



G-Cloud Master Services Agreement

FRAMEWORK REFERENCE: RM1557.14

Contents

1. DEFINITIONS AND INTERPRETATION	1
2. TERM	5
3. PROVISION OF SERVICES	5
4. CLIENT OBLIGATIONS	6
5. FEES AND PAYMENT	8
6. INTELLECTUAL PROPERTY RIGHTS AND INDEMNITY	9
7. CONFIDENTIALITY	10
8. WARRANTY	12
9. LIMITATION OF LIABILITY	12
10. TERMINATION	13
11. DATA PROTECTION	14
12. EMPLOYEES	15
13. Employment Regulations	16
14. ANTI-SLAVERY	16
15. MISCELLANEOUS	17
SCHEDULE 1 - CHANGE CONTROL PROCEDURE	21
SCHEDULE 2 - DATA SECURITY POLICY	23
SCHEDULE 3 - DATA PROCESSING TERMS	26
SCHEDULE 4 - STATEMENT OF WORK PRO FORMA	30
SCHEDULE 5 – FRAMEWORK-LEVEL DATA PROCESSING DESCRIPTION AND COGNIZANT THIRD PARTY SUBPROCESSORS	32
SCHEDULE 6 - STANDARD CONTRACTUAL CLAUSES	33

THIS AGREEMENT is made on the date on which all parties have executed this Agreement.

BETWEEN

- (1) **[Insert Client Name]** a company incorporated and registered in England and Wales (company number []) which has its registered office at [] (“**Client**”); and
- (2) **COGNIZANT WORLDWIDE LIMITED** a company incorporated and registered in England and Wales (company number 07195160) which has its registered office at 280 Bishopsgate, London EC2M 4AG (“**Cognizant**”).

IT IS HEREBY AGREED as follows:

1. DEFINITIONS AND INTERPRETATION

In this Agreement and each SOW:

- 1.1. “**Acceptance**” means the acceptance or deemed acceptance of a Deliverable by the Client, as provided in clause 3.3 and “Accepted” shall be construed accordingly.
- 1.2. “**Acceptance Criteria**” means the criteria for acceptance of a Deliverable set out in the relevant SOW.
- 1.3. “**Acceptance Date**” means the date set out in a SOW by which the Client must notify Cognizant of its acceptance of a Deliverable, or if no date is specified in the SOW, then the date determined in accordance with clause 3.3.
- 1.4. “**Acceptance Testing**” means the conduct of agreed tests set out in the relevant SOW (or, if no such tests are set out, such tests as are agreed by the parties) to determine if a Deliverable has been Accepted.
- 1.5. “**Affiliate**” means, with respect to a legal entity, any other legal entity which is from time to time a direct or indirect subsidiary or holding entity of that entity or a direct or indirect subsidiary of any such holding entity.
- 1.6. “**Agreement**” means these terms and conditions, the attached schedules and any document referred to and incorporated herein by reference, as may be amended by the parties from time to time.
- 1.7. “**Anti-Slavery Laws**” mean all applicable anti-slavery and human trafficking laws, statutes and regulations, including to the Modern Slavery Act 2015.
- 1.8. “**Change**” has the meaning given to it in clause 3.4.
- 1.9. “**Change Order**” means a written statement signed by the parties, in the format set out in the Appendix to Schedule 1, recording the parties' agreement to make changes pursuant to the Change Control Procedure.
- 1.10. “**Change Control Procedure**” means the procedure described in clause 3.4 and schedule 1 to make changes to the Services.
- 1.11. “**Change Control Proposal**” has the meaning given to it in paragraph 4 of schedule 1.
- 1.12. “**Change Request**” has the meaning given to it in paragraph 3 of schedule 1.
- 1.13. “**Client Employee**” means any individual employed by the Client or its Affiliates or any subcontractors of the Client or its Affiliates;
- 1.14. “**Client Entity**” means the Client, any of its Affiliates

- 1.15. **“Client Materials”** means any software, systems, hardware, documentation, information, data or other materials owned by or licensed by a third party to the Client that are provided to a Cognizant Entity by or on behalf of the Client and which may be used by a Cognizant Entity in connection with the provision of the Services.
- 1.16. **“Cognizant Entity”** means Cognizant, any of its Affiliates or any of its or their sub-contractors.
- 1.17. **“Cognizant Intellectual Property”** means Intellectual Property Rights that have been or are acquired or developed by or on behalf of Cognizant or its licensors (including Third Party Items) before, on or after the Effective Date and any modifications, enhancements or derivatives of such Intellectual Property Rights but excluding Newly Created IPR.
- 1.18. **“Confidential Information”** means all information or proprietary materials which is disclosed before or after the Effective Date by one party (**“disclosing party”**) to the other (**“receiving party”**), however conveyed (including by way of oral descriptions, demonstrations or observations), and which relates to the business affairs of the disclosing party or its Affiliates, customers, employees, suppliers or subcontractors, including existing or contemplated products, services, operations, technology, processes, plans or intentions, developments, trade secrets, know-how, design rights, technical data, engineering, techniques, methodologies and concepts, market opportunities, business plans, sales, pricing and other financial information, unpublished patent specifications, photographs, databases, computer software in disk, cassette, tape or electronic form and data storage or memory in, any items of, computer hardware or any other materials or media of whatever nature and all information derived from the above, together with the existence and provisions of this Agreement and all SOWs and the negotiations relating to them.
- 1.21. **“Data Protection Legislation”** means 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, and repealing Directive 95/46/EC ("General Data Protection Regulation"), including any applicable delegated acts adopted by the European Commission and any applicable national legislation made under or otherwise adopted by Member States of the EEA pursuant to specific rights or powers contained within the General Data Protection Regulation, together with any replacement legislation or any equivalent legislation of any other applicable jurisdiction and all other applicable laws and regulations in any relevant jurisdiction relating to the processing of personal data and privacy.
- 1.19. **“Deliverables”** means the items specifically identified in the relevant SOW which Cognizant is obliged to produce and/or develop specifically for, and to provide to, the Client.
- 1.20. **“Dispute”** means any contractual or other dispute, controversy, difference, claim, or question of interpretation arising out of, or in connection with, this Agreement or a SOW or the breach thereof.
- 1.21. **“EEA”** means the European Economic Area.
- 1.22. **“Effective Date”** means [the date on which all parties have executed this Agreement] [OR] [Insert Date].
- 1.23. **“Employment Regulations”** means the Acquired Rights Directive 2001/23/EC (as amended, replaced or consolidated from time to time) including in any jurisdiction (whether in the European Union or not), any legislation which incorporates the Acquired Rights Directive 2001/23/EC (as amended from time to time) into local law or any legislation dealing with the transfer by operation of law of the employment of employees from one employer to another including the Transfer of Undertakings

(Protection of Employment) Regulations 2006 (SI 2006/246) and any predecessor regulations.

- 1.24. **“Fees”** means all monies payable by the Client to Cognizant in connection with performance of the Services and/or supply of the Deliverables, including all charges and compensation, in accordance with the provisions of this Agreement and as set out in the relevant SOW.
- 1.25. **“Force Majeure Event”** means an event which is beyond the reasonable control of the party affected by it (or its Affiliates or sub-contractors), including act of God, natural disasters, fire, flood, storm, war, military action, riot, civil commotion, acts of state, terrorism, epidemic, pandemic, explosion, malicious damage, non-availability of public networks, accident or breakdown of machinery, strike, lock-out or labour disputes.
- 1.26. **“Good Industry Practice”** means the standard of skill, care, knowledge and foresight which would reasonably and ordinarily be expected from a person engaged in providing services which are the same as the relevant services in similar circumstances.
- 1.27. **“Intellectual Property Rights”** or **“IPRs”** means: patents, utility models, supplementary protection certificates, petty patents, rights in trade secrets and other confidential or undisclosed information (such as inventions (whether patentable or not) or know-how), registered designs, rights in copyright (including authors' and neighbouring or related rights), database rights, design rights, trademarks and service marks and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.
- 1.28. **“Latent Data”** means data that is stored by a party on routine back-up media for the purpose of disaster recovery including, but not limited to deleted files and other non-logical data types, memory dumps, swap files, temporary files, printer spool files and metadata that can customarily be retrieved only by computer forensics experts and is generally considered inaccessible without the use of specialised tools and techniques.
- 1.29. **“Newly Created IPR”** means those materials and Intellectual Property Rights created specifically for the Client pursuant to this Agreement or any SOW but excluding modifications, enhancements or derivatives of Cognizant Intellectual Property
- 1.30. **“Residual Information”** means the general knowledge, ideas, know-how, experience, and techniques that would be retained in the unaided memory of an ordinary person skilled in the art, not intent on appropriating the proprietary information of the disclosing party.
- 1.31. **“Services”** means the services to be provided by Cognizant to the Client under the Statements of Work, including the development of any Deliverables.
- 1.32. **“Specifications”** means the specifications for the Deliverables set out in the relevant SOW.
- 1.33. **“Statement”** means any warranty, statement, representation, misrepresentation (as to facts or otherwise) understanding, undertaking, proposal or other communication.
- 1.34. **“Statement of Work”** or **“SOW”** means a document agreed in writing by the parties thereto pursuant to the terms of this Agreement setting out specific Services and Deliverables to be provided by Cognizant to the Client (or its Affiliate) and all relevant requirements and information relating thereto, including project scope, project activities and tasks to be performed by each party, their roles and responsibilities, assumptions, any delivery timescales, relevant Acceptance Criteria, Acceptance Date, Acceptance Testing, the charging mechanism and the applicable Fees, where applicable, a data processing description, and including any document referred to and incorporated therein by reference. A pro forma SOW is included at Schedule 4 (SOW Pro Forma).

- 1.35. **“Tax”** means all taxes, imposts, duties, levies, or fees of any kind payable to any governmental, fiscal or taxing authority in the United Kingdom or elsewhere. The definition of “Tax” includes any penalties, additions, fines or associated interest. The words **“Taxes”** and **“Taxation”** and similar expressions will be interpreted in accordance with this definition.
- 1.36. **“Third Party Items”** mean any third party software, tools, applications, utilities, cloud infrastructure or IPR owned or licensed by a third party that may be distributed, resold, or otherwise provided by Cognizant.
- 1.37. **“Trade Control Laws”** include trade, export control, import, and antiboycott laws, as well as economic or financial sanctions and trade embargoes, in each case, imposed, administered, or enforced in countries where the Client and Cognizant operates, including those laws administered by the European Union or its Member States, Her Majesty’s Treasury of the United Kingdom, the U.S. government, or the United Nations Security Council.
- 1.38. **“Warranty Period”** means a period of thirty (30) days following Acceptance of the relevant Deliverable or such other period set out in the applicable SOW.
- 1.39. **“Working Day”** means a day (other than a Saturday or Sunday) on which the retail banks are ordinarily open for business in the relevant location.
- 1.40. **Interpretation.** In this Agreement and any SOW: (a) the clause headings are inserted for convenience only and shall not affect in any way the meaning or interpretation of this Agreement or any SOW; (b) reference to any agreement, contract, document or deed shall include that document as varied, supplemented or novated from time to time; (c) reference to a party shall, upon any assignment or other transfer that is permitted by this Agreement, be construed to include those successors and permitted assigns or transferees; (d) the words “including”, “include”, “for example”, “in particular” and words of similar effect shall not limit the general effect of the words which precede them; (e) references to a clause are references to a clause of this Agreement or of a SOW, as the context requires; (f) references to any notice given under this Agreement or any SOW shall mean a notice given in accordance with clause 15.4; (g) reference to any legislative provision shall be deemed to include any statutory instrument, by-law, regulation, rule, subordinate or delegated legislation or order and any rules and regulations which are made under it, and any subsequent re-enactment or amendment of the same; (h) a reference to a person will include any individual, firm, partnership, organisation, institution, trust or agency, corporate body and unincorporated association; and (i) words used in the singular tense should be interpreted to include the plural tense and vice versa, and words which refer to one gender should be interpreted to include other genders.
- 1.41. **Order of Precedence and Relationship between Agreement and SOWs.**
- (a) If there is any conflict, ambiguity or inconsistency between the clauses of this Agreement and any SOW, the clauses of this Agreement shall prevail.
 - (b) This Agreement governs the relationship between the Client/its Affiliates and Cognizant/its Affiliates in respect of the provision of the Services by Cognizant and/or its Affiliates to the Client and/or to the Client’s Affiliates pursuant to SOWs entered hereunder.
 - (c) The parties acknowledge and agree that, notwithstanding the terms of any purchase order or other documents (even where such purchase order or other documents are expressed to apply to the provision of the Services), only the terms of this Agreement and applicable SOWs will apply to the provision of the Services to the exclusion of any such terms (including the exclusion of such purchase order terms or other documents).

2. TERM

This Agreement shall come into force on the Effective Date and shall continue unless and until terminated in accordance with its terms. The term of each SOW shall be set out in that SOW.

3. PROVISION OF SERVICES

3.1. **Services.** Cognizant shall provide the Services in accordance with this Agreement and the relevant terms set out in each SOW.

3.2. **Statements of Work.** Cognizant and the Client may, but are not obligated to, develop and enter into one or more SOWs. Each SOW shall be a separate and independent contract between the parties to it, shall specifically identify this Agreement and shall be subject to and incorporate the terms and conditions of this Agreement. A SOW shall not be effective unless executed by a representative of each party to it. The Agreement shall remain in effect until the completion of any outstanding Statements of Work.

3.3. **Acceptance of Deliverables.** If Cognizant provides any Deliverable where: a) a SOW says such Deliverable is subject to testing; or b) where Cognizant otherwise agrees in writing that such Deliverable should be tested, then the remainder of this clause 3.3 shall apply:-

- (a) The Client shall review, evaluate and/or carry out Acceptance Testing in respect of each Deliverable by the applicable Acceptance Date to determine if such Deliverable satisfies the applicable Acceptance Criteria in all material respects. If the SOW does not set out an Acceptance Date for a Deliverable then the Acceptance Date shall be five (5) Working Days from delivery of the relevant Deliverable to the Client.
- (b) Cognizant shall provide reasonable assistance to assist the Client in carrying out the Acceptance Testing.
- (c) The Client shall promptly notify Cognizant in writing of its acceptance of the Deliverable. The Client shall be deemed to have accepted a Deliverable at the earlier of: (a) the Client not providing a written notice to Cognizant specifying that such Deliverable has failed to meet its Acceptance Criteria in all material respects by the Acceptance Date; or (b) the Client placing the Deliverable into operation in a production environment.
- (d) The Client shall promptly notify Cognizant if a Deliverable fails the Acceptance Testing, and Cognizant shall use reasonable endeavours to remedy such failure at its cost within a reasonable amount of time. If Cognizant fails to remedy the affected Deliverable then the Client may, by written notice to Cognizant, at its sole option:
 - (i) accept the Deliverable as is; or
 - (ii) reject the Deliverable and/or terminate the relevant SOW pursuant to clause 10.1(a).

3.4. **Project Schedule and Changes.** Each SOW shall set out (a) the projected allocated activities/responsibilities of each party; (b) time scales applicable to the Services; and (c) where applicable, a data processing description in the format set out in Schedule 4 Annex A. All statements and agreements concerning time are good faith estimates based upon information available and circumstances existing at that time, including any assumptions set out in the SOW. Each SOW is subject to amendment in the event of any change in such information, circumstances or assumptions, the occurrence of

a failure or delay by the Client or third party to comply with its obligations, or upon modification of the scope, timing or level of work or resources to be performed or provided by Cognizant (“**Change**”). The parties acknowledge that any such Change may have an impact on the Fees, the project schedule and other services. Either party shall be entitled to propose Changes in accordance with the Change Control Procedure or otherwise agreed in writing pursuant to clause 15.5. Neither party shall have any obligation in respect of any Change until agreed in writing pursuant to clause 15.5 or under an agreed Change Order.

- 3.5. **Affiliates.** Cognizant may engage any of its Affiliates to provide Services and Deliverables to the Client and any Affiliate of the Client under this Agreement. Notwithstanding anything to the contrary in this Agreement, Cognizant will remain fully liable for Services and Deliverables provided under this Agreement by its Affiliates. Any Affiliate of the Client may enter into SOW(s) with Cognizant and, only for the purposes of any such SOW(s), shall be considered “Client” as that term is used in this Agreement.

4. **CLIENT OBLIGATIONS**

- 4.1. **Working Environment.** The Client shall provide for Cognizant, its agents, subcontractors, consultants and employees, in a timely manner and at no charge: (a) access to the Client’s and its relevant Affiliates’, contractors’ or customers’ premises, suitable office accommodation, equipment, data, information and other facilities (including Client Materials) as required by Cognizant and be responsible for preparing and maintaining the relevant premises or equipment and Client Materials for the supply of the Services; (b) the same appropriate training as it provides to its own staff on health and safety and information security policies relevant to each such premises and inform Cognizant in writing of all health and safety rules and regulations and any other reasonable security requirements that apply at any of the Client’s or relevant Client Affiliates’ premises from where the Services are provided; (c) obtain in advance and maintain all necessary licences and consents and comply with all relevant legislation in relation to the Services including obtaining all relevant third party licences and consents to allow Cognizant to access and use Client Materials; and (d) any other items set out in the relevant SOW.
- 4.2. **Client’s Personnel Commitment.** The Client shall, and shall ensure that all its personnel and those of its relevant Affiliates and contractors who may be necessary or appropriate for the successful implementation of the Services, co-operate with Cognizant in all matters relating to the Services and, on reasonable notice: (a) are available to assist Cognizant’s personnel by answering business, technical and operational questions and providing requested information, documents, guidelines and procedures in a timely manner; (b) participate in the Services as set out in the SOW; (c) participate in Service-related meetings as requested by Cognizant; (d) contribute to any software and system testing, including testing of the Deliverables; (e) provide such information and documentation as Cognizant may require, and ensure the accuracy of the same; and (f) are available to assist Cognizant with any other activities or tasks required to complete the Services in accordance with the SOW. The Client acknowledges that, except where Cognizant is notified otherwise in writing, Cognizant Entities will be entitled to rely on the apparent authority of any Client’s personnel providing instructions to them whom it is reasonable to assume is authorised to do so, and Cognizant shall not be liable for any consequences of Cognizant following the instructions of actual or apparently authorised Client’s personnel or of its contractors as applicable.
- 4.3. The Client shall be responsible for, and assumes the risk of, any problems or delays resulting from the content, accuracy, completeness and consistency of all such data, materials and information supplied by the Client.

- 4.4. The Client shall, and shall ensure that all its personnel and those of its Affiliates and contractors: (i) do not access any of Cognizant's or its other clients' premises without the prior written consent of Cognizant; and (ii) comply at all times with Cognizant's security policy and instructions when at Cognizant's premises.
- 4.5. **Visa/Work Permits.** In the event that it is necessary for Cognizant to obtain visas or work permits for Cognizant's personnel involved in the provision of the Services, the Client shall cooperate with Cognizant by taking all reasonably necessary actions as requested by Cognizant to facilitate Cognizant's efforts in that respect.
- 4.6. **Export Control.** Both parties shall comply with all export control laws and regulations of the US, UN, EU and its Member States and other countries (hereinafter referred to as "Export Control Laws") applying to the performance, receipt, or use of the Services, Deliverables, software, subscription service, documentation, technology, data, information, items, or Client Background IP (hereinafter collectively referred to as "Export Controlled Items").
- (a) Client shall notify Cognizant, sufficiently in advance, of:
- (i) any Export Control Laws (e.g. EAR, ITAR, EC Regulation (EC) No. 428/2009) and classifications (e.g. ECCN) applicable to the Export Controlled Items;
 - (ii) any significant information with regard to any import or export license or any other governmental authorization potentially required for the provision, delivery, receipt, use, import, export, re-export and/or intra-community transfer of the Export Controlled Items; and
 - (iii) any significant information regarding refusal, delay of granting or extension, amendment or lapse of import or export licenses or any other governmental authorizations, embargoes and/or sanctions relevant for the Export Controlled Items.
- (b) Client shall obtain and maintain all necessary licenses, consents and permits required for the unrestricted provision, delivery, receipt, use, import, export, re-export and/or intra-community transfer of Export Controlled Items. For the avoidance of doubt, if Client or, on behalf of the Client, Cognizant (including its Affiliates): imports, exports, re-exports and/or transfers any Export Controlled Items, from the place of performance (or any other place where the Export Controlled Items are explicitly designated to be used as determined in the relevant SOW), to any other place, then such transfer is performed solely at Client's risk and responsibility and Client is responsible for compliance with any applicable Export Control Laws.
- (c) Notwithstanding the foregoing, Client agrees that it will not provide Cognizant with any technology, technical data, Client Background IP or information that is subject to control under the ITAR (International Traffic in Arms Regulations) or other military or defence-related export controls.
- 4.7. **Export Authorisations.** Client shall obtain, maintain, and share with Cognizant, all necessary licenses, consents and permits required for the unrestricted provision, delivery, receipt, use, import, export, re-export, transfer, or retransfer of Export Controlled Items.
- 4.8. **Corruption and Bribery.** Each party shall comply with all applicable laws and regulations regarding anti-corruption and anti-bribery. To the extent that the Services or Deliverables cannot be performed or provided without violation of any law, regulation, or other control, then Cognizant shall not be obligated to provide the same and the applicable SOW shall be amended accordingly.

- 4.9. **Economic Sanctions.** Client acknowledges and warrants that, for commercial reasons, Cognizant's Services will not include support of Client or Client's Affiliate business activity in the countries and jurisdictions of Cuba, Iran, North Korea, Syria, Russia, Belarus, and the Crimea, Kherson, Zaporizhzhia, Donetsk, and Luhansk regions of Ukraine. Furthermore, Client represents and warrants that Client and those under its reasonable controls shall not use the Services and/or Deliverables to engage, facilitate, or support countries, persons, and institutions subject to any applicable economic sanctions enforced by the US, UK, EU, EU member states, and other countries, including Cuba, Iran, North Korea, Syria, Russia, Belarus, and the Crimea, Kherson, Zaporizhzhia, Donetsk, and Luhansk regions of Ukraine.

5. **FEES AND PAYMENT**

- 5.2 5.1 **Fees.** The Client shall pay Cognizant the Fees. The Client shall reimburse Cognizant for all reasonable out-of-pocket travel, living, ancillary expenses and other reimbursable items paid or incurred by Cognizant in connection with the provision of the Services. Cognizant shall have no obligation to perform any Services when any amount required to be paid by the Client remains due and unpaid beyond the date such amount is due. Any suspension of Services by Cognizant as a result of the Client's failure to make payment as required shall extend the due dates of Deliverables and other Services to the extent impacted by such suspension or delay, and Cognizant shall not be liable to the Client for any liabilities, losses, costs or damages arising therefrom. Cognizant may offset any liability or payment due to the Client against future Fees payable via a credit note. **Rates.** Starting 12 months after the Effective Date and every 12 months thereafter, the rates for Services provided on a time & material basis, including any rates included in any SOW, shall be automatically increased for inflation based on the percentage change in the then-prior 12 month period to the index of inflation applicable to the country from which the Services are being provided. The applicable index of inflation is CPI-UK for UK based Services, CPI-IW (Industrial Worker) for India-based Services and, for any other country, the most analogous and commonly accepted index of inflation used in such country, which shall be mutually agreed by the parties using good faith efforts. The relevant rates shall be increased by the same percentage as the positive percentage difference between the applicable inflation index for the then-current year and the inflation index on the date that was 12-months prior to the then-current year.
- 5.3 **Invoicing.** Unless otherwise set out in a SOW, Cognizant shall invoice the Client for all Fees and reimbursable items payable to Cognizant monthly in arrears. The Client shall pay each invoice within thirty (30) days of the date of such invoice without deduction or setoff, provided that the Client may withhold payment of invoiced amounts which are promptly disputed in good faith pending resolution of such good faith dispute. Client must notify Cognizant in writing of any dispute or disagreement with invoiced charges within thirty (30) days after the date of invoice. In the absence of such notice, Client shall be deemed to have agreed to the charges as invoiced after the expiration of such time period.
- 5.4 **Taxes.**
- (a) All fees are exclusive of Taxes. Client shall pay amounts equal to any federal, state or local sales, use, excise, privilege, value added, goods and services or other taxes, duties, imposts, levies or similar assessment relating to the Services and Deliverables provided by Cognizant hereunder, exclusive of taxes based on Cognizant's net income or net worth.
 - (b) Client and Cognizant agree to cooperate on any tax matters arising from the provision of the Services and Deliverables under this Agreement. Both parties agree to provide reasonable assistance to the other in order to mitigate any taxes applicable to the Services and Deliverables provided to Client or to

payments made pursuant to this Agreement with respect to the Services and Deliverables.

- (c) Where withholding taxes apply under applicable law, Client shall provide to Cognizant reasonable assistance, which shall include the provision of documentation as required by revenue authorities (including official receipts and withholding tax certificates) to enable Cognizant to claim exemption from or obtain a repayment of such withheld taxes. Client shall provide Cognizant with the required documentation sent to: Tax Department, Cognizant Technology Solutions U.S. Corporation, 300 Frank W. Burr Boulevard, Teaneck, New Jersey 07666. Client shall accept valid exemption certificates and forms to reduce or eliminate withholding taxes.

6. INTELLECTUAL PROPERTY RIGHTS AND INDEMNITY

- 6.1. **Deliverables.** Subject to clause 6.3, upon payment in full, the Deliverable shall become the property of the Client and the Newly Created IPR shall vest in the Client. The Client's ownership of a Deliverable does not include any Cognizant Intellectual Property that is incorporated into the Deliverable. Cognizant agrees to take, at the Client's cost and expense, such steps and actions requested by the Client which are reasonably necessary to assure the conveyance to the Client of all right, title and interest in and to the Deliverable, including copyright.
- 6.2. **Residual Rights.** Nothing in this Agreement or any SOW shall prohibit or restrict (a) Cognizant or its Affiliates or their respective employees, agents, or subcontractors from using or disclosing in the course of its business any Residual Information acquired by such persons in the performance of the Services, provided that in so doing it does not breach any obligation of confidentiality arising pursuant to this Agreement or any SOW; or (b) the use or exploitation by Cognizant and its Affiliates of any Cognizant Intellectual Property.
- 6.3. **Cognizant Intellectual Property.** The Client acknowledges that as part of performing the Services, Cognizant's personnel may utilize Cognizant Intellectual Property and Residual Information. The Client acknowledges that Cognizant Intellectual Property and Residual Information, and any derivatives of Cognizant Proprietary Intellectual Property or Residual Information, is the sole property of Cognizant (or its licensor) and that Cognizant (or its licensor) shall at all times retain sole and exclusive title to and ownership thereof. Where Cognizant Intellectual Property owned by Cognizant is embedded into a Deliverable, the Client is hereby granted a royalty-free, non-exclusive and non-transferable right to use such Cognizant Intellectual Property solely in conjunction with the relevant Deliverable and for the purpose of its intended use, subject to (a) the restriction that it may not be extracted from that Deliverable or used as a standalone product and (b) any further limitations set out in the relevant SOW. Save as set out in this clause 6.3, nothing in this Agreement or any SOW shall be construed to grant to the Client any right, title, licence or other interest in, to or under any Cognizant Intellectual Property. Any license to Cognizant Intellectual Property that is (i) not embedded in a Deliverable; or (ii) commercially available, will be pursuant to a separate license agreement between the Client and Cognizant (or its licensor).
- 6.4. **Third Party Items.** Cognizant shall obtain the Client's prior consent before embedding in any Deliverables or installing in the Client's environment any Third Party Items. Any such Third Party Items will be made available to the Client under a separate agreement between the Client and the licensor of the Third Party Item or will be made available to the Client by Cognizant under a separate agreement with terms passed through from the supplier of the Third Party Item. To the extent Cognizant is entitled to do so under the applicable third party agreement, where the Third Party Item is made available to the Client by Cognizant under a separate agreement, Cognizant shall pass through to the Client any end-user warranties and indemnities offered by the third party supplier and/or shall use commercially reasonable efforts to enforce the warranties and

indemnities on behalf of the Client. Third Party Items are provided or recommended by Cognizant AS-IS and without any warranty, liability or indemnity of any kind from Cognizant.

- 6.5. **Client Materials.** All Client Materials will be owned by or fully licensed to the Client. Cognizant acknowledges that Client Materials are the sole property of the Client (or its licensor) and the Client (or its licensor) shall at all times retain sole and exclusive title to and ownership thereof. Cognizant Entities are permitted to use and modify the Client Materials as necessary to perform the Services. The Client will reasonably cooperate with Cognizant in respect of any audit related to Cognizant's use and possession of Client Materials or Client's use and possession of Cognizant Intellectual Property.
- 6.6. **Indemnity.** Cognizant and the Client (in such case, the "**indemnifying party**") each agree to indemnify the other (in such case, the "**indemnified party**") from and against any costs and damages awarded against the indemnified party by a court pursuant to a final judgment or a settlement by the indemnifying party, as a result of, and defend the indemnified party against, any claim of infringement of any patent or copyright related to the possession of a Deliverable (in the case of indemnification by Cognizant) or any claim relating to Cognizant's possession, use or modification of any Client Materials or breach by Client of any third party licence terms in respect of any Third Party Item provided to the Client by Cognizant (in the case of indemnification by the Client) ("**IPR Claim**"). The conduct of any IPR Claim shall be in accordance with clause 15.1.
- 6.7. **Exclusions.** Cognizant shall have no obligation under clause 6.6 or other liability for any IPR Claim to the extent resulting or alleged to result from: (a) use of the Deliverables or any part thereof in combination with any equipment, software or data not approved for use by Cognizant, or use in any manner for which the Deliverable was not designed, or any modification or alteration of the Deliverable by a person or entity other than Cognizant or its Affiliates or subcontractors; (b) any instructions, designs, specifications, information or materials provided by or on behalf of the Client to Cognizant; (c) any software or other materials supplied by or via any third party (including any Third Party Items); or (d) the Client's continuing the allegedly infringing activity after being notified or after being provided with modifications that would have avoided or mitigated the alleged infringement.
- 6.8. **Infringement Remedies.** In the event of an IPR Claim, or if Cognizant reasonably believes that an IPR Claim is likely to be made, Cognizant may, at its option and in lieu of indemnification: (a) modify the applicable Deliverables so that they become non-infringing but functionally equivalent; (b) replace the applicable Deliverables with items that are non-infringing but functionally equivalent; or (c) obtain for the Client the right to use such Deliverables upon commercially reasonable terms. Clauses 6.6 to 6.8 set out the sole and exclusive remedy and entire liability and obligation of each party with respect to IPR Claims.

7. **CONFIDENTIALITY**

- 7.1. **Confidentiality Obligations.** The receiving party shall:
- (a) keep Confidential Information of the disclosing party secret and confidential, and use security measures and a degree of care to protect the Confidential Information which are no less than the receiving party applies to its own confidential or proprietary information of a similar nature, but in no event less than reasonable care;
 - (b) not disclose the disclosing party's Confidential Information to any third party except with the prior written consent of the disclosing party or in accordance with this clause 7; and

- (c) only use the disclosing party's Confidential Information to perform its obligations under this Agreement and SOWs.

7.2. **Exceptions.**

- (a) Notwithstanding clause 7.1, the receiving party may disclose the disclosing party's Confidential Information to its directors and employees (and Cognizant may disclose it to its Affiliates, sub-contractors or other third parties in order to enable Cognizant to provide the Services), who have a need to know such Confidential Information in connection with this Agreement or a SOW (together, "**Representatives**"), provided that such Representatives have executed an agreement with the receiving party with confidentiality provisions that are at least as stringent as the confidentiality requirements under this Agreement. The receiving party shall take reasonable steps to enforce the terms of any such agreement to protect the disclosing party's Confidential Information.
- (b) The obligations set out in clause 7.1 shall not apply in respect of Confidential Information that:
 - (i) was in the receiving party's possession at the time of disclosure and without restriction as to confidentiality;
 - (ii) is or becomes generally available to the public through no breach of this agreement or other wrongful act by the receiving party;
 - (iii) has been received from a third party without restriction; or
 - (iv) is independently developed by the receiving party without regard to the Confidential Information of the disclosing party.

7.3. **Compelled Disclosure.** The receiving party may disclose Confidential Information as required to comply with binding orders of courts and governmental entities that have jurisdiction over it, provided that (insofar as legally permissible) the receiving party: (a) gives the disclosing party reasonable written notice to allow the disclosing party to seek a protective order or other appropriate remedy; (b) discloses only such Confidential Information as is required by the court or governmental entity; and (c) uses commercially reasonable endeavours to obtain confidential treatment for any Confidential Information so disclosed.

7.4. **Return of Confidential Information.** Subject to clauses 7.5 and 7.6, promptly following the earlier of: (a) the termination of this Agreement (unless the return or destruction of such Confidential Information would prohibit or restrict Cognizant's ability to perform its obligations under a SOW); (b) termination of an applicable SOW, and (c) the written request of disclosing party, the receiving party shall destroy or return all documents or other materials provided by disclosing party to the receiving party constituting Confidential Information, together with all copies, including computer disks in the possession of receiving party. Upon request, the receiving party shall confirm such destruction in writing to the disclosing party. Where the request for the return or destruction of Client Confidential Information prevents, hinders or delays Cognizant in the performance of the Services, Cognizant shall have no liability for any non- or partial performance of its obligations or any delay in respect of the same.

7.5. **Latent Data.** Latent Data which is Confidential Information shall be subject to destruction in due course but shall remain subject to clauses 7.1 to 7.3 until it is so destroyed.

7.6. **Legal Counsel.** Notwithstanding anything to the contrary in this clause 7, legal counsel for the receiving party may retain one copy of Confidential Information as well as documents, memoranda, notes and other writings prepared based on the Confidential Information. In addition the receiving party may retain such material or copies of such

material containing Confidential Information furnished by the disclosing party to the extent required by law and may use it solely for the purpose provided by such law. During such retention, all such Confidential Information contemplated herein shall remain subject to clauses 7.1 to 7.3.

8. **WARRANTY**

8.1. **Mutual Warranties.** Each party warrants to the other that:

- (a) it has the requisite power and has taken all actions necessary to execute this Agreement and any SOW; and
- (b) this Agreement and each SOW when signed by each party, constitutes legal, valid and binding obligations of that party in accordance with its terms.

8.2. **Performance Warranties.** Cognizant warrants to the Client that:

- (a) the Services shall be performed by qualified personnel with reasonable diligence and care and in accordance with Good Industry Practice;
- (b) the Services shall conform in all material respects to the applicable requirements set out in the relevant SOW; and
- (c) each Deliverable shall conform in all material respects with its Specifications during the applicable Warranty Period.

8.3. **Remedies.** Cognizant does not warrant that any Deliverable shall operate uninterrupted or error-free, without prejudice to clause 8.2. In the event that any Deliverable fails to conform to the warranty in clause 8.2(c) in any material respect, the sole and exclusive remedy of the Client will be for Cognizant to (at its expense) use commercially reasonable endeavours to cure or correct such failure promptly.

8.4. **Requirements for Warranty Claims.** The warranty in clause 8.2(c) is subject to:

- (a) the Client providing Cognizant with prompt written notice of any warranty claim specifying the non-conformity and such notice being given within the Warranty Period;
- (b) the Client fully cooperating with Cognizant relating to the warranty claim, including assisting Cognizant to locate and reproduce the non-conformity; and
- (c) the absence of any tampering, misuse, failure to comply with Cognizant recommendations or instructions as to use and operation, or any alteration or other modification of such Deliverable by any person or entity other than Cognizant.

8.5. **Client's Responsibility.** If the Client asserts any claim in respect of defective Services or Deliverables hereunder (including under the warranties in clause 8.2) and such claim relates to any matter that is determined not to be Cognizant's responsibility under this Agreement or any SOW (including any problem with Client Materials that was not caused by any Services performed by Cognizant), the Client shall be responsible to pay Cognizant for all evaluation, correction or other services performed by Cognizant relating to such claim on a time and materials basis at Cognizant's then-standard billing rates.

9. **LIMITATION OF LIABILITY**

9.1. This clause 9 sets out the entire liability of the parties (including any liability for the acts and omissions of its employees, agents, subcontractors and Affiliates) in respect of all claims arising under or in connection with this Agreement and any SOW (including under any Standard Contractual Clauses entered into pursuant to this Agreement or

any SOW), whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation, on indemnity basis or otherwise.

- 9.2. Nothing in this Agreement or any SOW shall exclude or limit either party's liability to the other party for: (a) death or personal injury as a result of negligence; (b) fraud or fraudulent misrepresentation; (c) any other liability which cannot be limited or excluded by law; or (d) as regards the Client, any claim by Cognizant for Fees due for payment.
- 9.3. Subject to clause 9.2, in no event shall either party (including its Affiliates) be liable to the other in contract, tort (including negligence), breach of statutory duty, misrepresentation, on indemnity basis or otherwise, for any of the following losses or damages howsoever caused and even if such losses and/or damages were foreseen, foreseeable or known, or that party was advised of the possibility of them in advance: (a) any loss of business or business opportunity, loss of revenue, loss of actual or anticipated profits, loss of contracts, loss of anticipated savings, loss of, damage to, or corruption of, data, economic loss, loss of goodwill, in each case whether such losses are direct, indirect or consequential; or (b) any indirect, special, exemplary, punitive or consequential loss or damage.
- 9.4. Subject to clauses 9.2 and 9.3, the maximum aggregate liability of each party (including its Affiliates) to the other party (including its Affiliates), for all causes of action, whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation, on indemnity basis or otherwise, for any losses whatsoever and howsoever caused: (a) arising under or in connection with a SOW shall be limited to the Fees paid under that SOW; (b) provided always that the maximum aggregate liability arising under or in connection with this Agreement (including all SOWs) shall be limited to the total Fees paid under this Agreement (including all SOWs) in the twelve (12) months prior to the first claim (where the first claim is made after the termination of this Agreement, this limitation shall be calculated as being an amount equivalent to the amount in the final twelve (12) months of this Agreement or the last SOW as applicable); save that neither party's liability in respect of clause **Error! Reference source not found.** (Employment Regulations) shall be capped.
- 9.5. If Cognizant's performance of its obligations under this Agreement or any SOW is prevented, hindered or delayed by any act or omission of the Client, its Affiliates, agents, subcontractors, consultants or employees, as a result of the client failing to meet any Client responsibility as set out in the relevant SOW, or if any assumption contained in a SOW is untrue or incorrect or in respect of any consequences arising as a result of Cognizant or Cognizant's personnel following the instructions of any Client's personnel ("**Relief Event**"), Cognizant shall not be liable for any costs, charges, liabilities or losses sustained or incurred by the Client that arise directly or indirectly from such Relief Event and Cognizant shall be relieved of its obligations to provide the Services and Deliverables to the extent performance of such obligations is impeded. The Client acknowledges that such prevention or delay may result in additional Fees for the Services.
- 9.6. Each party shall mitigate its loss, including in relation to indemnities, and nothing in this Agreement or any SOW shall act to reduce or affect such duty to mitigate.

10. **TERMINATION**

- 10.1. Either party to this Agreement may terminate this Agreement or either party to a SOW may terminate that SOW (as applicable) with immediate effect by written notice to the other if the other party:
- (a) commits a material breach of this Agreement or the relevant SOW (as applicable) which has not been remedied within thirty (30) days of receipt of a written notice specifying both the material breach and the intention to terminate

this Agreement or the relevant SOW (as applicable) if the material breach is not remedied;

- (b) has appointed to it an administrator or administrative receiver; or
 - (c) being a partnership, in addition to the above, suffers bankruptcy orders being made against all of its partners.
- 10.2. Either party may suspend or terminate this Agreement or any SOW (as applicable) without liability for breach if, at any time, it reasonably believes that Services provided thereunder may violate applicable Trade Control Laws. Any and all claims for compensation, warranty, liability, penalty and damages against Cognizant due to delays, obstructions, restrictions of performance, or non-performance of Services and/or Deliverables resulting from any applicable Trade Control Laws, such as refusal, delay of granting or extension, amendment or lapse of import or export licenses, or any other governmental authorizations, embargoes and/or sanctions shall be excluded.
- 10.3. Either party to this Agreement may terminate this Agreement and either party to a SOW may terminate that SOW (as applicable) in accordance with clause 15.3.
- 10.4. Termination, expiry, or the occurrence of any event or circumstance which could give rise to termination of a SOW shall not of itself give rise to termination or the right to terminate any other SOW unless specifically stated in such other SOW. Unless otherwise specifically stated in a SOW, termination, expiry, or the occurrence of any event or circumstance which could give rise to termination of this Agreement shall not of itself give rise to termination or the right to terminate any SOW and, irrespective of termination or expiry of this Agreement, the terms and conditions of this Agreement shall continue to apply to and govern any such surviving SOW. Where this Agreement has been terminated no more SOWs may be entered into.
- 10.5. The rights of termination specified in this clause and elsewhere in this Agreement are intended to be exhaustive and in lieu of any other rights of termination howsoever arising, whether at common law or otherwise. Accordingly, the parties agree that no rights of termination of this Agreement or any SOW exist, save as expressly stated in this Agreement.
- 10.6. Upon termination of this Agreement and/or the respective SOW, Cognizant shall be entitled to recover payment for all Services rendered and expenses incurred through the date of termination (including for work in progress), and in the event of termination of this Agreement or any SOW by Cognizant (whether in whole or in part), pursuant to clause 10.1, Cognizant shall also be entitled to recover reasonable stranded costs to the extent they cannot reasonably be mitigated.

11. DATA PROTECTION

- 11.1. For the purposes of this clause 11 and Schedule 3, the terms “personal data”, “data processing”, “data controller” or “controller”, “data processor” or “processor”, “data subject” and “special categories of personal data” shall have the meaning given to them in the Data Protection Legislation. “Employee Personal Data” means the personal data of either Cognizant's personnel or the Client's personnel, as the context requires.
- 11.2. In connection with this Agreement or any SOW, either party may process personal data provided to it by the other and when it does so, the receiving party may be either a controller or a processor of such personal data, including in the following circumstances:
- (a) when the Client provides personal data, of which it is the controller, to Cognizant for Cognizant to process on its behalf as part of the provision of the

Services (and not for customer relationship, invoicing or Service preparation reasons), Cognizant shall process such personal data as a processor;

- (b) when Cognizant provides Employee Personal Data (either as a controller, or a processor acting on behalf of a controller) to the Client, including for the Client to process as part of evaluating such staff or to implement security measures at the Client site, the Client shall process such Employee Personal Data as a controller; and
- (c) when the Client provides Employee Personal Data, of which it is the controller, to Cognizant (including employee contact details) for customer relationship or invoicing reasons or in respect of preparation for the provision of the Services, Cognizant shall process such Employee Personal Data as a controller.

11.3. Each party shall comply with:

- (a) the obligations that apply to it under Data Protection Legislation; and
- (b) in circumstances where clause 11.2(a) applies, the Data Processing Terms set out in Schedule 3.

11.4. Where Employee Personal Data is processed in accordance with clause 11.2 (b) and/or (c), each party shall act as an independent controller in respect of such Employee Personal Data.

11.5. **Standard Contractual Clauses for Controllers.** In this Clause 11.5, the "Standard Contractual Clauses for Controllers" shall mean the standard contractual clauses (Module One: controller to controller) as approved by the European Commission Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries, including any applicable country-specific addendum(s). Where Employee Personal Data originating from the EEA, Switzerland or the UK is transferred by a disclosing party to a receiving party outside of the EEA, Switzerland or the UK (as applicable) on a controller to controller basis, and the receiving party is located in a country that has not been designated by the European Commission (or the relevant regulatory authority) as providing an adequate level of protection for personal data, the parties shall, where required by Data Protection Legislation, enter into the Standard Contractual Clauses for Controllers. For the purposes of the Standard Contractual Clauses for Controllers, the disclosing party shall be deemed the "Data Exporter" and the receiving party shall be deemed the "Data Importer". Where there is any conflict between the terms of this Agreement, any SOW and the Standard Contractual Clauses for Controllers, the Standard Contractual Clauses for Controllers shall prevail. Such Standard Contractual Clauses shall be amended to include the following mutatis mutandis: the liability of the data importer(s) to the data exporter(s) under the Standard Contractual Clauses (and any other related agreement executed pursuant to the Agreement, the SOW or these Clauses) shall be governed by the limitations and exclusions of liability applicable to Cognizant in this Agreement and accordingly, the liability of the data importer(s) and Cognizant taken together shall not exceed any applicable limitations in this Agreement.

12. EMPLOYEES

12.1. **No Employee Relationship.** Cognizant's and its agents' and subcontractors' employees are not and shall not be deemed to be employees of the Client. The performance of the Services by Cognizant under this Agreement will not constitute a transfer of employer authority over employees of Cognizant from Cognizant to the Client. The Client agrees that Cognizant retains all management responsibilities in respect of the employees of Cognizant and agrees to promptly refer all grievances, disciplinary, performance management or other personnel issues to Cognizant. Cognizant shall be solely responsible for the payment of all compensation to its employees including any employment-related taxes.

- 12.2. **Non-Solicitation Obligations.** During the term of this Agreement and any SOW and for a period of twelve (12) months thereafter, neither party shall, directly or indirectly for themselves or on behalf of anybody else, solicit for employment or engagement or employ, or accept services provided by, any current or former employee or independent contractor of the other party (including those of Cognizant Affiliates engaged in the provision of Services hereunder), who performed any work in connection with or related to the Services. This restriction does not apply to employment or engagement of an individual who responds of their own volition to general recruitment activities not specifically targeted at that individual.

13. **EMPLOYMENT REGULATIONS**

- 13.1. If, on the start of the provision of any part of the Services, any alleged claims or obligations arising from or related to the employment of any Client Employee or any contract of employment relating to a Client Employee or any collective agreement is or are alleged to have effect as if originally made against or concluded with Cognizant or any of its Affiliates or its or their subcontractors (a "Cognizant Entity") as a result of the provisions of the Employment Regulations, then the Client shall indemnify each Cognizant Entity and keep each Cognizant Entity indemnified against all losses, liabilities, damages, claims and expenses (including reasonable legal expenses) ("**Cognizant Employment Losses**") which any Cognizant Entity may incur in connection with or related to such allegations including Cognizant Employment Losses incurred in connection with the termination by a Cognizant Entity of the alleged employment of a Client Employee provided that Cognizant notifies the Client of such claim or alleged transfer within 5 Working Days of becoming aware of it and provided that such termination takes place as soon as reasonably practicable under the applicable law.
- 13.2. If, on the termination of any part of the Services, any alleged claims or obligations arising from or related to the employment of any individual employed by a Cognizant Entity (a "Cognizant Employee") or any contract of employment relating to a Cognizant Employee or any collective agreement is or are alleged to have effect as if originally made against or concluded with Client or any of its Affiliates (a "Client Entity") as a result of the provisions of the Employment Regulations, then Cognizant shall indemnify each Client Entity and keep each Client Entity indemnified against all losses, liabilities, damages, claims and expenses (including reasonable legal expenses) ("**Client Employment Losses**") which any Client Entity may incur in connection with or related to such allegations including Client Employment Losses incurred in connection with the termination by a Client Entity of the alleged employment of a Cognizant Employee provided that the Client notifies Cognizant of such claim or alleged transfer within 5 Working Days of becoming aware of it and provided that such termination takes place as soon as reasonably practicable under the applicable law.

14. **ANTI-SLAVERY**

- 14.1. In performing their obligations under this Agreement, the Client and Cognizant shall each:
- (a) comply with all the Anti-Slavery Laws; and
 - (b) have and maintain throughout the term of this Agreement their own policies and procedures to ensure their compliance with the Anti-Slavery Laws.
- 14.2. Each party confirms to the other that as at the date of this Agreement, in respect of their own officers and employees, no person has been convicted of any offence involving slavery or human trafficking.
- 14.3. Each party shall notify the other party as soon as it becomes aware of any actual slavery or human trafficking in its supply chain which is directly involved in the provision of the Services.

- 14.4. Each party shall respond promptly to all slavery and human trafficking due diligence questionnaires issued to it by the other party in relation to the Services from time to time and shall ensure that its responses to all such questionnaires are complete and accurate to the best of its knowledge.

15. **MISCELLANEOUS**

- 15.1. **Conduct of claims in respect of indemnity clauses.** No indemnity clause in this Agreement shall apply unless the indemnified party: (a) promptly notifies the indemnifying party of any claim or event (which may reasonably be considered as likely to give rise to a liability under an indemnity clause) made or occurring, or of which the indemnified party has knowledge; (b) gives the indemnifying party full opportunity to control the response to, defence and settlement of such claim, and provided further that the indemnified party shall not at any time admit liability or settle any such claim or action without the prior written consent of the indemnifying party; and (c) cooperates with the indemnifying party, at the indemnifying party's cost and expense in the defence or settlement of that claim. The indemnified party shall have the right to participate in the proceedings at its cost.
- 15.2. **Adequacy of Damages.** Each party acknowledges that money damages may be both incalculable and an insufficient remedy for any breach of clauses 6 (Intellectual Property Rights) and 7 (Confidentiality) of this Agreement and that any such breach by a party may cause the other party irreparable harm. Accordingly, each party also agrees that, in the event of any such breach or anticipated breach, the other party, in addition to any other remedies at law or in equity it may have, shall be entitled, without the requirement of posting a bond or other security, to seek equitable relief, including injunctive relief and specific performance from any court of competent jurisdiction.
- 15.3. **Force Majeure.** If either party is delayed or prevented from complying with its obligations under this Agreement or any SOW by a Force Majeure Event, then such party shall not be in breach of this Agreement or the affected SOW (as applicable) nor liable for any failure or delay in performance of any of its obligations. If the Force Majeure Event continues for more than two months, either party may terminate any SOW affected by the Force Majeure Event by giving 30 days' written notice to the other party. In the event that Services may be disrupted by a Force Majeure Event with respect to which working from remote locations is deemed by Cognizant to be the optimal business continuity measure then, if the assets on hand and capabilities exist for Cognizant personnel to perform the Services from remote locations, including from personal residences ("**Remote Locations**"), and to the extent it is not already performing the Services from the Remote Locations, Cognizant shall have the right to perform the Services from the Remote Locations using networking, connectivity, security and data handler protocols established by Cognizant and provided to Client (the "**Remote Protocols**") and the Remote Protocols shall supersede any and all terms of this Agreement and all schedules, exhibits or attachments hereto and thereto that require any different measures. Notwithstanding any other provision of this Agreement, Cognizant shall have no responsibility or liability hereunder for any security or data loss incident arising in connection with Cognizant providing Services from Remote Locations except to the extent such incident is caused by Cognizant's failure to implement the Remote Protocols, which such liability shall be subject to the liability cap in clause 9.
- 15.4. **Notices.**
- (a) Notices required to be given pursuant to clauses 5.3, 7.3, 8.4, 10, **Error! Reference source not found.**, 15.1 or 15.6, or which invoke or relate to any actual or potential dispute or any allegation of a breach of contract or commission of a tort ("**Formal Notices**") shall be given in writing to the other party and delivered by registered mail, or international air courier. Notices will be effective when received as indicated on the facsimile, registered mail, or

other delivery receipt. All Formal Notices shall be given by one party to the other at its address stated on the first page of this Agreement unless a change thereof previously has been given to the party giving the notice, and any Formal Notices to Cognizant shall be addressed for the attention of Cognizant's General Counsel.

- (b) All notices which are required to be given by this Agreement or a SOW which are not Formal Notices shall be sent to the person and address designated by the receiving party and the provisions of clause 15.4(a) shall otherwise apply, except that they may instead be given by email if an email address has been designated for such purposes. If so, they shall be deemed effective when sent unless the sender receives an automated response notifying him of problems in the delivery of the message or that the recipient is not in regular receipt of emails.

15.5. **Amendments.** No variation of this Agreement, any SOW or any of the documents referred to in it shall be valid unless it is in writing and signed by or on behalf of each of the parties: (a) to this Agreement (in respect of changes to this Agreement); and (b) to the relevant SOW (in respect of changes to that SOW).

15.6. **Waivers.** No reasonable delay by either party to exercise any right or remedy arising under, or in connection with, this Agreement or any SOW (collectively, any "action") shall act as a waiver, or otherwise prejudice or restrict the rights of that party, in relation to that action or any other contemporaneous or future action.

15.7. **Severability.** If any provision (or part thereof) of this Agreement or a SOW is determined to be partially void, illegal, invalid or unenforceable in any respect by any court or body of competent jurisdiction or by virtue of any legislation to which it is subject, or by virtue of any other reason whatsoever, it shall be void or unenforceable to that extent only, and the legality, validity and enforceability of any of the other provisions or the remainder of any such provision shall not to be affected or impaired. If any illegal, invalid or unenforceable provision would be legal, valid or enforceable if some part of it were deleted, such provision shall apply with the minimum modification(s) necessary to make it legal, valid or enforceable.

15.8. **Counterparts.** This Agreement and each SOW may be executed in several counterparts and by remote signature, and by the parties on separate counterparts, but shall not be effective until each party has executed at least one counterpart. Each counterpart shall be deemed an original of this Agreement or a SOW (as the case may be), and all of which taken together shall constitute one and the same agreement.

15.9. **Entire Agreement.** Subject to clause 9.2:

- (a) this Agreement and each SOW does and will constitute the entire agreement and understanding between the parties in respect of its subject matter and supersede, cancel and nullify any previous agreements, Statements and all other prior or contemporaneous communications between the parties or given by or on behalf of the parties and relating to its subject matter;
- (b) except as expressly set out in this Agreement or a SOW, neither party makes or gives (and each party hereby excludes to the maximum extent permitted by law) any Statement or condition of any kind, whether statutory, express or implied, including any implied warranty of merchantability, satisfactory quality, fitness for a particular purpose or any representation, warranty or condition from course of dealing or usage of trade;
- (c) each party acknowledges that it has not, and will not have, relied on or been induced to enter into this Agreement or any SOW by, and shall have no remedy (whether in equity, contract, tort under the Misrepresentation Act 1967 or otherwise) in respect of, any Statement (whether made negligently or

innocently by either of them or any other third party, save for fraud or fraudulent misrepresentation) unless that Statement is expressly set out in this Agreement or a SOW;

- (d) neither party shall be entitled to (and waives any right to) claim the remedies of rescission or damages for misrepresentation arising out of, or in connection with, any Statement whether made by either of them or any other third party and whether or not it is set out in this Agreement or a SOW.

- 15.10. **Assignment.** Neither Party may assign or otherwise transfer any of its rights, duties or obligations under the Agreement without the prior written consent of the other Party, except Cognizant may, upon prior written notice to the Client (but without any obligation to obtain consent), assign the Agreement or any of its rights hereunder to any of its Affiliates if such entity agrees in writing to assume and be bound by all of the obligations of Cognizant under the Agreement.
- 15.11. **Publicity.** Cognizant may in its general promotional material (a) identify the Client as a client of Cognizant, save that it does not disclose any Confidential Information regarding the relationship between the parties, including the terms of this Agreement or any SOW, without the prior consent of the Client; and (b) use the Client's logo in such materials provided its use conforms with any guidelines issued by the Client to Cognizant from time to time. The Client agrees to provide a reference for Cognizant from time to time.
- 15.12. **Consents and Approvals.** Except where expressly provided as being in the discretion of a party, where approval, acceptance, consent or similar action by either party is required under this Agreement or the applicable SOW, it shall not be unreasonably withheld or delayed, and each party shall make only reasonable requests under this Agreement or any SOW.
- 15.13. **Contracts (Rights of Third Parties) Act 1999.** A person who is not a party to this Agreement or a SOW shall have no right to enforce any terms of this Agreement or that SOW, including under the Contracts (Rights of Third Parties) Act 1999.
- 15.14. **Relationship of the parties.** Nothing in this Agreement or any SOW is intended to create or shall be deemed to constitute a partnership, a joint venture or legal relationship of any kind between the parties that would impose liability upon one party for an act (or failure to act) of the other party, or to authorise either party to act as agent for the other. Except where otherwise expressly provided in this Agreement, neither party shall have authority to make representations, act in the name or on behalf of, or otherwise to bind the other. Each party shall act reasonably in the performance of this Agreement and each SOW.
- 15.15. **Further assurance.** Each party shall, at the reasonable request and the cost of the other, do, execute, perform or procure to be done, executed or performed, all such further acts, deeds, documents and things as may from time to time be necessary to give full effect to this Agreement or a SOW.
- 15.16. **Survival.** Termination or expiry of this Agreement or any SOW, however caused, shall be without prejudice to any obligations or rights of either of the parties which may have accrued before termination or expiry and shall not affect any provision of this Agreement which is expressly or by implication intended to come into effect on, or to continue in effect after, such termination or expiry (including clauses 5, 6, 7, 8, 9, 11, 12.2, **Error! Reference source not found.** and 15).
- 15.17. **Bargain.** The disclaimers, exclusions and limitations of liability set forth in this Agreement form an essential basis of the bargain between the Parties, and, absent any of such disclaimers, exclusions or limitations of liability, the provisions of this Agreement, including, without limitation, the economic terms, would be substantially different.

15.18. Dispute Resolution.

- (a) **Informal Negotiations.** In the event of any Dispute, prior to filing a notice of a claim, the party claiming a Dispute shall send a written notice to the other party describing the basis for the Dispute and the requested remedy, and inviting the other party to have its executive confer with a named executive of the claiming party to attempt to negotiate a resolution. The claiming party may file the notice of the claim in accordance with clause 15.18(b), after the executive conference is completed, if the invitation to confer is declined, or if, within ten (10) business days after the Dispute notice is delivered, there is no response to the invitation or the parties are unable to schedule the conference.
- (b) **Arbitration:** Any and all Disputes shall be settled through the negotiation process set out in clause 15.18(a) and, if not resolved through such process, by final and binding arbitration administered in accordance with the provisions of this clause 15.18(b): (1) the arbitration shall be governed by the provisions of the Arbitration Act 1996 and the London Court of International Arbitration ("LCIA") procedural rules shall be applied and are deemed to be incorporated into this Agreement (save that in the event of any conflict between those rules and this Agreement, this Agreement shall prevail); (2) the decision of the arbitrator shall be binding on the parties (in the absence of any material failure by the arbitrator to comply with the LCIA procedural rules); and (3) the tribunal shall consist of three arbitrators to be agreed by the parties and in the event that the parties fail to agree the appointment of the arbitrators within ten (10) Working Days or, if the person(s) appointed is unable or unwilling to act, as appointed by the LCIA; and (4) the arbitration proceedings shall take place in London.

15.19. Governing Law. This Agreement, each SOW and any dispute or non-contractual obligation arising out of or in connection with them shall be governed by and construed in accordance with the laws of England and, subject to clauses 15.2 and 15.177, the parties submit to the exclusive jurisdiction of the courts of England.

SIGNED

[Insert Client Name]

COGNIZANT WORLDWIDE LIMITED

Signature: _____

Signature: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

SCHEDULE 1 - CHANGE CONTROL PROCEDURE

1. Where the Client or Cognizant sees a need for a Change to the Services it may propose a Change only in accordance with the Change Control Procedure as set out in this Schedule 1 or in the applicable SOW.
2. Any discussions which may take place between the Client and Cognizant in connection with a request or recommendation before the authorisation of a resultant Change shall be without prejudice to the rights of either party.
3. Where either party wishes to propose any Change to this Agreement or any SOW, it will notify the other party of that fact by sending a written change request ("**Change Request**") to the other party's appropriately appointed representative, specifying in as much detail as is reasonably practicable the nature of the Change.
4. As soon as reasonably practical, Cognizant will provide the Client with a written proposal in relation to the relevant Change (a "**Change Control Proposal**") containing the following information:
 - 4.1 impact of the Change on the Services including any changes to specifications or other variations to the Agreement or the SOW;
 - 4.2 applicable charges for the implementation and on-going operation of the relevant Change, including any alteration of the Fees or additional Fees relating to the proposed Change;
 - 4.3 an estimated timetable for the implementation of the Change Request.
5. When information has been provided under paragraph 4, the Client shall evaluate the Change Control Proposal and respond to Cognizant as soon as reasonably practicable and in any event no later than five (5) Working Days (or a longer period agreed by the parties) after its receipt by the Client.
6. If the Client agrees to the Change Control Proposal, the parties shall endeavour to agree the terms of the Change Order which shall be set out in the format set out in the Appendix to this Schedule 1.
7. A Change Order signed by both parties shall constitute an amendment to the Services pursuant to clause 3.4.

Appendix - Change Order Form

<u>Change Order</u>
<u>Title of Change:</u>
<u>Originator:</u>
<u>Date:</u>
<u>Reason for Change:</u>
<u>Description (giving details, including any specifications):</u>
<u>Deliverables:</u>
<u>Acceptance Testing and Criteria:</u>
<u>The Fees (if any):</u>
<u>Estimated Timetable:</u>
<u>Likely Impact on the Agreement or the SOW:</u>
<u>Signed for and on behalf of the Client:</u>
<u>Signed for and on behalf of Cognizant:</u>

SCHEDULE 2 - DATA SECURITY POLICY

Taking into account the available technology, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk to data subjects' rights, Cognizant has agreed to implement the following technical and organisational measures in respect of the Personal Data, designed to provide a level of security appropriate to the risk.

1. **Definitions.** Capitalized terms used in this Schedule have the following meanings:

1.1 Personal Data means personal data (as defined under applicable data protection law) processed by Cognizant on behalf of Client pursuant to this Agreement.

1.2 Client Systems means information systems and resources supplied or operated by Client or its other service providers, including network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity.

1.3 Cognizant Infrastructure means information processing resources supplied or operated by Cognizant, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications, internet connectivity, printers and hard drives that are used, either directly or indirectly, in support of Cognizant Processing.

1.4 Cognizant Processing means any information collection, storage or processing (as defined by applicable data protection law) performed by Cognizant or its approved subcontractors: (a) that directly or indirectly supports the Services now or hereafter furnished to Client under the Agreement, and (b) using any Personal Information.

1.5 Security Incident means (i) any act or omission that compromises the security, confidentiality, privacy, availability, or integrity of Personal Data; (ii) the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Personal Data or interference with system operations that contain Personal Data; (iii) 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. Provided, however, that the definition of Security Incident shall not include those non-material attempts.

2. **Information Security Management Programme and Policies.**

2.1 Policies and Procedures. Cognizant shall maintain written security management policies and procedures designed with the intent to prevent, detect, contain, and correct breaches of measures taken to protect the confidentiality, integrity, availability, or security of Personal Data. These policies and procedures shall: (a) assign specific data security responsibilities and accountabilities to specific individual(s); and (b) include a risk management programme that includes periodic risk assessments.

2.2 Infrastructure Protection. To the extent applicable to the provision of the services provided to Client, Cognizant shall maintain policies and procedures to protect Cognizant Infrastructure, including: (a) security programmes (policies, standards, processes, etc.); (b) processes for becoming aware of, and maintaining, security patches and fixes; (c) procedures for employing mechanisms to restrict access to the Cognizant Infrastructure, including all local-site networks that may be accessed via the internet (whether or not such sites transmit information); (d) procedures designed to protect the Cognizant Infrastructure against attack and penetration; and (e) processes designed to prevent, detect, and eradicate viruses.

3. **Access Control.**

3.1 Identification and Authentication. Access to Personal Data or any Cognizant Infrastructure shall be Identified and Authenticated as defined in this clause. "Identification" or "Identified" refers to processes that establish the identity of the person requesting access

to the Personal Data and/or Cognizant Infrastructure. “Authentication” refers to processes that validate the purported identity of the requestor. For access to Personal Data or Cognizant Infrastructure, Cognizant shall require Authentication by the use of an individual, unique user ID and an individual password or other appropriate Authentication technique. Cognizant shall maintain procedures designed for the protection, integrity, and soundness of any passwords created by Cognizant and/or used by Cognizant in connection with the performance of the services to Client.

3.2 Account Administration. Cognizant shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Cognizant Infrastructure and Personal Data, and shall include procedures for granting and revoking emergency access to Cognizant Infrastructure.

3.3 Access Control. Cognizant shall maintain appropriate access control mechanisms designed with the intent to prevent access to Personal Data and/or Cognizant Infrastructure, except by authorized users. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. Cognizant shall maintain appropriate mechanisms and processes designed to detect, record, analyse, and resolve unauthorized attempts to access Personal Data or Cognizant Infrastructure.

4. Personnel Security.

4.1 Access to Personal Data. Cognizant shall require its personnel and its approved sub-processors’ personnel who have, or may be expected to have, access to Personal Data or Client Systems to comply with the provisions of this Schedule. Cognizant shall remain responsible for any breach of this Schedule by its personnel or the personnel of its approved sub-processors.

4.2 Security Awareness. Cognizant shall require that its employees and approved sub-processors remain aware of Cognizant’s security practices, and their responsibilities for protecting Personal Data. This shall include: (a) protection against viruses; (b) appropriate password protection and password management practices; and (c) appropriate use of workstations and computer system accounts.

5. Risk Management.

5.1 General Requirements. Cognizant shall maintain appropriate safeguards and controls and exercise due diligence designed to protect Personal Data and Cognizant Infrastructure against unauthorized access, use, and/or disclosure, considering: (a) the applicable data protection law; (b) information technology and industry practices; (c) the type of Personal Data; and (d) the relative level and severity of risk of harm should the integrity, confidentiality, availability or security of Personal Data be compromised, as determined by Cognizant as part of an overall risk management programme.

5.2 Security Evaluations. Cognizant shall periodically evaluate its processes and systems for compliance with obligations imposed by applicable data protection law or contract with respect to the confidentiality, integrity, availability, and security of Personal Data and Cognizant Infrastructure. Cognizant shall document the results of these evaluations and any remediation activities taken in response to these evaluations.

5.3 Internal Records. Cognizant shall maintain and implement policies and programmes to capture, record, and examine information relevant to Security Incidents and other security-related events. In response to such events, Cognizant shall take appropriate action to address and remediate identified vulnerabilities to Personal Data and Cognizant Infrastructure.

6. Physical Security. Cognizant shall maintain appropriate physical security controls (including facility and environmental controls) designed to prevent unauthorized physical access to Cognizant Infrastructure and areas in which Personal Data are stored or processed. Cognizant shall adopt and implement a written facility security plan that documents these

controls and the policies and procedures through which these controls will be maintained. Cognizant shall maintain appropriate records of maintenance performed on Cognizant Infrastructure and on the physical control mechanisms used to secure Cognizant Infrastructure.

7. Communications Security.

7.1 Encryption. Where applicable, Cognizant shall maintain encryption, in accordance with standards mutually agreed upon between the parties, for all transmission of Personal Data via public networks.

7.2 Protection of Storage Media. Cognizant shall delete Personal Data from all storage media prior to disposal or re-use. All media on which Personal Data is stored shall be protected against unauthorized access or modification. Cognizant shall maintain reasonable and appropriate processes and mechanisms designed to maintain accountability and tracking of the receipt, removal and transfer of storage media used for Cognizant Processing or on which Personal Data has been stored.

7.3 Data Integrity. Cognizant shall maintain processes designed to prevent unauthorized or inappropriate modification of Personal Data that is processed by Cognizant.

8. Remote Access to Client Systems. Cognizant's remote access to Client Systems shall be limited to the extent minimally necessary to provide the services to Client.

9. Security Incident Monitoring and Response. Cognizant shall maintain processes designed to detect, identify, report, respond to, and resolve Security Incidents in a timely manner, and will have processes and procedures in place to notify Client as required by applicable data protection law or as agreed otherwise between Cognizant and Client.

10. Business Continuity Management. Cognizant shall have a plan in place designed to counteract interruptions to business activities and protect critical business processes from the effects of major failures of information systems or disasters. Such plans shall be designed to restore business operations in a timely manner.

SCHEDULE 3 - DATA PROCESSING TERMS

These Data Processing Terms shall apply only to the extent that: (i) Cognizant or a Cognizant Affiliate established in EEA, Switzerland or the UK processes personal data on behalf of Client or a Client Affiliate; (ii) Cognizant or a Cognizant Affiliate processes Personal Data on behalf of a Client or Client Affiliate that is established in the EEA, Switzerland or the UK; or (iii) Cognizant processes personal data of data subjects located in the EEA, Switzerland or the UK on behalf of the Client or a Client Affiliate.

1. Data Protection

- 1.1 Relationship of the parties:** The Client (the controller) appoints Cognizant as a processor to process the personal data described in part 3 of Schedule 5 and Annex A of each SOW (the "In-Scope Personal Data").
- 1.2 Prohibited data:** The Client shall not disclose (and shall not permit any data subject to disclose) any: (i) special categories of In-Scope Personal Data; or (ii) In-Scope Personal Data in relation to criminal convictions and offences, to Cognizant for processing that are not expressly disclosed in part 3 of Schedule 5 or Annex A of a SOW.
- 1.3 Purpose limitation:** Cognizant shall process the In-Scope Personal Data as a processor for the purposes described in part 3 of Schedule 5 or Annex A of each SOW and only in accordance with the lawful documented instructions of the Client (the "Permitted Purpose"), except where otherwise required by any law applicable to Cognizant. The Agreement and each SOW sets out Client's complete instructions to Cognizant in relation to the processing of Personal Data. Any processing required outside of the scope of these instructions will require prior agreement between the parties, including agreement on any additional fees that Client shall pay. Client agrees that any necessary changes to its data processing instructions shall be by way of written notification to Cognizant.
- 1.4 International transfers:** If and to the extent that In-Scope Personal Data originating from the EEA, Switzerland or the UK will be transferred or otherwise processed by Cognizant outside of the EEA, Switzerland or the UK (as applicable) in a country that has not been designated by the European Commission (or the relevant regulatory authority) as providing an adequate level of protection for personal data, Cognizant and Client shall ensure an adequate level of protection by any of the recognized methods in Data Protection Legislation, including but not limited to entry into the standard contractual clauses (Module Two: controller to processor) as approved by the European Commission Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries, including any applicable country-specific addendum(s), as set out in Schedule 6 (the "Standard Contractual Clauses (controller to processor)"). Client authorizes any transfers of In-Scope Personal Data to, or access to In-Scope Personal Data from such destinations outside the EEA, Switzerland and the UK, as applicable subject to any of these adequacy measures having been taken.
- 1.5 Confidentiality of processing:** Cognizant shall ensure that any person that it authorises to process the In-Scope Personal Data (including Cognizant's and Cognizant Affiliates' staff, agents and subcontractors) (an "Authorised Person") shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty or otherwise). Cognizant

shall ensure that all Authorised Persons process the In-Scope Personal Data only as necessary for the Permitted Purpose.

- 1.6 **Security:** Cognizant shall implement appropriate technical and organisational measures designed to protect the In-Scope Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access (each a "Security Incident") as set out in Schedule 2.
- 1.7 **Subprocessing:** Client agrees that Cognizant may engage the following types of subprocessors:
- (a) Cognizant Affiliates; and
 - (b) third party subprocessors authorized by Client (subject to paragraphs 1.9 and 1.10);

to fulfil Cognizant's contractual obligations under the Agreement (including pursuant to any SOW) and to provide services to Client on Cognizant's behalf. The third party subprocessors (excluding Cognizant Affiliates) authorized by Client on the Effective Date of the Agreement, if any, are listed at Part 1 of Schedule 5 and additional third party subprocessors (excluding Cognizant Affiliates) authorized by the Client, will be listed in Annex B Part 1 of the applicable SOW (together "Cognizant Subprocessors"). Cognizant shall, subject to paragraphs 1.9 and 1.10 of this Schedule 3, impose data protection terms on any Cognizant Subprocessor it appoints that protect the In-Scope Personal Data to the same standard provided for by this Schedule 3 and remain fully liable for any breach of this Schedule 3 that is caused by an act, error or omission of a Cognizant Subprocessor. For the avoidance of doubt, any Cognizant Subprocessor listed in Part 1 of Schedule 5 of the Agreement may be appointed for any SOW and any Cognizant Subprocessor listed in Annex B Part 1 of a SOW will be appointed for that SOW only.

- 1.8 **Changes to Subprocessors:** Cognizant may, by giving reasonable notice to the Client, add or make changes to the Cognizant Subprocessors. If the Client objects to Cognizant's appointment of an additional Cognizant Subprocessor within five (5) calendar days of such notice on reasonable grounds relating to the protection of the In-Scope Personal Data, then Cognizant will not appoint the additional Cognizant Subprocessor and will work with the Client to find an alternative.
- 1.9 **Special Subprocessor arrangements:** The Client acknowledges that Cognizant has engaged or will engage the Cognizant Subprocessors listed at Part 2 of Schedule 5 or Annex B Part 2 of any SOW ("Special Subprocessors") on terms and conditions that may not reflect some or all of the requirements set out in this Schedule 3, or the Standard Contractual Clauses (controller to processor), where applicable. The Client further acknowledges that it has had or will have the opportunity to review the terms and conditions Cognizant has entered or will enter with these Special Subprocessors, in order to assess the nature of the processing they will conduct, the standard of data protection they will provide, and the liability they will accept for any breaches of data protection compliance. Having conducted this assessment, the Client consents to Cognizant's use of these Special Subprocessors and agrees that the extent of Cognizant's liability to the Client for any breach of this Schedule 3, the Agreement or the Standard Contractual Clauses (controller to processor) that is caused by any of the Special Subprocessors shall (notwithstanding paragraph 1.7) be limited strictly to the extent of the liability which Cognizant is able to recover from that Special Subprocessor under its terms and conditions.

- 1.10 Changes to Special Subprocessors: Cognizant may, by giving reasonable notice to the Client, add or make changes to the Special Subprocessors. In such cases, Cognizant shall give the Client an opportunity to review the terms and conditions that Cognizant has entered or will enter into with these Special Subprocessors. If the Client objects to Cognizant's appointment of an additional Special Subprocessor within five (5) calendar days of such notice, then Cognizant will not appoint the additional Special Subprocessor and will work with the Client to find an alternative. Where an additional Special Subprocessor is engaged pursuant to this paragraph, then the extent of Cognizant's liability in respect of such Special Subprocessor will be the same as that set out in paragraph 1.9 above.
- 1.11 Cooperation and data subjects' rights: Cognizant shall provide reasonable assistance (including by appropriate technical and organisational measures in so far as is possible) to the Client (at Client's expense) to enable the Client to respond to any request from a data subject to exercise any of its rights under Data Protection Legislation (including its rights of access, correction, objection, erasure and data portability, as applicable). In the event that any such request is made directly to Cognizant, Cognizant shall promptly inform the Client providing full details of the same.
- 1.12 Data Protection Impact Assessment: Cognizant shall, upon written request from the Client and at the Client's expense, provide the Client with reasonable assistance, to the extent necessary to facilitate the Client's compliance with data protection impact assessment and prior consultation requirements under Data Protection Legislation.
- 1.13 Security incidents: Upon becoming aware of a Security Incident, Cognizant shall inform the Client without undue delay and shall provide timely information as the Client may reasonably require including in order for the Client to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Data Protection Legislation.
- 1.14 Deletion or return of Data: Upon termination or expiry of the Agreement or any SOW, Cognizant shall (at the Client's election) destroy or return to the Client all relevant In-Scope Personal Data (including all copies of the In-Scope Personal Data) in its possession or control. This requirement shall not apply to the extent that Cognizant is required by any applicable law to retain some or all of the In-Scope Personal Data.
- 1.15 Security Reports & Audits:

Cognizant agrees to provide, upon Client's reasonable request, copies of relevant external security certifications, audit report summaries of audits performed by Cognizant to verify Cognizant's compliance with its security obligations under this Agreement and/or any other relevant documentation relating to the Services necessary to verify Cognizant's compliance with this Schedule 3. While it is the parties' intention ordinarily to rely on the provision of such documentation to verify Cognizant's compliance with this Schedule 3, Cognizant shall permit the Client (or its appointed third party auditors) to audit Cognizant's processing of the Personal Data under this Agreement following a Security Incident suffered by Cognizant or when instructed by a competent data protection authority. Except for audits instructed by a competent data protection authority, for which Client will give Cognizant as much notice as reasonably possible, Client must give Cognizant 45 days' notice of its intention to audit with finalized audit scope and evidence request list provided no less than 20 days in advance of a site visit.

Client agrees to conduct its audit during normal business hours, take all reasonable measures to prevent unnecessary disruption to Cognizant's operations, and such audit shall not exceed a period of 40 hours. Any such audit shall be subject to the following limitations: (i) use of any third party auditor shall be subject to Cognizant's prior written approval, such approval not to be unreasonably withheld or delayed; and (ii) Client or any auditor conducting any such audit shall at all times comply with any and all reasonable security and confidentiality guidelines and other policies of Cognizant with respect to the audit.

1.16 Compliance: The Client shall be responsible for ensuring:

- (a) it has complied, and will continue to comply, with Data Protection Legislation;
- (b) all In-Scope Personal Data has been, and will continue to be, collected and processed in accordance with notice, consent and other requirements of the Data Protection Legislation (and, where applicable, the collection and processing has been notified to the relevant authorities);
- (c) it has, and will continue to have, the right to transfer, or provide access to, the In-Scope Personal Data to Cognizant and its subprocessors, for processing for the Permitted Purposes and such processing by Cognizant will not breach Data Protection Legislation; and
- (d) its instructions to Cognizant, in respect of the processing of the Personal Data, are lawful and will not create legal or regulatory liability on the part of Cognizant if followed.

SCHEDULE 4 - STATEMENT OF WORK PRO FORMA

THIS STATEMENT OF WORK (SOW) is made on _____
20__

BETWEEN

- (1) **[Insert Client Name]** a company incorporated and registered in England and Wales (company number []) which has its registered office at [] ("**Client**"); and
- (2) **COGNIZANT WORLDWIDE LIMITED** a company incorporated and registered in England and Wales (company number 07195160) which has its registered office at 280 Bishopsgate, London EC2M 4AG ("**Cognizant**"),

pursuant to the terms of the Master Services Agreement entered into between [*insert client MSA party details*] and Cognizant Worldwide Limited ("Agreement"), which are hereby incorporated into this SOW. For good and valuable consideration (the adequacy and receipt of which are hereby acknowledged by the parties) the parties to this SOW agree as follows.

1. DEFINITIONS

Unless otherwise set out herein, defined terms shall have the meaning ascribed to them in the Agreement.

2. SOW TERM

This SOW shall commence on [insert date] and shall continue for a period of [insert period] unless and until terminated earlier in accordance with the terms of the Agreement.

3. SERVICES DESCRIPTION

4. FEES / CHARGING MECHANISM

5. ACCEPTANCE

6. CLIENT RESPONSIBILITIES

7. ASSUMPTIONS

Annex A: Data Processing Description

This Annex A forms part of the SOW and describes the processing that Cognizant will perform on behalf of the Client in order to provide the Services.

Client: Controller

Please document the Client's activities (as a controller) relevant to the processing:

Cognizant: Processor – documented instructions

Please document Cognizant's processing activities relevant to the Services. The personal data will be subject to the following processing activities:

Duration of Processing

Please document the duration of the processing activities:

Categories of data subjects

The personal data to be processed concern the following categories of data subjects (please specify):

Types of data

The personal data to be processed concern the following types of data (please specify):

Special categories of data (if appropriate)

The personal data to be processed concern the following special categories of data (please specify):

Annex B: Cognizant Third Party Subprocessors

This Annex B forms part of the SOW and describes the Cognizant Subprocessors and Special Subprocessors used in connection with the Services.

PART 1: Third party subprocessors

PART 2: Special Subprocessors

Special Subprocessor	Processing to be provided	Link to terms and conditions (where available)

SCHEDULE 5 – FRAMEWORK-LEVEL DATA PROCESSING DESCRIPTION AND COGNIZANT THIRD PARTY SUBPROCESSORS

PART 1: Third party subprocessors

PART 2: Special Subprocessors

Special Subprocessor	Processing to be provided	Link to terms and conditions (where available)

PART 3: Data Processing Description

This Part 3 describes the processing that Cognizant will perform on behalf of the Client in order to provide the Services. Where the data processing activities are not known on the Effective Date, this schedule will be intentionally left blank and the processing that Cognizant will perform on behalf of the Client will be set out in Annex A of each applicable SOW.

Client: Controller

Please document the Client's activities (as a controller) relevant to the processing:

Cognizant: Processor – documented instructions

Please document Cognizant's processing activities relevant to the Services. The personal data will be subject to the following processing activities:

Duration of Processing

Please document the duration of the processing activities:

Categories of data subjects

The personal data to be processed concern the following categories of data subjects (please specify):

Types of data

The personal data to be processed concern the following types of data (please specify):

Special categories of data (if appropriate)

The personal data to be processed concern the following special categories of data (please specify):

SCHEDULE 6 - STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES

Module 2: controller - processor

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”) have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9 - Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 - Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 - Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

These Clauses are entered into pursuant to the [Master Services Agreement] [add full name] made between [add full name of parties] on [add date], as amended from time to time, (the “MSA”) and the associated [Statement of Work] dated [add date] ((the “SOW”) for [add name of SOW/description of services]. The liability of the data importer(s) to the data exporter(s) under these Clauses (and any other related agreement executed pursuant to the MSA, the SOW or these Clauses) shall be governed by the limitations and exclusions of liability applicable to [Cognizant contracting party to MSA] under the MSA and accordingly, the liability of the data importer(s) and [Cognizant contracting party to MSA] taken together shall not exceed any applicable limitations in the MSA. The foregoing shall not be taken to limit or exclude the data importer’s liability to any data subject under these Clauses.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On

request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer

shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) **OPTION 1: SPECIFIC PRIOR AUTHORISATION** The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the subprocessor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date. [*Drafting note: It is suggested that the time period in clause 9(a)/(b) aligns with the time period for notification of a new subprocessor in the MSA*]

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including

personal data, the data importer may redact the text of the agreement prior to sharing a copy.

- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.

- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- (ii) the data importer is in substantial or persistent breach of these Clauses; or
- (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of _____ (*specify Member State*).
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

[Drafting note: include language in square brackets below to incorporate the UK amendment to the SCCs. UK amendments are set out in Annex IV]

["By signing we agree to be bound by the Standard Contractual Clauses as amended by the UK Addendum to the EU Commission Standard Contractual Clauses dated: [INSERT/the date of signature]" *[and add the date (where all transfers are under the UK Addendum)]*]

[OR]

["By signing we agree to be bound by the Standard Contractual Clauses and the Standard Contractual Clauses as amended by the UK Addendum to the EU Commission Standard Contractual Clauses dated" *[and add the date (where there are transfers both under the Clauses and under the Addendum)]*]

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.....

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

.....

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

.....

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

.....

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III – LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: ...
 Address: ...
 Contact person's name, position and contact details: ...
 Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...
2. ...

ANNEX IV – UK ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

UK Addendum to the EU SCCs

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 Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	[To be added]	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: [insert] Trading name (if different): NA Main address (if a company registered address): [insert] Official registration number (if any) (company number or similar identifier): [insert]	Full legal name: Cognizant Technology Solutions India Pvt Ltd. Trading name (if different): NA Main address (if a company registered address): 5/535, Old Mahabalipuram Rd, Thoraipakkam, Tamil Nadu 600096 Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): <input type="text"/> Job Title: [insert] Contact details including email: [insert]	Full Name (optional): <input type="text"/> Job Title: Chief Privacy and Data Ethics Officer Contact details including email: dataprotectionofficer@cognizant.com

Signature (if required for the purposes of Section 2)	See Appendix of the controller-processor SCCs (Module 2)	See Appendix of the controller-processor SCCs (Module 2)
--	--	--

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<p>✓ <input type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: [To be added]</p> <p>Reference (if any): This Addendum is appended to the controller-processor SCCs (Module 2) between the parties described in Table 1 above.</p> <p>Other identifier (if any):</p>
-------------------------	---

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: As set out in the Appendix of the controller-processor SCCs (Module 2)

Annex 1B: Description of Transfer: As set out in the Appendix of the controller-processor SCCs (Module 2)

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in the Appendix of the controller-processor SCCs (Module 2)

Annex III: List of Sub processors (Modules 2 and 3 only): As set out in the Appendix of the controller-processor SCCs (Module 2)

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum	Which Parties may end this Addendum as set out in Section 19:
-----------------------------	---

when the Approved Addendum changes	<input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter
---	--

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
 - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
 - c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK.

The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
 - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
 - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
 - a its direct costs of performing its obligations under the Addendum; and/or
 - b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.



About Cognizant

Cognizant (Nasdaq-100: CTSI) engineers modern businesses. We help our clients modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast changing world. Together, we're improving everyday life. See how at www.cognizant.com or @Cognizant.

UK Headquarters

Cognizant Worldwide Limited

280 Bishopsgate,
London EC2M 4AG England
+44 (0)20 7297 7600

Contact: inquiryPSandHealth@cognizant.com

© Copyright 2024, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.

