7. Suspension, Cancellation or Expiration of Certification

7.1. SAI Global, in its sole discretion, may suspend or cancel a Certification if SAI Global gives notice to the Customer that it considers a Certification is no longer appropriate, the Customer is in breach of this Agreement or a Significant Change occurs without the Customer notifying SAI Global for its review.

7.2. SAI Global will notify the Customer of the suspension or cancellation, provide the Customer with information outlining the steps that must be taken by the Customer to enable the suspension to be removed or cancellation avoided.

7.3. Customer failure to resolve the issues that have resulted in the suspension in a time established by SAI Global shall result in withdrawal or reduction of the scope of Certification. Any such reduction shall be in accordance with the requirements of the applicable Standard. Upon satisfactory resolution of the conditions that caused the suspension, SAI Global will notify the Customer when the suspension has been removed. In the event the conditions for suspension cannot be resolved, SAI Global may take further action up to and including withdrawal of Certification.

8. Termination of this Agreement

8.1 The Customer undertakes and agrees that upon any suspension, withdrawal, or termination of Certification, it shall immediately discontinue the use of all the advertising materials that contains any reference to the Certification and shall take all necessary actions as may be required by the Certification scheme (e.g. the return of certification documents).

8.2 Either party may terminate this Agreement for convenience (subject to the payment of all outstanding fees), at any time upon providing ninety (90) days' written notice to the other party.

8.3 Either party may terminate this Agreement upon written notice if the other party breaches any material provisions of this Agreement which remains uncured for fifteen (15) days or if a party becomes insolvent or bankrupt.

8.4 Upon termination of this Agreement for any reason or the cancellation of a Accredited Certificate, the Customer must stop all claims and statements that their Management System/ product/process/service is Certified by SAI Global and do the following:

8.4.1 cease using any Certification Mark or Logo in connection with the Certification (if any);

8.4.2 withdraw from public display and, as required by SAI Global, return the original and all copies of the Accredited Certificate;

8.4.3 cease all advertising, promotion and other publication of the fact of Certification;

8.4.4 take steps to remove signage, posting and other indications on the Customer's premises, property, plant and uniforms which infer, directly or indirectly, a that an Certified Management System/ product/process; and

8.4.5 take all other necessary steps to ensure third parties are not misled to believe that the Certification has not expired or been cancelled.

9 Appeals

SAI Global has documented systems for the handling of appeals, complaints and disputes which are available upon request.

10 Sector Specific Terms and Condition

Any supplemental sector specific terms and conditions will be provided to the Customer as sector specific scheme requirements. If a Customer is unsure whether these terms are applicable they must advise SAI Global prior to accepting Certification.

11 Confidential Information

11.1 "Confidential Information" means any non-public information including (i) technical information including but not limited to inventions, know-how, trade secrets, methods, techniques, processes, designs, drawings, diagrams, software, computer code, the structure, sequence and organization of software, formulae and analysis, and (ii) business information including but not limited to price lists, Customer lists, cost analyses, reports, surveys and market information and data whether communicated in tangible or intangible form.

11.2 Confidential Information shall be kept in confidence by the receiving party using the same degree of care as such party uses to prevent unauthorized disclosure of its own Confidential Information but in no event less than a reasonable degree of care and the receiving party shall not disclose such Confidential Information to third parties nor use it except to carry out the purposes of this Agreement. This obligation of confidentiality shall not apply to information which (a) is or becomes in the public domain through no breach by the receiving party; (b) is previously known or independently developed by the receiving party; (c) is learned by the receiving party from a third party entitled to disclose it ; or (d) is required to be disclosed by operation of law or as required by a Standards Body under whose auspices SAI Global performs certification services provided that the receiving party shall use reasonable efforts to notify the disclosing party prior to disclosure.

11.3 When required by a Standard as part of the Certification Scheme Procedures the Customer shall authorise SAI Global to share a copy of the final audit report and supporting documentation as required by the Standard.

12 License of Marks

12.1 Subject to the terms of this Agreement SAI Global grants to Customer a non-exclusive, non-transferable, revocable license during the term to use the certification trademark indicating passage of SAI Global's applicable certification program (the "SAI Global Mark") to be provided to Customer subsequent to the successful completion of an audit for the sole purpose of marketing and promoting Customer's successful completion of the audit. Such use of the SAI Global Mark shall be in a manner consistent with this Agreement.

12.2 At least fifteen (15) days in advance of the first use of the SAI Global Mark in connection with a particular marketing or promotional campaign or strategy, Customer will provide SAI Global with a sample of such use requesting SAI Global's prior written approval of such use. SAI Global will use commercially reasonable efforts to notify Customer of its approval or disapproval of such use within ten (10) days of receipt of the request for approval. Customer will promptly cease and desist from any such use not approved in writing by SAI Global. Customer will use the SAI Global Mark in conformance with any trademark usage policies provided by SAI Global from time to time including affixing the symbol "™" or "®" to all SAI Global Marks as directed by SAI Global. Customer will not take any action inconsistent with SAI Global's ownership of the SAI Global Marks and any benefits accruing from Customer's use of the SAI Global Marks will automatically vest in SAI Global except as otherwise provided in this Agreement.

12.3 Customer will not form any combination marks with the SAI Global Mark without the prior written approval of SAI Global. If SAI Global determines, in good faith, that Customer's use of the SAI Global Mark tarnishes, blurs or dilutes the quality associated with the SAI Global Marks or associated goodwill, SAI Global shall notify Customer in writing of the same specifying the offending use and offering an alternative use that will allow Customer to continue to use the SAI Global Mark without tarnishing, blurring or diluting the quality associated with the SAI Global Mark or associated goodwill. If Customer does not cease the offending use promptly, but in any event within five (5) days after receipt of such notice from SAI Global, SAI Global may revoke Customer's license to use the SAI Global Marks. Except for the limited rights expressly granted herein by SAI Global to Customer, nothing in this Agreement shall serve to transfer to Customer any intellectual property rights in or to the SAI Global Services, other SAI Global Marks or other intellectual property owned, licensed or claimed by SAI Global. Customer acknowledges and agrees that to the best of its knowledge SAI Global has sole right, title and interest in and to the SAI Global Marks, all goodwill and SAI Global intellectual property. Customer will promptly inform SAI Global of any known or reasonably suspected infringement or misappropriation of SAI Global's trademarks, copyrights or other intellectual property rights.

12.4 The Customer undertakes and agrees that all use of a Certification trademark shall comply with all the requirements that may be prescribed in the Certification scheme relating to the use of marks of conformity, and for information related to the product.

13 Warranties

13.1 SAI Global warrants that it has been granted the right and authority to provide the Services by the applicable Standards Body.

13.2 SAI Global warrants that the Services will be provided in a good and workmanlike manner.

13.3 SAI Global's warranties are the express warranties set forth in this Section.

13.4 SAI Global specifically disclaims to the fullest extent permitted by law any and all other warranties, express, implied or statutory, including without limitation any implied warranties of merchantability and fitness for a particular purpose.

14 Indemnity

14.1 The Customer shall be liable for and shall indemnify SAI Global against all or any of the following:

14.1.1 any loss caused by the Customer's failure to perform its obligations in relation to this Agreement;

14.1.2 any claims of third parties arising out of or relating to the use of the Certification by the Customer in breach of these terms and conditions; and

14.1.3 all liabilities relating to any loss or damage of whatsoever nature suffered by whosoever as a result of the use of the Certification in breach of these terms and conditions.

15 Limitation of Liability

15.1 Nothing in this Agreement shall exclude or limit SAI Global's liability for personal injury and death arising out of SAI Global's negligence and the Customer undertakes that it will not without SAI Global's prior written consent settle or compromise any such claim by a third party or for fraud.

15.2 SAI Global shall not be liable to the Customer for or in respect of any consequential loss to the Customer for or arising out of any breach of this Agreement or any negligence in connection with the supply of the Services hereunder. "Consequential loss" shall include (but not

be limited to) loss of profit, revenue, use, goodwill or other loss, any payment made or due to any third party, economic loss, and any loss or damage caused by the delay of the supply of the Services under this Agreement.

15.3 The liability of whatsoever nature of SAI Global to the Customer arising out of or in connection with this Agreement shall be conclusively waived by the Customer if written particulars of any claim made by the Customer giving rise to the liability setting out full details of the specific matters in respect of which such claim is made is not received by SAI Global within six (6) months after the date of the Customer becoming aware of the possibility of such a claim, and in no event shall the liability of SAI Global to the Customer exceed in total the annual price paid by the Customer under this Agreement.

15.4 SAI Global's cumulative liability to the Customer arising out of or relating to this Agreement shall not exceed in aggregate the annual fees paid by the Customer to SAI Global whether in contract, warranty, negligence, tort, strict liability or otherwise.

16 Anti-Bribery and Corruption

16.1 Both parties shall:

16.1.1 comply with all applicable laws, statutes and regulations relating to anti-bribery and anti-corruption including but not limited to the Bribery Act 2010;

16.1.2 have and shall maintain in place throughout the term of this Agreement its own policies and procedures, including but not limited to adequate procedures under the applicable bribery laws and Bribery Act 2010, to ensure necessary compliances and shall enforce them where appropriate;

16.1.3 promptly report to the other party any request or demand for any undue financial or other advantage of any kind received in connection with the performance of this Agreement;

16.1.4 immediately notify the other party (in writing) if a foreign public official becomes an officer or employee of that party or acquires a direct or indirect interest and the party warrants that it has no foreign public officials as direct or indirect owners, officers or employees at the date of this Agreement; and

16.1.5 within three (3) months of the date of this Agreement, and annually thereafter, certify to the other party in writing signed by an officer of the party, compliance with this Section 16 by the party and all persons associated with it. Each party shall provide such supporting evidence of compliance as the other party may reasonably request.

16.2 The parties shall ensure that any person associated with it who is performing services in connection with this Agreement, does so only on the basis of a written contract which imposes on and secures from such person terms equivalent to those imposed on the party in this Section 16. Each party shall be responsible for the observance and performance by such persons of the terms equivalent, and shall be directly liable to the other party for any breach by such persons of any of the terms equivalent.

16.3 Breach of this Section16 shall be deemed a material breach under Section8.2.

16.4 For the purpose of this Section16, the meaning of adequate procedures and foreign public official and whether a person is associated with another person shall be determined in accordance with section 7(2) of the Bribery Act 2010 (and any guidance issued under section 9 of that Act), sections 6(5) and 6(6) of that Act and section 8 of that Act respectively. For the purposes of this Section 16, a person associated with either party includes, but is not limited to, any subcontractor of the party.

17 General

17.1 Neither SAI Global nor any of its employees, contractors and agents shall be deemed to be employees of the Customer and SAI Global shall be solely responsible for payment of compensation to all of SAI Global's employees, contractors and agents and as to them, shall maintain in force, at its sole cost and expense, any worker's compensation insurance coverage required by law.

17.2 No party is liable for any failure to perform or delay in performing its obligations under this Agreement if that failure or delay is due to flood, fire, earthquake or other occurrence beyond that party's reasonable control (a force majeure event). If that failure or delay exceeds sixty (60) days the other party may terminate this Agreement upon thirty (30) days' written notice to the other party.

17.3 Except as expressly stated herein, there is no intention by either party to exchange or license intellectual property pursuant to this Agreement. Any such exchange or license will require an executed amendment to this Agreement.

17.4 If any part of this Agreement is held to be unenforceable in any jurisdiction the validity of the remaining parts shall be unaffected and the unenforceable part shall be rewritten to reflect as closely as possible the intent of the parties.

17.5 A waiver of any breach of this Agreement shall not constitute a waiver as to future breaches.

17.6 This Agreement constitutes the entire agreement of the parties with respect to the subject matter hereof and may not be modified except in writing signed by both parties. Customer may use its form of purchase order for convenience but may not vary the terms of this Agreement thereby.

17.7 This Agreement supersedes and extinguishes all previous drafts, agreements and understandings between the parties, whether oral or in writing, relating to its subject matter.

17.8 Each party irrevocably agrees that this agreement will be governed by the laws of Ireland and the courts of Ireland shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

17.9 These terms and conditions shall have precedence in all circumstances over any other terms and conditions of the Customer unless expressly agreed in writing between the Customer and SAI Global. SAI Global will not be deemed to have accepted any terms and conditions of the Customer unless expressly agreed in writing by SAI Global to the Customer.

17.10 Nothing in this Agreement shall be deemed to create an agency, joint venture or partnership relationship between the parties.

17.11 All notices which either party hereto may or is required to give or to serve upon the other party shall be sent by first class recorded delivery pre-paid at the address specified in this Agreement and shall be deemed to have been delivered two (2) business days after the date of sending. This Agreement shall not be assigned by the Customer.

17.12 Words contained in this Agreement importing the plural meaning shall where the context so admit include the singular meaning and vice versa, and headings used in this Agreement are for reference only and do not form part of this Agreement.

17.13 This Agreement may be executed in counterparts, all of which shall be deemed to constitute one agreement. When the authorised representative of either party signs this Agreement, a copy, duplicate, or electronic file or facsimile of such signed Agreement shall have the same force and effect as one bearing an original signature.

17.14 All provisions of this Agreement that expressly or by implication are intended to survive the termination or expiration of this Agreement shall remain in force according to their terms.

17.15 SAI Global and the Customer acknowledge that they have required that this Agreement and all documentation, notices and judicial proceedings entered into, given or instituted pursuant hereto or relating directly or indirectly hereto be drawn up in English.

18 Data Protection

18.1 The provisions related to the processing and protection of Personal Information and Data are set out in Schedule A - Protection of Personal Information and Data – and form part of this Agreement.

18.2 The provisions related to information security are set out in Schedule B – Information Security Terms and Conditions – and form part of this Agreement.

18.3 SAI Global shall, at all times during and after the Term, indemnify the Customer and keep the Customer indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against or agreed to be paid by the Customer arising from any breach of SAI Global's obligations under this Section 18 except and to the extent that such liabilities have resulted directly from the Customer's instructions.

Schedule A
Data Protection

1. Scope

This Schedule applies where and only to the extent that SAI Global Processes Customer Data that originates from the EEA or that is otherwise subject to EU Data Protection Law on behalf of Customer in the course of providing Services to the Customer.

2. Roles and Scope of Processing

2.1 Role of the Parties. As between SAI Global and Customer, Customer is the Controller of Customer Data, and SAI Global shall Process Customer Data only as a Processor acting on behalf of Customer.

2.2 Customer Processing of Customer Data. Customer agrees that (i) it will comply with its obligations as a Controller under Data Protection Laws in respect of its Processing of Customer Data and any Processing instructions it issues to SAI Global; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Data Protection Laws for SAI Global to Process Customer Data pursuant to the Agreement.

2.3 SAI Global Processing of Customer Data. SAI Global will Process Customer Data only for the purposes described in this Agreement and only in accordance with Customer's documented lawful instructions.

2.4 Details of Processing - As defined in the Proposal Document.

3. Sub-processing

3.1 Authorized Sub-processors. Customer agrees that SAI Global may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by SAI Global and authorized by Customer are listed below:

Name of Subprocessor	Country in which Subprocessor is located
Agreal – (Audit Partner)	France
Agroin – (Audit Partner)	Spain
SertificSystem	Belarus
Tecnoqualita - – (Audit Partner)	Italy
Verizio – (Audit Partner)	United Kingdom
Workplace Fire & Safety Training– (Audit Partner)	United Kingdom
Valiguard– (Audit Partner)	Sweden
Intact – (Auditing Systems Partner)	Austria
Salesforce CRM and Auditing Systems Partner	USA, Singapore
UMB – (Audit Partner)	UAE & Lebanon
Szutest	Egypt

3.2 Sub-processor Obligations. SAI Global will: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this Agreement and for any acts or omissions of the Sub-processor that cause SAI Global to breach any of its obligations under this Agreement.

3.3 Changes to Sub-processors. SAI Global shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email will suffice) if it adds or removes Sub-processors at least ten (10) calendar days' prior to any such changes. Customer may object in writing to SAI Global's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection.

4. Security

4.1 Security Measures. SAI Global shall maintain an information security program that complies with applicable privacy laws and is consistent with standard practices and security standards in SAI Global's industry, such as those published by the International Standards Association (ISO 27001:2013) and the National Institute of Standards and Technology (NIST). Such program shall include appropriate administrative, technical, physical, organizational, and operational safeguards and other security measures to maintain the security and confidentiality of Personal Data and to protect it from known or reasonably anticipated threats or hazards to its security and integrity. SAI Global will review its information security program at least annually, or after significant changes occur, to ensure its continuing compliance, suitability, adequacy and effectiveness.

4.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by SAI Global relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that SAI Global may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

4.3 Personnel. SAI Global will ensure that any person who is authorized by SAI Global to Process Customer Data (including its staff, agents and authorized Sub-processors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). Further, SAI Global shall take steps to ensure that any person who is authorized by SAI Global to have access to Customer Data does not Process such data except on instructions from Customer, unless such person is required to Process such data by applicable EU Data Protection Law.

4.4 Personal Data Breach Response. Upon becoming aware of a Personal Data Breach, SAI Global shall notify Customer without undue delay and will provide timely information relating to the Personal Data Breach as it becomes known or as is reasonably requested by Customer. SAI Global shall promptly take reasonable steps to mitigate and, where possible, to remedy the effects of any Personal Data Breach.

5. Audits and Certifications

5.1 Customer acknowledges that SAI Global is regularly audited against International standards, by independent third party auditors subject to control objectives based on guidance from the Information Technology Governance Institute, and has obtained ISO 27001:2013 certification for its Global Hosting services. Upon reasonable written request, SAI Global shall supply a summary copy of its audit and certification report(s) ("Report") to Customer, which Reports shall be subject to the confidentiality provisions of any non-disclosure agreement provided by SAI Global for Customer's execution in connection with the Reports. SAI Global shall also respond to any written audit questions submitted to it by Customer provided that Customer shall not exercise this right more often than once per twelve (12) months unless following a Breach.

6. International Transfers

6.1 Data Centre Locations. SAI Global may transfer and Process Customer Data anywhere in the world, where the SAI Global, its Affiliates or its Sub-processors maintain Processing operations. The primary processing location and additional locations where personal data may be processed or viewed is detailed in the Proposal Document. SAI Global will at all times provide an adequate level of protection for the Customer Data Processed, in accordance with the requirements of Data Protection Laws.

6.2 Model Clauses. To the extent that SAI Global Processes any Customer Data that is protected by EU Data Protection Law or that originates from the EEA in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that SAI Global shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by complying with the Model Clauses in Schedule C to this agreement which is incorporated herein by this reference. SAI Global agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses (notwithstanding that Customer may be an entity located outside of the EEA).

7. Return or Deletion of Data

7.1 Upon termination or expiration of the Agreement, SAI Global shall (at Customer's election) return or to the fullest extent technically feasible delete all Customer Data in its possession or control. This requirement shall not apply to the extent SAI Global is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data SAI Global shall securely isolate and protect from any further Processing, except to the extent required by applicable law.

8. Data Subject requests

8.1 To the extent permitted by law, SAI Global will inform the customer without undue delay of requests from Data Subjects exercising their Data Subject rights (e.g. rectification, deletion and blocking of data) addressed directly to SAI Global regarding Customer Personal Data. The SAI Global at no time will communicate directly with the Data Subject.

8.2 If the customer is obliged to provide information regarding the customers Personal Data to Other Controllers or third parties (e.g. Data Subjects or the Supervisory Authority),the SAI Global has, in some services, provided the Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, the SAI Global shall assist the customer in doing so by providing all required information. If the customer or other Controllers are obliged to provide information about the processing of the customers Personal Data to a Data Subject, SAI Global shall assist the customer in making the required information available.

9. Cooperation

9.1 If a law enforcement agency or government body sends SAI Global a demand for Customer Data, SAI Global will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, SAI Global may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency or government body, then SAI Global will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless SAI Global is legally prohibited from doing so.

9.2 To the extent SAI Global is required under EU Data Protection Law, SAI Global shall provide requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

Schedule B

Information Security Terms and Conditions

Capitalized terms used but not defined herein shall have the meanings given to them in the Agreement.

1. Definitions. As used in this Schedule, the following capitalized terms shall have the meanings provided in this section or as defined in the Agreement.

a. "Audit Log" is a time-based record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event, including without limitation who accessed a system and what operations he or she has performed during a given period of time.

b. "Customer Material" is deemed to have the same definition as set forth in the Agreement and pursuant to the Agreement is deemed to be Confidential Information.

c. "Confidential Information" is deemed to have the same definition as set forth in the Agreement.

d. Information Security Incident. "Information Security Incident" is defined as any situation while providing Services as defined in the underlying Agreement where Customer Confidential Information is deemed lost (e.g. Licensor is not aware where the Customer Confidential Information is or the Customer Confidential Information is not where it is expected to be in relation to the provision of the Services as defined in the underlying Agreement) or is subject to unauthorized or inappropriate access by third parties, in a manner that results in Customer Confidential Information being inappropriately being released to a third party while under the control of Licensor. In addition, Information Security Incident includes the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system. Examples of Information Security Incidents include, but are not limited to, unauthorized account use; computer or network systems intrusion; unauthorized changes to system hardware, firmware, or software; password stealing or cracking; unwanted disruption or denial of service; and theft or loss of equipment or device containing Customer Confidential Information.

e. "Open Network" is any open, unsecured or untrusted network such as the Internet.

f. "Security Tests". "Security Tests" means test procedures performed by Licensor with the intent of preventing Information Security Incidents, including without limitation test of IT general controls, tests of IT application controls, penetration tests, compliance scans and vulnerability scans.

g. 'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

h. "Sensitive Data" includes any of the following information: social security numbers, any government-issued identification number (e.g. driver's license, passport), individually identifiable patient data or EPHI, Cardholder Data, account number, credit or debit card number, in combination with any required security code, access code, or password (e.g., a PIN) that would permit access to an individual's financial account, human resources employee files, or any information that is deemed protected or confidential by contractual obligations or any federal, state or local law or regulation.

i. Systems. "Systems" means any systems, whether located at the Licensor or its subcontractors, which are used in the provision of Services pursuant to the underlying Agreement between the parties to store, access, process or transmit any Customer Confidential Information whether held electronically, on paper, or in any other form.

2. Access to Customer Confidential Information. Licensor shall restrict access to Customer Confidential Information or Personal Data to only its employees, contractors, consultants ("Workers") who require access to this information to support Licensor's performance of the contracted Services for the Customer or as otherwise described in the underlying Agreement. In no event will Customer Confidential Information be provided to Licensor by email, text or other insecure internet based communication. Licensor shall require all Workers or the applicable legal entities on whose behalf they perform, to sign a confidentiality agreement that is in substance at least as restrictive as the confidentiality provisions between Licensor and Customer. Prior to receiving access to Customer Confidential Information or Personal Data, Workers will receive security awareness training appropriate to their job function. The access rights of Workers will be removed immediately upon termination or adjusted upon change in job function. Licensor management must review Worker access to Customer Confidential Information or Personal Data at least annually. Licensor will closely monitor all access to Customer Confidential Information or Personal Data.

3. Transfer of Customer Confidential Information. Pursuant to the Agreement, Licensor shall impose or has imposed comparable security requirements contained in this Schedule on its third parties who are permitted access to Customer Confidential Information and will remain fully responsible for its third parties' compliance. Licensor will not permit Customer Information to be transferred to any third party that does not comply, unless the transfer is:

a) Required by subpoena or order of a court or tribunal of competent jurisdiction, or by a government agency or official requesting to obtain the information in the course of an investigation;
b) Necessary in connection with litigation or other forms of dispute resolution between Licensor and either the Customer or the individual to whom the information relates; or
c) Necessary Authorized by the Customer (Customer shall promptly and reasonably respond to all requests for transfer) or the subject individual in writing.

Transfer of Personal Data (where the Data Subject is a resident of the European Union and as such falls under the jurisdiction of Regulation (EU) 2016/679 General Data Protection Regulation) which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, the conditions laid down in the regulation are complied with by the controller and processor (as summarized in Schedule A), including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization. All provisions in the regulation shall be applied in order to ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined.

4. **Information Security.** Licensor shall maintain an information security program that complies with applicable privacy laws and is consistent with standard practices and security standards in Licensor's industry, such as those published by the International Standards Association (ISO 27001), National Institute of Standards and Technology (NIST). In addition, such program shall include appropriate administrative, technical, physical, organizational, and operational safeguards and other security measures to maintain the security and confidentiality of Customer Confidential Information and to protect it from known or reasonably anticipated threats or hazards to its security and integrity. Licensor agrees to maintain current patching levels within reasonable timeframes as standard in Licensor's industry and so long as each individual patch is issue free of errors and does not put Licensor's security at risk. The level of security and protection provided shall be commensurate with the nature of the Customer Confidential Information to be protected so long as the nature of such Customer Confidential Information is previously disclosed to Licensor. Licensor will review its information security program at least annually, or after significant changes occur, to ensure its continuing compliance, suitability, adequacy and effectiveness. The Licensor information security program shall to the extent necessary, include but not be limited to the following broad topics in a manner which is reasonable and appropriate and which aligns with Licensor's industry standards, and the required standards required to maintain any and all certifications set forth in this agreement:

a) Roles and Responsibilities: Established roles and responsibilities for information security and compliance, which extends to top management, and includes an assigned privacy and security officer, and/or a designated team assigned with privacy, security and compliance oversight;

b) Risk Management: A risk management program which includes an analysis of the criticality of data, an annual assessment of risks to the privacy and security of data which is commensurate with the criticality of the data, and a remediation plan to address any identified vulnerabilities and risks;

c) Security Policy: An information security policy program which creates and maintains a comprehensive library of documented policies and procedures (Information Security Management System) which support all aspects of the information security program and which is reviewed and approved by top management annually or when significant changes to the regulatory or technical environment occur, to ensure that the policies and procedures are appropriate, accurate, and current, and in alignment with industry standards;

d) Workforce Security: Comprehensive screening of new workforce members before being granted access to Sensitive or Personal Data, including background checks, as well as appropriate supervision during employment, procedures for employee sanctions and procedures for terminations and role change;

e) Security Awareness Training: Training workforce about information security best practices, internal information security policies and their obligations to protect sensitive or Personal upon hiring and at a minimum frequency of annually thereafter. Training about federal rules (e.g. HIPAA Privacy and GDPR) is provided to staff asspecific to their roles.

f) Physical and Environmental Security: Policies and Standards specific to protecting physical areas which house data and systems (Data Centers, Communications rooms, general offices) as well as guarding against environmental damage and theft;

g) Change / Test Procedures: Documented policies about system and application change control process, including appropriate segregation of test and operational data, system-supported segregation of duties, system planning, acceptance, and release;

h) Third Party Management: Accurate and current accounting of all subcontractors and third parties, along with enforceable agreements which outline security controls, audit rights and compliance with applicable laws;

i) Protection Against Malware: Implementation of technical and procedural controls to guard against malicious software ensuring the that the use of current software which is configured and maintained to according to suppliers recommendations;

j) Back-up and Testing Procedures: Maintaining documented procedures for backing-up and restoring data and testing those procedures regularly;

k) Network Security Management: Implementation of technical and procedural controls to protect the confidentiality and integrity of data passing over networks (internal and external), using industry standard perimeter controls well defined and appropriate security zones, and the segmentation of internal networks;

l) Media Handling: Procedures for media management including controls for portable media, media sanitization and disposal, and media accountability and tracking;

m) Exchange of Information: Procedures for secure exchange of information being transmitted or physically shipped to external parties, including encryption of confidential or sensitive information, protection of information in transit, and policies governing appropriate disclosure of information to third parties;

n) System Event Logging and Monitoring: Configuring systems to log critical system events and user activity to a central system, procedures for protecting, retaining and accessing all logs. Automated and manual processes for appropriately monitoring logs;

o) Access Controls: Documented policies for authorizing and provisioning user and system access to electronic resources which are based on the principle of least privilege, enforced industry standard authentication methods, and procedures for routine reviews of user and system accounts;

p) Mobile Computing Controls: Policies governing the use of mobile devices and remote access;

q) Encryption: Policies which address the use of cryptographic controls for information in a manner which is supported by current industry standards;

r) Patching and Vulnerability Management: Implemented tools and procedures for routine vulnerability scanning, identification, mitigation Procedures for and applying security patches and updates in a manner consistent with system developer recommendations and industry best practices;

s) Incident and Event Reporting and Management: Documented procedures for monitoring security events, identifying security incidents, responding to and mitigating security incidents, and data breach response and notification;

t) Disaster Recovery and Contingency Planning: Documented procedures for disaster response, data recovery, and emergency mode operations;

5. Storage of Customer Confidential Information. Licensor shall classify as confidential all Customer Confidential Information and all storage media holding Customer Confidential Information to the extent consistent with Licensor's then current storage taxonomy. Storage of Customer Confidential Information must be handled in a manner consistent with the access principles in Section 5 above. Records containing Customer Confidential Information in paper format must be stored and secured appropriately in areas to which access is restricted to authorized Workers. Licensor shall ship Customer Confidential Information that is not in electronic format via commercial courier or a delivery mechanism that allows for accurate tracking of delivery status but may hand deliver records. Records containing Customer Confidential Information in electronic format must be stored in a secure computer network satisfying the requirements of this Section 6, the adequacy of which Licensor will monitor to protect Customer Confidential Information against emerging security threats, and which Licensor will enhance as necessary to address such threats. Customer Confidential Information cannot be stored electronically outside of Licensor's network environment without the customers approval and then only if the storage device (e.g., laptop, computer disk, etc.) is protected by appropriate encryption technology which aligns with the industry standards for strong encryption such as those published by NIST. In addition, the following safeguards will be employed:

a) **Media Disposal**. Licensor shall dispose of any media which stores Customer Confidential Information in accordance with its Secure Destruction policies which will contain sanitization guidelines.

b) Licensor shall maintain written certification that retired media has been properly destroyed in accordance with its Secure Destruction Policies.

c) **Media Transport**. Licensor may not transport or ship media containing Confidential Information or Sensitive Data unless the media is Encrypted using Strong Encryption.

d) **Media Re-Use**. Licensor shall not donate or sell, any media which is known to have stored Customer data to any third party.

e) Media Sanitization. Licensor shall sanitize media which stores Customer data before reuse by Licensor within the Licensor facility in accordance with its Secure Destruction policies which will contain sanitization guidelines.

f) **Audit Logging** Licensor agrees to implement audit logging on any Licensor systems which store Customer data. Audit Log entries must be generated for the following general classifications of events to the extent applicable to the Licensor systems: view access to PHI by unique user ID, login/logout (success and failure); failed attempts to access system resources (files, directories, databases, services, etc.); system configuration changes; security profile changes (permission changes, security group membership); changes to user privileges; actions that require administrative authority (running privileged commands, running commands as another user, starting or stopping services, etc.).Each Audit Log entry will include appropriate information about the logged event such as date and time of event; type of event; user associated with event; and logical identifiers (e.g. system name and port).

6 Vulnerability Management. Licensor shall employ threat and vulnerability management procedures on any networks which store Customer data. Licensor agrees to provide summary evidence of external scans to Customer upon request. Procedures shall include but not be limited to; Regular routine internal and external vulnerability scans; Routine network and application layer penetration tests (not less than annually); A process to identify new vulnerabilities and assign a risk-based criticality rating; A process to identify, alert operations staff and respond to security threats; A risk-based remediation process to address any findings. Licensor shall immediately initiate a project to address remediation of any critical findings.

7. Transmission of Information. An electronic record that contains Customer Confidential Information cannot be transmitted electronically outside a secure network environment satisfying the requirements of Section 6 other than by a secure network connection or by communications protected by appropriate encryption technology which aligns with encryption standards for strong encryption applicable to Licensor's industry. Likewise, Licensor shall not require any individual to transmit Customer Confidential Information over the internet unless the connection is secure or the Customer Confidential Information is protected by encryption technology meeting this standard. The Licensor agrees to maintain a current security certificate on any secured web site and provide evidence of a valid certificate to Customer upon request. Licensor shall disable or replace components or transport security protocols which are outdated or known to be vulnerable.

8. **Information Security Incidents**. Licensor shall provide an escalation procedure to advise the Customer without undue delay, at the latest within 3 days, afterbecoming aware of any security, event or incident which has impacted the confidentiality, integrity, or availability of the Customers data. Such notification shall include the details of the Information Security Incident, along with a description of the Customer Confidential Information or Personal Data that may have been accessed, the effect of the Information Security Incident on the Customer Confidential Information or Personal Data, and the corrective action taken or to be taken by Licensor but Licensor will be under no obligation to provide information which puts its information security program or third party data at risk. At its sole expense, Licensor shall promptly take all appropriate corrective actions and shall cooperate with the Customer in all reasonable and lawful efforts to mitigate or rectify such Information Security Incident (including, without limitation, cooperation in complying with applicable breach notification laws).

9. **Inspection and Audit.** During each calendar year, Licensor will, at Licensor's cost, will cause to be conducted such audits and retain such certifications as agreed with the Customer and as set out in the Agreement.

Such Audits and Certifications are limited to:

SOC 1, Type II, SOC 2, Type II, (SSAE 18, or ISAE3402) report provided by an independent public accounting firm. Each SOC 1 and SOC 2 or ISAE3402 audit shall be conducted with the objective of obtaining a final, unqualified audit opinion for the applicable calendar year. The control objectives shall be based upon guidance from the Information Technology Governance Institute

ISO27001:2013 Certification. ISO 27001:2013 is an internationally recognized and accepted specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

HIPAA. Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.

Detected Weakness; Unless otherwise agreed by the Parties, the, Licensor shall promptly remediate any material weakness or deficiency revealed by any such audit. Customer and its external auditors will be provided copies of relevant reports within a reasonable period following issuance, including any subsequent reports issued following Licensor's remediation of material weaknesses or deficiencies, as soon as reasonably possible after the conclusion of each such audit. Customer shall have the right to provide a copy of such reports to any applicable regulators. At Customer's request, Licensor shall confirm in writing that there have been no changes in the relevant policies, procedures and internal controls since the completion of any such audit or, as applicable, that material weaknesses or deficiencies have been remediated (i.e., through a mutually agreeable representation letter).

Customer reserve the right to, not more than once, annually ,upon request and with reasonable notice of not less than 30 days, perform an audit or security assessment of Licensor's compliance with this Agreement as well as Licensor's overall regulatory compliance. Such an audit may include, but is not limited to, a review of internal compliance related policies and procedures, documentation of compliance activities, the Licensor's annual self-audit and remediation plans, or other similar items. Licensor agrees to cooperate fully and in a timely manner with any Customer requests related to audits or security assessments. Notwithstanding the above Licensor shall not be obligated to place its information security program or third party data at risk.

10. **Destruction and Return of Customer Information.** Pursuant to the Agreement, within thirty (30) days of the completion of Licensor's services for the Customer (or such earlier time as the Customer requests) and at the Customer's discretion, Licensor shall return to Customer or securely destroy all Customer Information in Licensor's possession, custody or control in such a manner as to eliminate the possibility that Customer Information is capable of being read or reconstructed. In addition, upon request Licensor shall provide to Customer a written certification by an officer of Licensor confirming that such return or destruction occurred. If Licensor cannot destroy or destruction is not practical, all Customer Information as required herein due to recordkeeping law, technological constraints or the pendency of litigation requiring Licensor to retain the Customer Information in its existing format, Licensor shall ensure the confidentiality of the Customer Information, that it shall not use or disclose Customer Information after termination of its services for the Customer in a manner inconsistent with its obligations hereunder or the underlying Agreement, and that it will comply with its destruction obligations once the legal prohibition on destruction has expired or the technological constraints have been removed.

SCHEDULE C
(MODEL CLAUSES)

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: [Enter Customer name here] .....

Address:.....

Tel.: ..... ; fax: .....;e-mail: ..... ;

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: [Enter SAI Global Entity here] .....

Address: .....

Tel.:..... ; fax: .....;e-mail: .....

Other information needed to identify the organisation:

……,

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Schedule 1 (as outlined in DPA section 2.4 above).

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.