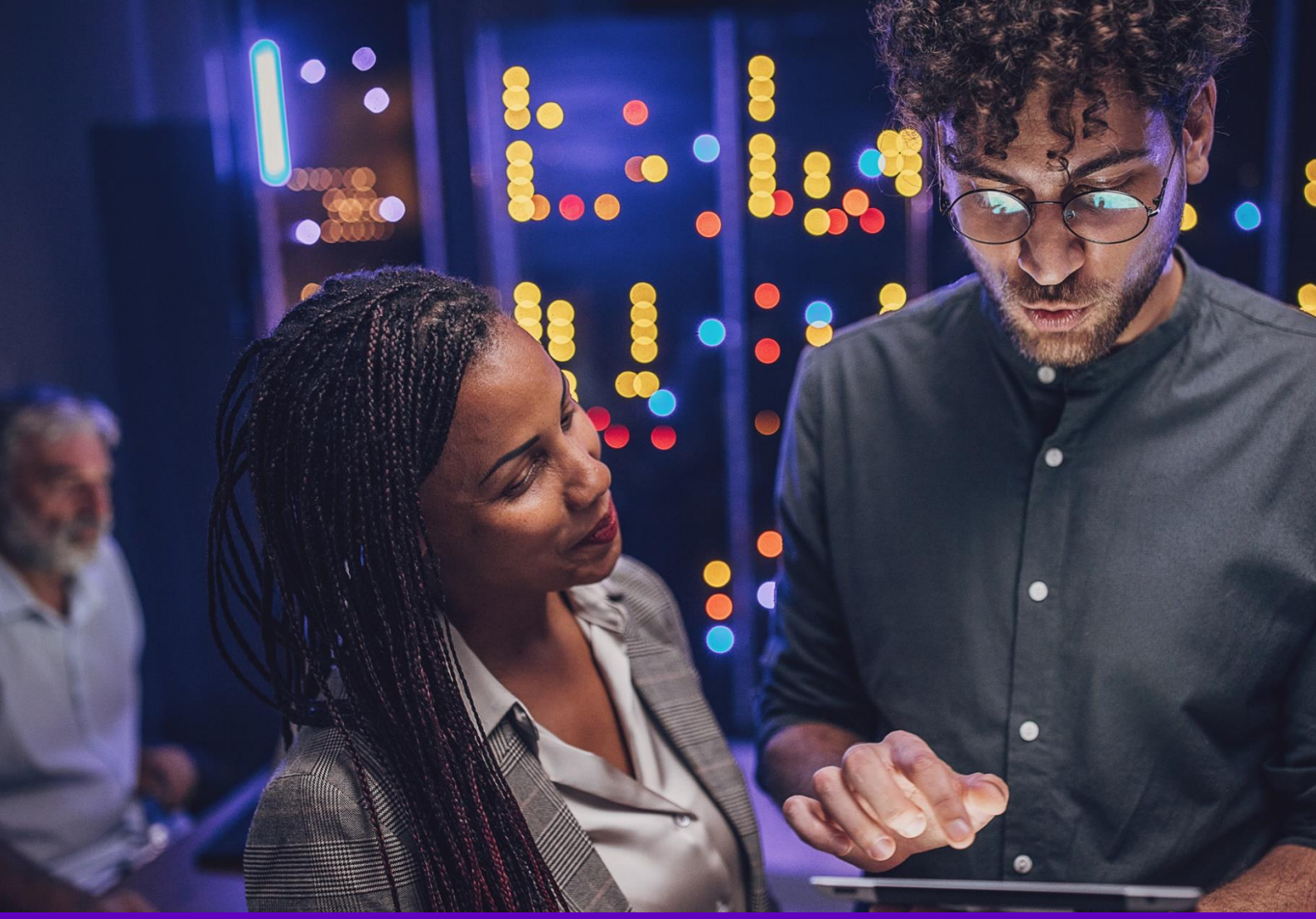

G-Cloud 14 Terms & Conditions

Accenture Standard Terms & Conditions

May 2024

accenture

Contents

1. Master Services Agreement....4
2. Schedule 1 - Change Control Procedure....8
3. General Accenture Cloud Terms....9
4. Appendix A – Definitions....18
5. Service Specific Terms - Amazon Web Services (AWS)....19
6. Attachment A - Security Standards....21
7. Attachment B - Encryption and Security Architecture Requirements....22
8. Service Specific Terms - Microsoft Azure (Azure)....23
9. Service Specific Terms - Google Cloud (Google)....25
10. SAP Cloud Services Agreement....27
11. Data Ingestion Terms Addendum....30
12. ServiceNow Terms and Conditions....33
13. Accenture Sales Contract....34
14. Power Virtual Agent (PVA) Terms and Conditions....37
15. Data Processing and Security Addendum....38

[Due to constraints in uploading multiple documents, we have consolidated the terms and conditions for all our services, other than Security Services, into this single document. The Master Services Agreement, its Schedule and the Data Processing and Security Addendum are intended to apply to all such services. Where applicable, the General Accenture Cloud Terms together with a relevant Service Specific Terms and/or ServiceNow, Sales, the SAP Cloud Service Agreement, the Data Ingestion Terms or PVA terms may also apply. Security Services terms and conditions are uploaded separately for the Security Services offerings only.]

1. Master Services Agreement

1.1 Services

This Master Services Agreement ("**MSA**") dated [insert date] ("**Effective Date**") sets out the terms and conditions under which Accenture (UK) Limited ("**Accenture**") with offices at 30 Fenchurch Street, London, EC3M 3BD will provide the services ("**Services**") and deliverables ("**Deliverables**") to [insert client name] ("**Client**") with offices at [insert client address], as specified in separately signed Statements of Work ("**SOW**(**s**)") (collectively the "**Agreement**") in which the terms and conditions set out in this MSA will be incorporated. Accenture and Client are jointly referred to as "**Parties**" and, solely, as "**Party**".

1.2 Warranties

Accenture warrants that its Services will be performed with reasonable skill and care, in accordance with the Agreement, and that the Deliverables will comply with their applicable specifications. Accenture will re-perform any work not in compliance with this warranty brought to its attention within 90 days after that work has been performed. To the extent permitted by law, all other warranties, terms, conditions and representations, express or implied, are excluded.

1.3 Acceptance

Client shall have the right to reject Deliverables by providing written notice within 10 business days after delivery identifying how the Deliverables fail to comply with their applicable specifications. If no such written rejection has been given, the Deliverable will be considered accepted.

1.4 Payment and taxes

Unless a different invoicing or payment structure has been agreed in the SOW, Accenture will, at the beginning of each month, invoice Client for the fees for that month (including a reasonable breakdown of detail), plus any applicable expenses and taxes; any necessary adjustments to the actual fees or billable expenses (which will be billed at actuals) incurred will be made in the next month's invoice. Client shall make payment in full, without set off or deduction, within 30 days of date of invoice. All Accenture fees and charges are exclusive of all taxes, including sales, use, value added, withholding, consumption and other similar taxes or duties. Each Party will be responsible for its own income, employment, and property taxes. Client will reimburse Accenture for any deficiency relating to taxes that are Client's responsibility under the Agreement. The Parties agree to cooperate with each other to help enable each Party to minimise any potential liability to the extent legally permissible and will provide to the other any tax exemptions or certifications reasonably requested.

1.5 Intellectual property

Each Party (or its licensors as applicable) shall retain ownership of its intellectual property rights, including patents, copyright, know-how, trade secrets and other proprietary rights ("IP") which were existing prior to each SOW, as well as IP developed, licensed or acquired by or on behalf of a Party or its licensors independently from the Services or the Deliverables, in each case including any modifications or derivatives to IP (collectively "Pre-Existing IP"). Client grants to Accenture (and its subcontractors), during the term of each SOW, a nonexclusive, fully paid, worldwide, non-transferable licence to use Client's Pre-Existing IP (and shall obtain the same licence/consent as required from any third-party), solely for the purpose of providing the Services and Deliverables. Client confirms it has the necessary rights for Accenture to use any IP or data provided by Client in connection with the Services and Deliverables. Except for Pre-Existing IP and third-party materials in the Deliverables, all IP in the Deliverables is assigned to the Client. Client grants Accenture a non-exclusive, fully paid, sublicenseable, worldwide licence to use the Deliverables (and no Client Confidential Information may be shared or exposed to others) for the purpose of providing the Services and developing the Deliverables.

Accenture grants to Client, subject to any restrictions applicable to any third-party materials embodied in the Deliverables, a perpetual, worldwide, non-transferable, non-exclusive, irrevocable right and licence to use Accenture Pre-Existing IP embedded in Deliverables for purposes of Client's and its affiliated companies' use, receipt and enjoyment of the Services and Deliverables only, and not on a stand-alone basis.

Accenture is not precluded from independently developing for itself, or for others, anything, whether in tangible or non-tangible form, which is competitive with, or similar to, the Deliverables, provided they do not contain Client Confidential Information. Certain Accenture assets (e.g. software, or platforms etc.), third-

party intellectual property and open-source software, may require additional terms, which will be addressed in the SOW where applicable. Accenture has the right to anonymise/de-identify and aggregate Client data with other data and leverage anonymous learnings and insights regarding use of Accenture products and/or services (the "Technical Data") and that Accenture owns Technical Data for any business purpose during and after the term of this Agreement (e.g., to develop, provide, and improve Accenture products and services). For the avoidance of doubt, as an agreed security measure, Client hereby directs Accenture to anonymise/de-identify any Client data prior to such data becoming Technical Data.

1.6 Indemnities

Accenture will defend and indemnify the Client, including its parents and affiliates, and their directors, employees, agents and representatives, against any third-party claims, including fines and penalties (and including interest and court costs), that Accenture IP used in the Services or embedded in a Deliverable, (a) infringes a third-party's copyright, trademark, or patent, or (b) misappropriates a third-party's trade secrets. If any Accenture IP used in the Services or embedded in the Deliverable is, or is likely to be held to be, infringing, Accenture will at its expense and option either: (i) procure the right for Client to continue using it, (ii) replace or modify it to make it non-infringing, or (iii) refund to Client the fees paid for it in exchange for a return. Client shall promptly notify Accenture in writing of the third-party claim, provide Accenture with sole defence of the claim and provide Accenture with reasonable cooperation in its defence and settlement of the claim.

Accenture will have no liability for any alleged infringement caused by the Client's modifications or use of the IP or Deliverable in breach of this Agreement, the unauthorised combination of the IP or Deliverable with thirdparty products or services, the failure to use corrections or enhancements to the IP or Deliverable provided by Accenture, or any infringement that is caused by Accenture complying with Client's specifications.

1.7 Liability

Except for Accenture's IP indemnification set out in Section 1.6 and for breach of the obligations relating to Confidential Information (other than a breach in respect of Personal Data which shall be subject to clause 7.2), the liability of either Party to the other in relation to any and all claims in any manner related to a SOW (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) will be for direct damages, not to exceed in the aggregate an amount equal to the total fees paid or payable to Accenture under the applicable SOW (or if the term of the SOW is 12 months or longer, the liability of each Party will be limited in the aggregate to the fees paid or payable under the applicable SOW during the 12 month period immediately preceding the event giving rise to the first claim.

The sole liability of Accenture to the Client in relation to any and all claims relating to Personal Data in any manner under a SOW (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) will be for direct damages, not to exceed in the aggregate an amount equal to the total fees paid or payable to

Accenture under the applicable SOW (or if the term of the SOW is 12 months or longer, the liability of Accenture will be limited in the aggregate to the fees paid or payable under the applicable SOW during the 12 month period immediately preceding the event giving rise to the first claim. This Clause 7.2 shall operate as a separate cap from the cap set out in Clause 7.1. This shall mean that any liability of Accenture (i) to which the cap set out in this Clause 7.2 applies shall not count towards the cap set out in Clause 7.1; or (ii) to which the cap set out in Clause 7.1 applies shall not count towards the cap set out in this Clause 7.2.

In no event will either Party be liable (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any: (i) consequential, indirect, incidental, special or punitive damages, or (ii) loss of profits, revenue, business, opportunity or anticipated savings (whether direct or indirect). Nothing in the Agreement excludes or limits either Party's liability to the other for: (i) fraud, (ii) death or bodily injury caused by negligence, and (iii) any other liability which cannot lawfully be excluded or limited.

1.8 Compliance with Laws

Each Party will comply with all laws and regulations applicable to their respective businesses including U.S. export control and sanction laws. Prior to providing Accenture any goods, software or technical data subject to export controls, Client will provide written notice specifying the nature of the controls and any relevant export control classification numbers.

1.9 Personal Data

Any Client data that identifies or directly relates to natural persons as may be further defined in applicable data privacy law ("**Personal Data**") shall remain at all times the property of Client. Except as expressly specified in the applicable SOW, the Parties acknowledge and agree that Accenture will not process Client Personal Data as part of the Services, and both Parties will use commercially reasonable efforts to monitor and restrict such access. However, if Accenture notifies Client that it has received Client Personal Data (excluding business contact information such as name, telephone, address and email) from Client that is not required to perform the Services, Accenture will notify Client, return, or destroy such Client Personal Data (as instructed by Client), and Client shall take steps to promptly rectify the situation to prevent recurrence. If it is agreed in a SOW that Accenture is to process Client Personal Data in connection with the Services, the general responsibilities of the Parties (with respect to the nature and purpose of such access, security controls and protocols, international transfer of data etc.) are set out in Data Processing and Security Addendum and the applicable SOW shall apply for processing of Client Personal Data. With respect to Client Personal Data that is provided to and processed by Accenture under an applicable SOW, Client shall be and remain the Data Controller and Accenture the Data Processor.

1.10 Confidentiality

Each Party may have access to information (in any form) that relates to the other Party and its activities which is identified by the disclosing Party as confidential or reasonably understood to be confidential ("**Confidential Information**"). The receiving Party agrees that Confidential Information may only be used for the purposes set out in the Agreement and that it will protect Confidential Information in the same manner that it protects its own similar confidential information, but in no event using less than a reasonable standard of care. Confidential Information may only be disclosed to an employee, subcontractor or (with the consent of the other Party) to a third-party if required for the purpose of the Agreement and provided such parties are bound by substantially similar obligations of confidentiality. Nothing in the Agreement will prohibit or limit either Party's use of information (i) previously known to it without an obligation not to disclose such information, (ii) independently developed by or for it without use of Confidential Information, (iii) acquired by it from a third-party which was not, to the receiver's knowledge, under an obligation not to disclose such information, or (iv) which is or becomes publicly available through no breach of the Agreement.

1.11 Termination

Client may, upon giving 30 days written notice, terminate a SOW for convenience or material breach unless Accenture cures such breach within the 30 day period. Accenture may, upon giving 30 days written notice, terminate a SOW for non-payment of undisputed fees, unless client pays such undisputed fees within the 30 day period. If a SOW is terminated, Client will pay Accenture for all Services and Deliverables rendered, including a pro-rated portion for Deliverables in progress and expenses incurred prior to the date of termination.

1.12 Audit

Client is entitled to conduct an audit, at its expense, for the purpose of determining whether Accenture is in compliance with its obligations under the Agreement, in accordance with a mutually agreed process designed to avoid disruption of the Services and protect the confidential information of Accenture and its other clients. Any access to Accenture's premises, personnel, data, records, controls, processes, and procedures relating to the Services will be subject to Accenture's reasonable access and security requirements. If material breaches of the Agreement are identified by an audit, Accenture shall take prompt action to mitigate any such breach and will bear the expense of the relevant audit.

1.13 Assignment and non-solicitation

Neither Party may assign the Agreement (other than, upon written notice, to a Party's subsidiary or affiliate under common control) without the prior written consent of the other, which consent will not be unreasonably withheld or delayed. The Agreement shall be binding on each Party's permitted assignees. Each Party is an independent contractor and does not have any authority to bind or commit the other. Nothing in the Agreement will be deemed or construed to create a joint venture, partnership, fiduciary or agency relationship between the Parties for any purpose. Neither Party will solicit any of the other Party's or its affiliates employees during their engagement in the Services; however, this restriction will not apply to employees who are not engaged in the Services or who independently respond to indirect solicitations (such as general advertisements) not targeting such employees.

1.14 Miscellaneous

The Agreement sets out the entire understanding between the Parties and supersedes, without limitation, all prior discussions, communications, representations and arrangements between them with respect to its subject matter. In the event of conflict, the terms of any SOW shall prevail over this MSA. Each Party acknowledges that it has not relied on or been induced to enter into this MSA by a representation that is not set out in this Agreement. If a court of competent jurisdiction finds any term of the Agreement to be invalid, such term will not affect the other terms of the Agreement. No waiver or modification of any provision of the Agreement or SOW will be effective unless it is in writing and signed by the Party against which it is sought to be enforced. The delay or failure by either Party to exercise or enforce any of its rights under the Agreement is not a waiver of that Party's right to later enforce those rights, nor will any single or partial exercise of any such right preclude any other or further exercise of these rights or any other right. Any notice or other communication provided under the Agreement will be in writing, addressed to such Party at the address set out in the Agreement, or upon electronic delivery by confirmed means. Accenture may request, and Client will provide reasonable written or verbal verification of the engagement and general nature of the services to Accenture clients. Client's Confidential Information and prices for the Services shall never be disclosed in such referrals without the permission of Client. There are no third-party beneficiaries to the Agreement. Neither Party will be liable for any delays or failures to perform due to causes beyond that Party's reasonable control (including a force majeure event). Accenture will not be liable for failure or delay caused by non-performance of (or delay in the performance of) the Client's obligations under this Agreement. The Parties will use reasonable endeavours to mitigate the impact of any such delays or failures. The Parties will act in good faith, including during governance meetings, to resolve and address the impact of any such issues.

1.15 Applicable law and Disputes

The Agreement shall be governed by and construed in accordance with the laws of England. The Parties will make good faith efforts to resolve within 30 days any dispute in connection with the Agreement by escalating it to higher levels of management. Each Party irrevocably submits to the exclusive jurisdiction of the courts of England in respect of any litigation.

AGREED TO BY:	**AGREED TO BY:**
Client: _____	**ACCENTURE (UK) LIMITED**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

2. Schedule 1 - Change Control Procedure

2.1 Change process

Each Party may propose a change to the scope of Services, timelines, project plan, charges for the Services, additional resources and the like of this Agreement and such change shall only be effective when it is set forth in a writing executed by authorized representatives of both Parties (**"Contract Change"**). Neither Party will be entitled to or obligated by such a change until a Change Order has been executed.

2.1.1 Change Request

To request a Contract Change, Accenture or Client, as applicable, will deliver a written request (the **"Change Request"**) to the Accenture Delivery Manager or the Client Account Manager, as the case may be, specifying in reasonable detail to the extent known: (i) the proposed Contract Change; (ii) the objective or purpose of such Contract Change; (iii) the particular SOW provisions that are affected by the Contract Change; and (iv) the requested prioritization and schedule for such Contract Change. The Parties must cooperate with each other in good faith in discussing the scope and nature of the Change Request. For clarity, changes to the terms and conditions in the body of the MSA will be subject to a formal amendment to the MSA (and not treated or addressed as a Change Request).

2.1.2 Change Response

If either Party wishes to proceed with the proposed Contract Change, as soon as practicable and to the extent applicable, Accenture will prepare and deliver to the Client Account Manager a written Change Order describing any changes in methodology, procedures, prioritization, products, services, assignment of personnel, deliverables and due dates, and other resources that Accenture believes would be required to affect the Contract Change. In addition, such Change Order will include, as appropriate or applicable: (i) an estimation of any additional Charges or change in the Charges that may be required; (ii) the categories of costs, if any, that may be avoided as a result of such Contract Change; (iii) a description of how the proposed Contract Change would be implemented; (iv) a description of the effect, if any, such Contract Change would have on the obligations of the Parties under the SOW; and (v) such other information as may be relevant to the proposed Contract Change. The Accenture Delivery Manager and the Client Account Manager will meet to determine whether they desire for Accenture to proceed with the implementation of the proposed Contract Change in accordance with the Change Order.

2.2 Approval

Upon agreement of the Parties, the Change Order as finally agreed to by the Parties will amend this SOW. Neither Party is obliged nor may it vary its obligations under this SOW unless and until a Change Response is approved by the Parties. No Change Order shall be implemented unless and until signed by authorized representatives of both Parties. Accenture shall be entitled to charge Client for any material costs relating to the preparation, investigation and implementation of Change Orders instigated by Client.

3. General Accenture Cloud Terms

[Due to constraints in uploading multiple documents, we have consolidated these into one document. In the event of provision of AWS, the AWS Service Specific Terms would apply, in the event of provision of Microsoft Azure, the Microsoft Azure Service Specific Terms would apply and in the event of provision of Google Cloud, the Google Cloud Service Specific Terms would apply.]

3.1 Agreement structure

3.1.1 The following General Cloud Terms ("General Cloud Terms"), together with the terms of any applicable service specific terms ("Service Specific Terms") [and any applicable statement of work or service order] (collectively, "Cloud Agreement"), shall govern the provision of Cloud Services by Accenture, and the consumption of Cloud Services by Client. These General Cloud Terms are only effective together with Service Specific Terms in which the terms and conditions set out herein will be incorporated. Each Cloud Agreement is a separate agreement and shall be interpreted without reference to any other agreement.

3.1.2 The terms and conditions of the [*Master Service Agreement*] entered into by the Parties on [*add date*] shall not govern or apply in any manner to the provision or consumption of Cloud Services, unless otherwise stated hereunder.

3.1.3 In the event of a conflict or inconsistency between these General Cloud Terms and the Service Specific Terms, the Service Specific Terms shall prevail to the extent of the conflict or inconsistency.

3.1.4 Capitalized terms used in the Cloud Agreement shall have the meaning given to them either in the provisions below or Appendix A.

3.2 Provision of cloud services

3.2.1 Accenture will provide the Cloud Services to Client, as further defined in the Service Specific Terms, in accordance with the Cloud Agreement.

3.2.2 Accenture shall perform the Cloud Services in compliance with any laws directly applicable to Accenture as a provider of the Cloud Services.

3.2.3 Accenture will use generally accepted industry standard security technologies in providing the Cloud Services as determined by Accenture. More detailed data processing and security policies, if any, shall be included in the applicable Service Specific Terms.

3.2.4 Accenture reserves the right to make updates and changes to the Cloud Services that Accenture deems necessary or otherwise appropriate, provided that Accenture may not make changes to the Cloud Services that would materially reduce or otherwise negatively impact the Cloud Services' core features and functionalities.

3.2.5 Accenture may use Cloud Vendor Solutions in the provision of Cloud Services, in which case Client agrees that Accenture can only provide and make available to Client those Cloud Vendor Solutions included in the Cloud Services under the terms and conditions that the relevant Cloud Vendor has made its Cloud Vendor Solutions available to Accenture. To the extent directly applicable to Client and to the relevant Cloud Services, Cloud Vendor terms shall be incorporated in the relevant Service Specific Terms.

3.2.6 Where Accenture uses Cloud Vendor Solutions in the provision of Cloud Services, Client acknowledges that the Cloud Vendors have reserved the right to change, discontinue and depreciate, or change or remove features or functionalities from, the Cloud Vendor Solutions from time to time. Where changes to the Cloud Vendor Solutions would have a material impact on the Cloud Services, Accenture will inform Client as soon as practically possible and at least [sixty (60) days] in advance of such changes to the Cloud Vendor Solutions coming into force, and enter into good faith negotiations with Client to agree on any necessary changes to the Cloud Services and the Cloud Agreement.

3.2.7 Accenture and the Cloud Vendors reserve the right to monitor Client's and Users' access and use of the Cloud Services for the purposes of: (i) obtaining Accenture Insights Data (as defined in Section 3.8.2 below) to further develop and improve the Cloud Services; and (ii) verifying Client's and Users' compliance with the Cloud Agreement.

3.3 Right of use

3.3.1 Accenture grants to Client a non-exclusive, non-transferable right, during the term of provision of Cloud Services set out in the applicable Service Specific Terms, to access and use (and permit Users to access and use) the Cloud Services, in accordance with the Cloud Agreement.

3.3.2 Client may access and use the Cloud Services for its own internal business purposes only. Client agrees that it shall not license, sub-license, sell, resell, transfer, assign, distribute or otherwise commercially exploit the Cloud Services by making them available for access or use by any third-party that is not a User.

3.3.3 Client shall be responsible for all acts and omissions of Users, as if they were the acts and omissions of Client, and for ensuring that anyone who uses the Cloud Services does so in accordance with the Cloud Agreement. Client shall not, and shall ensure that Users do not: (a) take any action or omission that poses a security risk or may otherwise adversely impact the Cloud Services, including by interfering with or disrupting any security controls and mechanisms of the Cloud Services; (b) host or transmit any content, data or information that is illegal, or that infringes any third-party's rights, such as IPR or right of privacy; (c) take any action or omission that otherwise violates applicable law; (d) copy, translate, make derivative works of, disassemble, decompile, reverse engineer or otherwise attempt to discover the source code or underlying ideas or algorithms embodied in the software applications or other systems used in the provision of the Cloud Services, unless expressly permitted under applicable law, or remove any titles or trademarks, copyrights or restricted rights notices in the systems, software and other materials used in the provision of the Cloud Services; or (e) access or use (or allow a third party to access or use) the Cloud Services for the purposes of building products or services that are competitive to the Cloud Services.

3.4 Suspension

3.4.1 Accenture reserves the right to suspend Client's and Users' rights to access and/or use all or any portion of the Cloud Services, or remove any relevant Client Content where Accenture reasonably believes (i) Client or Users are in breach of the Cloud Agreement, including without limitation Section 3.3.3; (ii) Client has failed to respond to a claim of alleged infringement; or (iii) Accenture is required to do so by applicable law, or any court or governmental body order. Accenture also reserves the right to suspend Client's and Users' right to access or use all or any portion of the Cloud Services where Client fails to pay to Accenture any amounts payable within thirty (30) days of such amounts being due.

3.4.2 To the extent permitted by applicable law, and if otherwise reasonable and feasible under the circumstances (as determined by Accenture in its discretion), Accenture will provide Client with written notice prior to suspension, and an opportunity to take steps to avoid such suspension. Any suspension or removal of Client Content shall not release Client from its obligations under the Cloud Agreement, including any obligation to pay the Fees. Accenture's suspension right is in addition to Accenture's right to terminate the Cloud Agreement pursuant to Section 3.12.

3.5 Client's responsibilities

3.5.1 Client is solely responsible for determining (a) the suitability of the Cloud Services for its business, and (b) the manner in which Client and its Users access and use the Cloud Services complies with all applicable laws.

3.5.2 Client is responsible for obtaining and maintaining all hardware, software, communications equipment and network connections necessary to access and use the Cloud Services, and for paying any applicable third-party fees and charges incurred to access and use the Cloud Services.

3.5.3 Except as described in the Cloud Agreement and to the extent that the Parties explicitly have agreed in any statement of work or service order that Accenture will provide any of the below-listed activities as part of its services, Client shall be responsible for taking appropriate steps to protect and maintain the security of the Cloud Services and the Client Content, including without limitation: (a) backing-up the Client Content to a sufficient standard to ensure Client's business continuity; (b) maintaining commercially reasonable security standards for Users' access to the Cloud Services, including without limitation the use of sufficiently secure passwords and regularly required password changes, and maintaining the confidentiality of any non-public authentication credentials associated with Client's use of the Cloud Services; and (c) using all reasonable endeavours to ensure that Users do not upload or distribute files that contain Viruses, malicious files or other harmful code, or

disrupt or attempt to disrupt the systems and networks used in the provision of the Cloud Services, including by using good industry practice virus protection software, and other customary procedures to screen Client Content.

3.5.4 Client shall notify Accenture as soon as it becomes aware of any breach or threatened breach of the terms of Sections 3.3.3 or 3.5.3 (b) or (c), or of any breach or threatened breach of security including any attempt by a third party to gain unauthorized access to the systems used in the provision of the Cloud Services, or any other security incident relating to the Cloud Services.

3.5.5 Client is responsible for responding to any request from a third party regarding Client's use of the Cloud Services, such as a request to take down content under applicable law.

3.6 Payment and taxes

3.6.1 Unless otherwise agreed in writing, Accenture will, at the beginning of each month, invoice Client for the Fees for that month, plus any applicable out-of-pocket expenses and applicable taxes; any necessary adjustments to the actual Fees or billable expenses incurred (which will be billed at actuals) will be made in the next month's invoice. Client shall make payment in full, without set off or deduction, within thirty (30) days of the date of invoice. Accenture shall be entitled to charge interest on invoices which remain unpaid for more than thirty (30) days, at a rate of 1% per month or the highest rate allowed by law, whichever is less. All Accenture Fees and charges are exclusive of all taxes, including sales, use, value added, withholding and consumption taxes, and each Party will be responsible for its own income, employment and property taxes.

3.6.2 The Parties agree to fully cooperate with each other to help each Party accurately determine and reduce its own tax liability and to minimize any potential liability to the extent legally permissible and will provide to the other any tax exemptions or certifications reasonably requested. Client will be responsible for payment of all taxes in connection with the Cloud Agreement, including withholding taxes and taxes incurred on transactions between and among Accenture, its affiliates, and third party subcontractors. Client will reimburse Accenture for any deficiency relating to taxes that are Client's responsibility under the Cloud Agreement.

3.7 Client content

3.7.1 Client (and Client's licensors, where applicable) own all right, title and interest, including all IPR, in and to the Client Content. Except as provided under the Cloud Agreement, Accenture obtains no other rights to Client Content.

3.7.2 Client authorizes Accenture to host, store, process and transfer the Client Content in accordance with the Cloud Agreement. Client agrees that it is solely responsible for all Client Content, and for complying with any applicable law relating to the Client Content, and for obtaining any licenses to, consents for and rights in Client Content necessary for Accenture to provide the Cloud Services to Client, without violating the rights of any third party or otherwise obligating Accenture to Client or to any third party.

3.7.3 Accenture assumes no obligations with respect to Client Content, other than as expressly set forth in the Cloud Agreement, or as required by applicable law.

3.7.4 In the event where Client Content contains any Personal Data, Client authorizes Accenture, Cloud Vendors and subcontractors (as applicable) to process such Personal Data, as required to perform the Cloud Services and in accordance with any data processing policy incorporated in or referred to in the applicable Service Specific Terms.

3.7.5 Client will obtain all required consents from data subjects and any other applicable third parties under applicable privacy and data protection laws before providing Personal Data to Accenture. To the extent required by applicable law, Client shall notify any data subjects whose data will be processed or stored on the Cloud Services that their data may be disclosed to law enforcement or other governmental authorities, and Client shall obtain the data subjects' consent to the same.

3.7.6 Client shall be and remain the Data Controller and Accenture the Data Processor with respect to any Client Personal Data that is provided to and processed by Accenture pursuant to any Cloud Agreement. Each Party shall comply with its respective obligations as the Data Controller and Data Processor under applicable privacy and data protection law.

3.7.7 Accenture will not disclose Client Content to any third party except: (i) with Client's written consent; (ii) to a Cloud Vendor or a subcontractor to the extent necessary for such Cloud Vendor or subcontractor to provide the Cloud Vendor Solution or subcontractor services, respectively; or (iii) as required by any applicable law, a court order or an authorized regulatory body and/or any law enforcement agency.

3.7.8 Client shall have the ability to access its Client Content hosted over the Cloud Services at any time during the term specified in the applicable Cloud Agreement. Client may export and retrieve its Client Content during such term, which will be subject to technical limitations caused by factors such as (i) the size of Client's instance of the Cloud Services; and (ii) the frequency and/or timing of the export and retrieval.

3.8 Intellectual property rights

3.8.1 Accenture and the Cloud Vendor(s) (and their third party licensors, where applicable) own all right, title and interest, including all Intellectual Property Rights, in and to (i) the systems, software and other content and materials used in the provision of the Cloud Services; and (ii) any suggestions, ideas, enhancement requests, feedback or recommendations provided by Client or any other party relating to the Cloud Services, and Client hereby assigns any Intellectual Property Rights in such items to Accenture.

3.8.2 Notwithstanding any provision in the Cloud Agreement to the contrary, (i) Accenture has the right to anonymize and aggregate Client Content with other data and leverage anonymous learnings and insights regarding use of Accenture products and/or services (the anonymised data, "Accenture Insights Data" or "AID") and Accenture owns, and may use, AID for any business purpose during and after the term the Cloud Agreement (including without limitation, to develop, provide and improve Accenture products and services); (ii) Accenture may also use Client Content to develop, provide and improve Accenture products and services; and (iii) the Accenture name, the Accenture logo and the product names associated with the Cloud Services, are trademarks of Accenture or third parties, and no right or license is granted to Client to use them.

3.9 WARRANTIES AND EXCLUSIONS

3.9.1 Each Party warrants that upon its execution, the Cloud Agreement will not materially violate any term or condition of any agreement that such Party has with any third party and that the officers executing the Cloud Agreement are authorized to bind such Party to the applicable terms and conditions.

3.9.2 Accenture warrants that the Cloud Services provided to Client pursuant to the Cloud Agreement will comply in all material respects with the services descriptions included in or referred to in the applicable Service Specific Terms.

3.9.3 The preceding warranties shall not apply where: (i) any problems have been caused by accident, abuse, or where Client's or Users' access or use of the Cloud Services is not in accordance with the Cloud Agreement or Accenture's instructions, including failure to meet minimum system requirements; (ii) the Cloud Services or any systems, software or other content or materials embodied therein are modified or altered by any party other than Accenture; or (iii) the Cloud Services are provided free of charge, and/or as a trial, pre-release or beta release.

3.9.4 To the extent permitted by law, (i) the preceding warranties exclude all other warranties, terms, conditions and representations, express or implied, including fitness for purpose, non-infringement, satisfactory quality, quiet enjoyment or otherwise, and (ii) except as expressly provided in Sections 3.9.1 and 3.9.2, Accenture, its affiliates and its licensors (including any Cloud Vendors) make no representations and provide no warranties of any kind, whether express, implied, statutory or otherwise regarding the Cloud Services or any third-party components or content embodied therein, including any warranty that the Cloud Services will be uninterrupted, error free, or free of harmful components, or that any content, including Client Content or third-party components or content, will be secure or not otherwise lost or damaged.

3.10 Indemnities

3.10.1 Subject to the limitations in Section 11, Accenture will defend Client and its affiliates, against any damages, losses, liabilities, costs and expenses (including reasonable legal fees) arising out of or relating to any claim brought against Client by a third party (that is not an affiliate of Client) alleging

that the Cloud Services, or use thereof by Client, infringe or misappropriate the Intellectual Property Rights of such third party. In addition to defending at its sole expense, Accenture will be obliged to pay only the amount of damages finally awarded against Client or the amount of any settlement agreed by Accenture.

3.10.2 If any portion of the Cloud Services is, or is likely to be held to be, infringing, Accenture will at its expense and option: (a) procure the right for Client to continue using it; (b) replace it with a noninfringing equivalent; or (c) modify it to make it non-infringing while still providing substantially the same level of functionality. If Accenture determines that none of the afore-mentioned options are commercially reasonable, Accenture may immediately terminate Client's access to the affected Cloud Service(s).

3.10.3 Accenture will not have any obligations or liability under Section 10.1 for any claims arising from: (a) infringement by combinations of the Cloud Services with any other product, service, software, content, data or method that has not been provided by Accenture; (b) any unauthorised modification of the Cloud Services; or (c) any use of the Cloud Services, other than as permitted under the Cloud Agreement. In addition, Accenture will have no obligations or liability under Section 10.1 for Client's or any User's use of the Cloud Services after Accenture has notified Client to discontinue use and Client has been afforded a reasonable opportunity to discontinue such use.

3.10.4 Subject to the limitations in Section 11, Client shall defend Accenture, its affiliates and licensors against any damages, losses, liabilities, costs and expenses (including reasonable legal fees) arising from or related to (i) any use of Cloud Services by Client or Users in violation of applicable law; (ii) any allegation that the Client Content violates, infringes or misappropriates any rights of a third party; or (iii) Client's or Users' use of the Cloud Services or other act or omission in violation of the Cloud Agreement. In addition to defending at its sole expense, Client will be obliged to pay only the amount of damages finally awarded against Accenture or the amount of any settlement agreed by Client.

3.10.5 Client will not have any obligations or liability under Section 10.4 for any claims arising from the Client Content after Client has notified Accenture to delete the Client Content within Accenture's control from the Cloud Services and Accenture has been afforded a reasonable opportunity to do so.

3.10.6 To receive the benefit of this Section 10, the indemnified Party must promptly notify the indemnifying Party in writing of the claim and provide reasonable cooperation and full authority to the indemnifying Party to defend or settle the claim, provided that such settlement does not impose any obligation (monetary or otherwise) on the indemnified Party (other than to cease using the infringing IPR or Cloud Services) without its consent.

3.10.7 This Section sets out the indemnified Party's sole and exclusive remedy and the indemnifying Party's entire liability to the indemnified Party with respect to any indemnified claims under this Section 10.

3.11 LIABILITY

3.11.1 Except as set out in Sections 3.11.2 and 3.11.3, each Party's total aggregate liability to the other whether based on an action or claim in contract, tort (including negligence), breach of statutory duty or otherwise arising out of, or in relation to, each Cloud Agreement will be limited to an amount equal to the Fees received by Accenture for the Cloud Services that gave rise to the liability under the relevant Cloud Agreement during the twelve (12) month period immediately preceding the event giving rise to the claim or, in respect of any such event occurring during the first twelve (12) months of the Cloud Agreement, the Fees payable by Client under the applicable Client Agreement during the first twelve (12) months.

3.11.2 The limitation of liability set out in Section 3.11.1 will not apply to (i) the Parties' obligations under Section 3.10; (ii) a violation of the other Party's IPR; and (iii) Accenture's right to collect unpaid Fees due hereunder.

3.11.3 Nothing under any Cloud Agreement excludes or limits either Party's liability to the other that cannot lawfully be excluded or limited.

3.11.4 To the extent permitted by any applicable law, neither Party nor any of either Party's respective affiliates will be liable to the other Party, however caused or on any theory of liability (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise), even if a Party has been

advised of the possibility of such damages, for any: (i) indirect, incidental, special, consequential, punitive or exemplary damages; (ii) loss of use, business interruption, loss of profits or savings, loss of business information, business, revenues, opportunity or anticipated savings, reputation harm, or goodwill (in each case, whether directly or indirectly arising); (iii) unavailability of any or all of the Cloud Services (without prejudice to Client's right to receive service credits under any service level agreement, if applicable); (iv) investments, diminution in stock price, expenditures or commitments related to use of or access to the Cloud Services; (v) cost of procurement of substitute services; (vi) unauthorized access to, compromise, alteration or loss of Client Content; or (vii) cost of replacement or restoration of any lost or altered Client Content.

3.11.5 To the extent permitted by any applicable law, no action, regardless of form, arising out of the Cloud Agreement may be brought by Client more than two (2) years after Client knew or should have known of the event which gave rise to the cause of action.

3.12 Term and termination

3.12.1 The term of these General Cloud Terms will commence on the Effective Date and will continue until terminated by either Party pursuant to this Section 3.12 ("Term"). The term of any Cloud Agreement shall be agreed in the Service Specific Terms.

3.12.2 In the event where no fixed term has been defined in the Service Specific Terms, either Party may terminate these General Cloud Terms for convenience upon ninety (90) days' written notice to the other Party.

3.12.3 Either Party may terminate these General Cloud Terms or any Cloud Agreement with immediate effect upon written notice if the other Party ceases its business operations or becomes subject to insolvency proceedings which are not dismissed within ninety (90) days, or otherwise becomes generally unable to meet its obligations under these General Cloud Terms or the Service Specific Terms.

3.12.4 Either Party may, upon giving thirty (30) days' written notice, terminate any Cloud Agreement due to a material breach of these General Cloud Terms or the relevant Service Specific Terms, unless the Party receiving the notice cures the breach within the thirty (30) day period.

3.12.5 Accenture may terminate the Cloud Service upon [sixty (60)] days' written notice to Client (i) in the event where the underlying contract between Accenture and the Cloud Vendor concerning the provision of the Cloud Vendor Solution terminates; or (ii) if termination of these General Cloud Terms and/or any Cloud Agreement is necessary to comply with applicable law or binding requests of governmental entities with authority to make such request.

3.12.6 If a Cloud Agreement is terminated by either Party, Client will pay Accenture for all Cloud Services rendered and expenses incurred prior to the date of termination.

3.12.7 Upon the effective date of expiration or termination of a Cloud Service, Accenture shall immediately cease Client's and Users' access to and use of the Cloud Services.

3.12.8 The Parties may agree in the applicable statement of work that Client shall have the ability to access and extract Client Content for a certain period after the expiration or termination of the applicable Cloud Agreement ("Retention Period"). In such case Accenture will procure that the applicable Cloud Vendor will retain the Client Content for the Retention Period, during which Client will cover the costs of the data storage unless otherwise agreed in writing. After the Retention Period, all Client Content will be deleted.

3.12.9 If mutually agreed by the Parties, Accenture shall provide to Client reasonable co-operation and assistance to facilitate the orderly wind down of the usage of the Cloud Services and/or to assist Client to transition to another service provider. Client will pay Accenture for such assistance at Accenture's then-current time and materials rates for the applicable services or as otherwise mutually agreed by the Parties.

3.13 Confidentiality

3.13.1 Each Party may have access to Confidential Information and the receiving Party agrees that Confidential Information may only be used for the purposes set out in the Cloud Agreement and that it will protect Confidential Information in the same manner that it protects its own similar confidential information, but in no event using less than a reasonable standard of care.

3.13.2 Confidential Information may only be disclosed by the receiving Party to an employee, subcontractor or (with the consent of the disclosing Party) to a third party if required for the purpose of the Cloud Agreement and provided such parties are bound by substantially similar obligations of confidentiality.

3.13.3 Nothing in the Cloud Agreement will prohibit or limit either Party's use of information: (i) previously known to it without an obligation not to disclose such information; (ii) independently developed by or for it without use of Confidential Information; (iii) obtained from a third party which was not, to the receiving Party's knowledge, under an obligation not to disclose such information; or (iv) which is or becomes publicly available through no breach by the receiving Party.

3.13.4 Each Party is entitled to disclose Confidential Information to the extent required by law or by any statutory or regulatory authority, provided that promptly upon receiving any such request and to the extent legally permissible, it: (i) advises the other Party of the full circumstances of the required disclosure; (ii) takes actions necessary or reasonably required by the other Party to minimize any disclosure; and (iii) to the extent possible, obtains confidentiality undertakings from the entity to whom the Confidential Information is to be disclosed.

3.13.5 The disclosing Party may, at any time, request that the receiving Party return, destroy and/or delete (and confirm the destruction and/or deletion of the same), and in such a manner that it cannot be recovered, all or part of the Confidential Information of the disclosing Party in the receiving Party's possession or control. Notwithstanding the foregoing, each Party may archive copies of Confidential Information that it is required to retain to comply with law and for its other record-keeping requirements.

3.13.6 Neither Party will use the other Party's name outside its company without prior written consent of the other Party. Notwithstanding the foregoing, Accenture shall be permitted to refer to Client as a customer reference concerning the general area of work under any Cloud Agreement, for opportunities at existing and prospective Accenture clients. Accenture may request, and Client will provide reasonable written or verbal verification of the engagement and general nature of the services to such Accenture clients (such verification not to be unreasonably withheld). Client's Confidential Information and prices for the Cloud Services shall never be disclosed in such referrals without Client's permission.

3.13.7 Client shall not disclose the terms and conditions of the Cloud Agreement or the pricing contained therein to any third party without the prior written consent of Accenture. Neither Party shall use the name of the other Party in publicity, advertising, or similar activity, without the prior written consent of the other Party. Notwithstanding the aforesaid, Client acknowledges and agrees that Accenture may provide information regarding Client's purchase, use and consumption of the Cloud Vendor Solution, and the related terms, to the relevant Cloud Vendor, subject to obligations of confidentiality with the Cloud Vendor.

3.14 Excuse

3.14.1 Neither Party will be liable for any delays or failures to perform due to causes beyond that Party's reasonable control (including a force majeure event). Without limiting the foregoing, to the extent Client fails to perform any of its responsibilities described in the Cloud Agreement, Accenture shall be excused from failure to perform any affected obligations under the Cloud Agreement and, in the event of delay, be entitled to a reasonable extension of time considering the particular circumstances, and a reasonable reimbursement of cost. Each Party will notify the other as promptly as practicable after becoming aware of the occurrence of any such condition.

3.15 Relationship and non-solicitation

3.15.1 Each Party is an independent contractor and does not have any authority to bind or commit the other. Nothing in the Cloud Agreement will be deemed or construed to create a joint venture, partnership, fiduciary or agency relationship between the Parties for any purpose. Neither Party will solicit, offer work to, employ, or contract with, directly or indirectly, any of the other Party's or its affiliates' employees during their engagement in the Cloud Services or during the twelve (12) months after the employee ceases to be engaged in such Cloud Services. However, this restriction will not apply to employees who are not engaged in the Cloud Services or who independently respond to indirect solicitations (such as general advertisements) not targeting such employees.

3.16 Miscellaneous

3.16.1 Entire Agreement. The Cloud Agreement sets out the entire agreement between the Parties and supersedes, without limitation, all prior discussions, communications, representations and arrangements between them with respect to its subject matter. Each Party acknowledges that it is entering into the Cloud Agreement solely on the basis of the agreements and representations contained herein, and that it has not relied upon any representations, warranties, promises, or inducements of any kind, whether oral or written, and from any source.

3.16.2 Assignment. Neither Party may assign the Cloud Agreement without the prior written consent of the other, which consent will not be unreasonably withheld or delayed. The Cloud Agreement shall be binding on each Party's permitted assignees.

3.16.3 Severability. If a court of competent jurisdiction finds any term of the Cloud Agreement to be invalid, illegal or otherwise unenforceable, such term will not affect the other terms of the Cloud Agreement and will be deemed modified to the extent necessary, in the court's opinion, to render such term enforceable while preserving to the fullest extent permissible the intent and agreements of the Parties set out in the Cloud Agreement.

3.16.4 No waiver. No waiver or modification of any provision of the Cloud Agreement will be effective unless it is in writing and signed by the Party against which it is sought to be enforced. The delay or failure by either Party to exercise or enforce any of its rights under the Cloud Agreement is not a waiver of that Party's right to later enforce those rights, nor will any single or partial exercise of any right preclude any other or further exercise of these rights or any other right.

3.16.5 Notices. Any notice or communication provided under the Cloud Agreement will be in writing, addressed to such Party at the address set out in the Cloud Agreement (plus Client must also send a copy of its notice (except for routine correspondence) to: Accenture LLP, Legal – General Counsel, 161 North Clark Street, Chicago, Illinois 60601), or upon electronic delivery by confirmed means. The notice will be deemed given and will be effective: (i) upon receipt when it is delivered to a Party personally; (ii) upon receipt if sent through certified mail, return receipt requested; or (iii) upon delivery by a nationally recognized overnight courier service such as FedEx (with confirmation of delivery). Either Party may designate a different address by giving ten (10) days' written notice to the other Party.

3.16.6 Third Party Rights. Accenture's licensors are third party beneficiaries under the Cloud Agreement. The Cloud Agreement does not otherwise create any third-party beneficiary rights, and it is agreed that Client's Users are not third-party beneficiaries.

3.16.7 Subcontractors. Accenture or the Cloud Vendors may provide the Cloud Services through the use of subcontractors (including Accenture affiliates as subcontractors), subject to remaining fully responsible for its subcontractors' performance. More information on the Cloud Vendor subcontractors or subprocessors may be provided in the Service Specific Terms.

3.16.8 Survival. All provisions of the Cloud Agreement that are by their nature intended to survive expiry or termination of the Cloud Agreement will survive such expiry or termination.

3.16.9 Variation. The Cloud Agreement may not be modified or amended except by the mutual written agreement of the authorized representatives of the Parties.

3.16.10 Counterparts. These General Cloud Terms and any Service Specific Terms may be executed electronically and in multiple counterparts, each of which will be considered an original, and all of which together will constitute one agreement binding on the Parties, even if both Parties are not signatories to the original or same counterpart.

3.16.11 Anti-bribery. Accenture maintains a robust set of business conduct and related guidelines covering conflicts of interest, market abuse, anti-bribery and corruption, and fraud (which cover requirements to comply with applicable law and regulation under Anti-Corruption Laws, as defined below). Accenture and its personnel comply with such policies and require contractors and subprocessors to have similar policies. Accenture has in place, and shall maintain in place throughout the Term, effective disclosure controls, policies and procedures designed to ensure compliance with Anti-Corruption Laws, and will enforce them where appropriate. At Client's request, Accenture will disclose such policies and procedures to Client. "Anti-Corruption Laws" means any applicable foreign or domestic anti-bribery and anti-corruption laws and regulations, including the UK Bribery

Act 2010, the US Foreign Corrupt Practices Act 1977 and any laws intended to implement the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, each as amended or updated from time to time.

3.16.12 Export Control. Each Party will comply with all export control and economic sanctions laws applicable to its performance under the Cloud Agreement. Client agrees that Client will not, and will procure that Users do not, use the Cloud Services in or in relation to any activities involving a country subject to comprehensive economic sanctions (including without limitation Cuba, Iran, North Korea, Sudan, Syria or the Crimea region of Ukraine), or involving a party in violation of such applicable trade control laws, or that require government authorization, without first obtaining the written consent of Accenture and the required authorization. For the avoidance of doubt, Client shall not grant access to the Cloud Services to any individual, entity or organization that is subject to trade sanctions or embargos by the United States, or to any applicable jurisdiction, individual, entity or organization that is listed on the OFAC Specially Designated Nationals List from time to time.

3.17 Governing law, jurisdiction and dispute resolution

3.17.1 The Cloud Agreement shall be governed by and construed in accordance with the laws of England.

3.17.2 The Parties will make good faith efforts to resolve within thirty (30) days any dispute in connection with the Cloud Agreement by escalating it to higher levels of management. Notwithstanding any dispute, each Party shall continue all of its obligations under the Cloud Agreement. In the event that Client does not pay an amount equal to or greater than two (2) months' average fees under any Cloud Agreement, then Accenture will be permitted to suspend the Cloud Services until such time as the matter in dispute is resolved.

3.17.3 Any dispute arising out of or in connection with the Cloud Agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration in accordance with the London Chamber of International Arbitration ("LCIA"). Any arbitration will be conducted on an individual, rather than a class-wide, basis. The seat of the arbitration shall be London, England. The tribunal shall consist of three arbitrators, with each Party selecting one arbitrator and the third selected by the LCIA. The language of arbitration shall be English. The Parties will be entitled to engage in reasonable discovery, including requests for production of relevant non-privileged documents. Depositions and interrogatories may be ordered by the arbitral panel upon a showing of need. All decisions, rulings, and awards of the arbitral panel will be made pursuant to majority vote of the three arbitrators and shall be final. The award will be in accordance with the applicable law, will be in writing, and will state the reasons upon which it is based. The arbitrators will have no power to modify or abridge the terms of this Agreement.

4. Appendix A – Definitions

"**Client Content**" means any software, content, materials, data and information supplied by Client to Accenture under the Cloud Agreement, including but not limited to any Personal Data (if applicable);

"**Cloud Service(s)**" means cloud services that may be provided by Accenture under a Cloud Agreement;

"**Cloud Vendor**" means a third-party cloud service provider, providing a Cloud Vendor Solution, as identified in the relevant Service Specific Terms;

"**Cloud Vendor Solutions**" means a cloud service identified in the relevant Service Specific Terms that is provided by a Cloud Vendor and that forms a component of the Cloud Services provided by Accenture;

"**Confidential Information**" means information (in any form) that relates to the other Party and its activities that is identified by the disclosing Party as confidential or that might be considered as such (and which shall include the terms of the Cloud Agreement, including pricing);

"**Data Controller**" means the entity that determines the purposes and means of the processing of Personal Data;

"**Data Processor**" means the entity that processes Personal Data on behalf of the Data Controller; "**Fees**" means all amounts (including fees, expenses and applicable taxes) payable by Client under the Cloud

Agreement;

"**IPR**" or "**Intellectual Property Rights**" means any rights, title and interest in patents, trademarks, service marks, trade and business names, rights in design, utility models, copyright, database rights, know-how (including trade secrets) and any other similar right whether presently existing, applied for or in relation to which there is a right to apply for registration and any analogous rights to any of the preceding rights under any other jurisdiction;

"**Party"** or **"Parties**" means Accenture and/or Client;

"**Personal Data**" means any Client Content that identifies or directly relates to natural persons as may be further defined in applicable data privacy law;

"**User**" means any individual or entity that the Parties agree in Service Specific Terms may access or use the Cloud Services; and

"Virus" means any item, software, device or code which is intended by any person to, or which is likely to, or which may:

(a) impair the operation of any software or computer systems;

(b) cause loss of, or corruption or damage to any software or computer systems or data;

(c) prevent access to or allow unauthorised access to any software or computer system or data; and/or

(d) damage the reputation of Client and/or Accenture, including any computer virus, Trojan horse, worm, software bomb, authorization key, license control utility or software lock.

5. Service Specific Terms - Amazon Web Services (AWS)

1. **Order of Precedence.** These Service Specific Terms for AWS (**"AWS Specific Terms"**) complement the General Accenture Cloud Terms and form a part of the Cloud Agreement. These AWS Specific Terms govern the provision and consumption of AWS Services only (as defined below). In the event of any conflict or inconsistency between these AWS Specific Terms and the General Accenture Cloud Terms, these AWS Specific Terms shall prevail to the extent of the conflict or inconsistency.

2. **Definitions.**

   "Acceptable Use Policy" means the policy available at http://aws.amazon.com/aup, as may be updated by AWS from time to time.

   "AWS" means Amazon Web Services, Inc. or its affiliates. "**AWS Customer Agreement**" means AWS' standard user agreement posted on the AWS Site. "**AWS Network**" means AWS' data center facilities, servers, networking equipment and host software systems (e.g., virtual firewalls) that are within AWS' control and are used to provide the AWS Services. **"AWS Services"** means each of the public cloud and other services made available by AWS that Accenture procures from AWS for the purposes of making the same available to Client.

   "AWS Service Terms" means the rights and restrictions relating to particular AWS Services located at http://aws.amazon.com/serviceterms, as may be updated by AWS from time to time. **"AWS Site"** means http://aws.amazon.com, as may be updated by AWS from time to time.

   "Service Level Agreement" or "SLA" means all service level agreements that AWS offers with respect to AWS Services, and which AWS posts at https://aws.amazon.com/legal/service-level-agreements/, as may be updated by AWS from time to time.

3. **AWS Services.** Accenture shall procure and provide AWS Services to Client, as more particularly defined in the SOW. Client acknowledges and agrees that Accenture can only provide and make AWS Services available to Client subject to the terms and conditions that AWS makes AWS Services available to the public. To the extent applicable, such terms (including the AWS Customer Agreement and AWS Service Terms) have been reflected and incorporated in these AWS Specific Terms and in the General Accenture Cloud Terms. Client acknowledges and agrees that in relation to AWS Services, Client shall not have any direct access to the root credentials, but Client will have access to AWS' administrative consoles (except for AWS' Billing Management Console).

4. **Acceptable Use Policy**. Client's access and use of the Cloud Services shall be subject to the Acceptable Use Policy. Client is solely responsible for monitoring any changes to the Acceptable Use Policy and for ensuring that its own, its affiliates' and its Users' access and use of the Cloud Services comply with the Acceptable Use Policy. Any violation of such policy may lead to suspension of the Cloud Services in accordance with Sections 4.1 and 4.2 of the General Accenture Cloud Terms.

5. **Service Level Agreement**. AWS shall provide the AWS Services in accordance with the applicable Service Level Agreement and the Service Level Agreement shall form a part of the Cloud Agreement as far as the relevant AWS Services are concerned. Client acknowledges and agrees that AWS has reserved the right to make changes to, replace and discontinue the applicable Service Level Agreement from time to time, but any such change, discontinuation or addition that will materially reduce the benefits offered to Client will only apply ninety (90) days after the effective date of such change, discontinuation or addition.

6. **Hosting of Client Content**. AWS' cloud infrastructure is built around regions and availability zones. AWS regions provide multiple, physically separated and isolated availability zones, as further described at https://aws.amazon.com/about-aws/global-infrastructure/?nc2=h_l2_cc. Client may specify the location(s) where Client Content will be hosted and, once Client has made its choice, AWS will not transfer Client Content from Client's selected region(s) without first notifying Client, unless necessary to comply with law or a valid and binding order of a law enforcement agency (such as a subpoena or court order).

7. **Processing of Client Content**. Accenture has entered into a data processing agreement (**"DPA"**) with AWS that aligns with the requirements of the General Data Protection Regulation (**"GDPR"**), and which also includes EU Model Clauses, which were approved by the European Union (**"EU"**) data protection authorities, known as the Article 29 Working Party. A copy of the AWS GDPR DPA is available at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf (or at such other location as may be

updated from time to time). The AWS GDPR DPA shall form a part of the Cloud Agreement insofar that the AWS Services are concerned, and AWS shall comply with them when acting as a data processor for Client.

8. **Compliance Program and Accreditations**. Information on AWS' compliance program, certifications and accreditation is available at https://aws.amazon.com/compliance/programs/. These include but are not limited to: (a) ISO 27001 by an Accredited Registrar, (b) Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS) for specified cloud environments (set out at

   http://aws.amazon.com/compliance/), which require procurement of the appropriate service, including any associated costs, (c) FedRAMP authorization from the U.S. Department of Health and Human Services for specified cloud environments (set out at http://aws.amazon.com/compliance/), which require procurement of the appropriate service, including any associated costs, and (d) SOC 1 Report and SOC 2 Report.

   Accenture will provide Client at least thirty (30) days' prior notice if, during the Term, Accenture knows that AWS will (a) not seek recertification as compliant with ISO 27001 (or a substantially equivalent standard), (b) not seek to be validated as compliant as a Level 1 service provider under the PCI-DSS (or a substantially equivalent standard), (c) not seek to maintain FedRAMP compliance (or a substantially equivalent standard) or (d) no longer maintain the controls described in the SOC 1 Report or the SOC 2 Report (or a substantially equivalent standard).

9. **Security.** AWS shall provide the AWS Services in accordance with the AWS Security Standards attached hereto as **Attachment A**. Client acknowledges that AWS reserves the right to modify the AWS Security Standards from time to time, provided that AWS continues to provide at least the same level of security as described in the AWS Security Standards.

10. **Security Audit Reports**. AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the AWS Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards (or other substantially equivalent alternative standards); (c) will be performed by independent third party security professionals at AWS' selection and expense; and (d) will result in a confidential summary concerning the audit results (**"Summary Report"**) so that Client can reasonably verify AWS' compliance with the security obligations under these AWS Specific Terms.

11. **[Encryption and Security Architecture Requirements**. Client shall comply with the Encryption and Security Architecture Requirements attached hereto as **Attachment B** unless otherwise specified in the SOW.

6. Attachment A - Security Standards

1. **Information Security Program**. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Client secure Client Content against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:
2. **Network Security**. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Cloud Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and User, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incidence response plans to respond to potential security threats.
3. **Physical Access Controls**. Physical components of the AWS Network are housed in nondescript facilities (**"Facilities"**). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.
4. **Limited Employee and Contractor Access**. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the assigned access privileges, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.
5. **Physical Security Protections**. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.
6. **Pre-Employment Screening**. AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees and contractors commensurate with the employee's or contractor's position and level of access to the Facilities. AWS will not permit an employee or contractor to have access to non-public Client Content or perform material aspects of the Cloud Services if such employee or contractor has failed to pass such background check.
7. **Continued Evaluation.** AWS will conduct periodic reviews of the security of the AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of the AWS Network and associated Cloud Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.
8. **Security Incident Notification.** "Security Incident" means a breach of AWS' security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Content. Accenture will notify Client of a Security Incident in accordance with any security breach notification laws applicable to Accenture and take any commercially reasonable measures within its control to mitigate the effects and to minimise any damage resulting from the Security Incident. Accenture's obligation to report or respond to a security breach is not to be construed as any admission by Accenture or AWS of any fault or liability with respect to the Security Incident.

7. Attachment B - Encryption and Security Architecture Requirements

At all times Client will comply with the following Encryption Requirements:

1. Client will encrypt all Client Content in transit by using SSL/TLS or other industry-standard encryption mechanisms.
2. Client will protect Client Content at rest as follows:
    a. At all times Client Content at rest will be encrypted using industry-standard encryption mechanisms.
    b. Client will implement cryptographic key management procedures sufficient to appropriately secure key material.
    c. Unencrypted Client Content will not be utilized as metadata or as parameters for configuring Cloud Services.
    d. Unencrypted Client Content will not be stored as part of an Amazon Machine Image.
    e. Client will not store account credentials as part of an Amazon Machine Image.

At all times Client will comply with the following Security Architecture:

3. Client will utilize all published security best practices in the Security Best Practices document available at http://aws.amazon.com/security/security-resources/. Client will comply with any updates or changes to the security best practices described above as soon as reasonably practicable (and in any event not later than sixty (60) days) following such update or change.
4. For all Cloud Services processing Client Content, Client will use Amazon Virtual Private Cloud when available.
5. AWS shall provide AWS Identity and Access Management ("**IAM**") in accordance with the AWS Service Terms. Client will not use root account credentials beyond initial account configuration of IAM, except for Cloud Services for which IAM is not available.
6. Client will manage multiple Users and their permissions with IAM or Security Token Service as follows:
    a. Use the principle of least privilege.
    b. The privileges granted to Users, groups, and secure tokens will be no more than the minimal privileges necessary.
    c. Every User will have unique security credentials.
    d. All security credentials will be regularly rotated, no less than quarterly.
    e. All AWS management console authentications will be via IAM Users using multifactor authentication or utilizing federated credentials.
7. Access limitation: Client will minimize permissions in Security Groups and Access Control Lists (both as described on the AWS Site) only to those Users required for the operation of Client's services. Client will minimize source and destination authorizations permitted to solely those required for the operation of Client's services.

8. Service Specific Terms - Microsoft Azure (Azure)

1. **Order of Precedence.** These Service Specific Terms for Azure **("Azure Specific Terms")** complement the General Accenture Cloud Terms and form a part of the Cloud Agreement. These Azure Specific Terms govern the provision and consumption of Azure Services only (as defined below). In the event of any conflict or inconsistency between these Azure Specific Terms and the General Accenture Cloud Terms, these Azure Specific Terms shall prevail to the extent of the conflict or inconsistency.
2. **Definitions.**

   "Acceptable Use Policy" means the acceptable use policy set forth in the Online Services Terms.

   "Azure Services" means the Microsoft services and features identified at http://azure.microsoft.com/services/ (except those licensed separately) and made available by Microsoft that Accenture procures from Microsoft for the purposes of making the same available to Client. "Azure Services" includes any open source components incorporated by Microsoft in those services and features.

   "Microsoft" means Microsoft Corporation, or its affiliates.

   "Online Services Terms" means the additional terms that apply to Client's use of Azure Services, published at https://www.microsoft.com/en-gb/Licensing/product-licensing/products.aspx, as may be updated by Microsoft from time to time.

   "Service Level Agreement" or "SLA" means the relevant service level agreement that Microsoft offers for the applicable Azure Services, published at https://www.microsoft.com/en-gb/Licensing/productlicensing/products.aspx, as may be updated by Microsoft from time to time.
3. **Azure Services.** Accenture shall procure and provide the Azure Services to Client, as more particularly defined in the SOW. Client acknowledges and agrees that Accenture can only provide and make the Azure Services available to Client subject to the terms and conditions that Microsoft makes the Azure Services available to the public. To the extent applicable, such terms (including the Online Services Terms) have been reflected and incorporated in these Azure Specific Terms and in the General Accenture Cloud Terms. Client acknowledges and agrees that in relation to Azure Services, Client shall not have any direct access to the root credentials.
4. **Online Services Terms.** The provision of Azure Services, and Client's access and use of the Azure Services, shall be subject to the Online Services Terms. Client agrees that the Online Services Terms form a binding and enforceable part of the Cloud Agreement, as far as Azure Services are concerned. The Online Services Terms in effect when Client orders a new, or renews an existing subscription, will apply to the Azure Services in question, for the applicable subscription term. For Azure Services that are billed periodically based on consumption, the Online Services Terms current at the start of each billing period will apply to usage during that period. Accenture recommends that Client downloads and prints the Online Services Terms for Azure Services in full for future reference.
5. **Acceptable Use Policy**. Client's access and use of the Azure Services shall be subject to the Acceptable Use Policy. Client is solely responsible for monitoring any changes to the Acceptable Use Policy and for ensuring that its own, its affiliates' and its Users' access and use of the Azure Services shall comply with the Acceptable Use Policy. Any violation of such policy may lead to suspension of the Azure Services in accordance with Sections 4.1 and 4.2 of the General Accenture Cloud Terms.
6. **Service Level Agreement**. Microsoft shall provide the Azure Services in accordance with the relevant Service Level Agreement and the Service Level Agreement shall form a part of the Cloud Agreement as far as the relevant Azure Services are concerned. Accenture recommends that Client downloads and prints the Service Level Agreement for Azure Services in full for future reference.
7. **Limited Warranty.** Each Azure Service will perform in accordance with the applicable Service Level Agreement during Client's use. Client's remedies for breach of this warranty are set out in the Service Level Agreement. During the term of each subscription for an Azure Service, Microsoft will provide the Azure Service as described in the Online Services Terms. The remedies above are Client's sole remedies for breach of the warranties in this section. Client waives any breach of warranty claims not made during the warranty period. The aforesaid warranties do not apply to free or trial products, previews and limited offerings. Furthermore, for Azure Services provided free of charge, Accenture's liability is limited to direct damages finally awarded up to US$5,000.

8. **Compliance and Certifications.** Microsoft's existing compliance certifications for Azure Services can be found in the Online Services Terms and the most current certifications have been listed at http://azure.microsoft.com/en-us/support/trust-center/. For the avoidance of doubt, nothing in this section shall apply to or modify Accenture's obligations with respect to any data processing or security provisions agreed between Accenture and Client.
9. **Data Protection Terms.** Azure Services shall be subject to the Data Protection Terms set out in the Online Services Terms. Client acknowledges and agrees that (i) Accenture will be the primary administrator of the Azure Services for the term of the applicable Cloud Agreement, and that Accenture will have administrative privileges and access to Client Content, however, Client may request additional administrator privileges from Accenture; (ii) Client can, at its sole discretion and at any time during the term of the Cloud Agreement, terminate Accenture's administrative privileges; and (iii) Accenture may collect, use, transfer, disclose and otherwise process Client Content, including Personal Data. Client consents to Accenture providing Microsoft with Client Content and information that Client provides to Accenture for purposes of ordering, provisioning and administering the Azure Services. Client appoints Accenture as its agent for purposes of interfacing with and providing instructions to Microsoft for purposes of this Section 9.

   Accenture's privacy practices with respect to Client Content or any services provided by Accenture are subject to the terms of Client's agreement with Accenture and may differ from Microsoft's Data Protection Terms included in the Online Services Terms; the commitments made in the Online Services Terms only apply to the Azure Services purchased under the Cloud Agreement. If Client uses software or services that are hosted by Accenture, that use will be subject to Accenture's privacy practices, which may differ from Microsoft's.
10. **Subprocessors.** Client acknowledges and agrees that Microsoft may hire third parties to provide limited or ancillary services on its behalf and Client consents to the engagement of these third parties and Microsoft affiliates as subprocessors. The above authorizations constitute Client's prior written consent to subcontracting by Microsoft of the processing of Client Content and any Personal Data contained therein, if such consent is required under the Standard Contractual Clauses or General Data Protection Regulation (GDPR) terms. Additional terms concerning such subprocessors are set out in the Online Services Terms. Further details regarding who can access Client Content hosted and processed on Azure Services is provided at https://www.microsoft.com/en-us/trustcenter/Privacy/Who-can-access-your-data-and-on-whatterms.
11. **Security Incident Notification**. If Accenture becomes aware of a Microsoft breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Content while processed by Microsoft (each a **"Security Incident"**), Accenture will promptly (1) notify Client of the Security Incident; (2) investigate the Security Incident and provide Client with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Client is solely responsible for complying with its obligations under incident notification laws applicable to Client and fulfilling any third-party notification obligations related to any Security Incident. Accenture's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Accenture or Microsoft of any fault or liability with respect to the Security Incident. Client must notify Accenture and Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Azure Services.
12. **Hosting of Client Content.** Client Content and Personal Data that Microsoft processes on Client's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its subprocessors operate. Client appoints Microsoft to perform any such transfer of Client Content and Personal Data to any such country and to store and process Client Content and Personal Data to provide the Azure Services. Microsoft will store Client Content at rest within certain major geographic areas (each a **"Geo"**) as follows: If Client configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Client Content at rest within the specified Geo. Certain services may not enable Client to configure deployment in a particular Geo or outside the United States and may store backups in other locations, as detailed in the Microsoft Trust Center (which Microsoft may update from time to time, but Microsoft will not add exceptions for existing services in general release). Usage of data centers in certain regions may be restricted to Clients located in or near that region. For information on Microsoft service availability by region, please refer to http://azure.microsoft.com/enus/regions.

9. Service Specific Terms - Google Cloud (Google)

1. **Order of Precedence.** These Service Specific Terms for Google (**"Google Specific Terms"**) complement the General Accenture Cloud Terms and form a part of the Cloud Agreement. These Google Specific Terms govern the provision and consumption of GCP Services only (as defined below). In the event of any conflict or inconsistency between these Google Specific Terms and the General Accenture Cloud Terms, these Google Specific Terms shall prevail to the extent of the conflict or inconsistency.

2. **Definitions.** "**Acceptable Use Policy**" means the acceptable use policy available at https://cloud.google.com/terms/aup, as may be updated by Google from time to time.

   "Data Processing and Security Terms" means the policy available at https://cloud.google.com/terms/data-processing-terms, as may be updated by Google from time to time. "**GCP Services**" means the services set forth at: https://cloud.google.com/terms/services (including any associated APIs). "**Google**" means Google LLC or its affiliates.

   "**Google Service Terms**" means the rights and restrictions for particular GCP Services, available at https://cloud.google.com/terms/service-terms, as may be updated by Google from time to time.

   "**Service Level Agreement**" or "**SLA**" means the relevant service level agreement that Google offers for the GCP Services, available at https://cloud.google.com/terms/sla/, as may be updated by Google from time to time.

3. **GCP Services**. Accenture shall procure and provide the GCP Services to Client, as more particularly defined in the SOW. Client acknowledges and agrees that Accenture can only provide and make the GCP Services available to Client subject to the terms and conditions that Google makes GCP Services available to the public. To the extent applicable, such terms (including the Google Service Terms) have been reflected and incorporated in these Google Specific Terms and in the General Accenture Cloud Terms. Client acknowledges and agrees that in relation to GCP Services, Client shall not have any direct access to the root credentials.

4. **Google Service Terms.** The provision of GCP Services, and Client's access and use of the GCP Services, shall be subject to the Google Service Terms. Client agrees that the Google Service Terms form a binding and enforceable part of the Cloud Agreement, as far as GCP Services are concerned.

5. **Acceptable Use Policy**. Client's access and use of the GCP Services shall be subject to the Acceptable Use Policy. Client is solely responsible for monitoring any changes to the Acceptable Use Policy and for ensuring that its own, its affiliates' and its Users' access and use of the GCP Services shall comply with the Acceptable Use Policy. Any violation of the Acceptable Use Policy may lead to suspension of the GCP Services in accordance with Sections 4.1 and 4.2 of the General Accenture Cloud Terms. Client agrees that if Google has a good faith belief that Client Content violates the Acceptable Use Policy, then in addition to any other rights Google or Accenture might have under the Cloud Agreement, Google may review such Client Content solely to confirm compliance with the Acceptable Use Policy.

6. **Additional Restrictions.** Client agrees that it shall not (and shall ensure that its Users shall not) (i) use the GCP Services to create, train or improve a substantially similar product or service, including any other machine translation engine; (ii) process or store any Client Content that is subject to the International Traffic in Arms Regulations maintained by the Department of State; or (iii) use the GCP Services to operate or enable any telecommunications service or in connection with any application that allows Users to place calls or to receive calls from any public switched telephone network.

7. **Documentation**. Accenture and/or Google may provide Client developer guides, user guides, instructions, specifications, descriptions and other technical and operational manuals related to the GCP Services ("**Documentation**"). Client agrees that it shall comply with any requirements or restrictions set forth in any such Documentation. "Documentation" includes all modifications, revisions, additions and/or other changes to the Documentation.

8. **Service Level Agreement**. Google shall provide the GCP Services in accordance with the relevant Service Level Agreement and the Service Level Agreement shall form a part of the Cloud Agreement as far as the relevant GCP Services are concerned. Accenture recommends that Client downloads and prints the Service Level Agreement for GCP Services in full for future reference.

9. **Security**. Google will take and implement the security measures set out at https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures. Client acknowledges and agrees that Google may update or modify such security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the GCP Services.
10. **Location of Client Data**. Except as otherwise agreed in these Google Specific Terms, Google may process and store Client Content in the United States or any other country in which Google or its agents maintain facilities.
11. **Processing of Client Data**. To the extent that Google processes Client Content which contains personal data (as defined in Regulation (EU) 2016/679 of 27 April 2016, General Data Protection Regulation ("GDPR")) under the Cloud Agreement, it shall implement and maintain sufficient technical and organisational measures designed to safeguard such personal data (published at https://cloud.google.com/security/). Accenture has further entered into an agreement with Google that incorporates the EU Standard Contractual Clauses, , for the transfer of personal data outside of the EEA. Google shall comply with its obligations under such EU Standard Contractual Clauses, whether acting as a data processor or sub-processor. Google will (taking into account the nature of the processing of Client personal data and the information available to Google) process Client personal data under the General Data Protection Regulation (GDPR) as set forth in the Data Processing and Security Terms.
12. **Data Incident Notification**. If Accenture becomes aware of a Data Incident as notified by Google, Accenture will: (a) notify Client of the Data Incident promptly after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Client Content. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Google recommends Client take to address the Data Incident. Google will not assess the contents of Client Content in order to identify information subject to any specific legal requirements. Without prejudice to Google's obligations under this section, Client is solely responsible for complying with incident notification laws applicable to Client and fulfilling any third party notification obligations related to any Data Incident(s). Accenture's notification of or response to a Data Incident under this section will not be construed as an acknowledgement by Accenture or Google of any fault or liability with respect to the Data Incident. "Data Incident" means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Content on systems managed by or otherwise controlled by Google. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Client Content, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

10. SAP Cloud Services Agreement

SAP Cloud Services Agreement

Dated [DATE]

This Agreement will be effective if fully executed on or before: XX

Between	**ACCENTURE UK LIMITED** (Company Number 04757301) of 30 Fenchurch Street, London, EC3M 3BD (**Accenture**)
And	**[xxxxxxx]** (Company Number XXX) of [ADDRESS] **(Customer)**

PREAMBLE

A) Accenture is a Value Added Reseller for SAP (UK) Limited Clockhouse Place, Bedfont Road, Feltham TW14 8HD (**SAP**) and is authorised to promote and market SAP Cloud Services for and on behalf of SAP.

B) Customer wishes to acquire the right to use SAP Cloud Services and wishes for Accenture to procure the same.

C) Customer acknowledges that the right to use the SAP Cloud Service procured pursuant to this Agreement shall be subject to SAP's terms and conditions as referenced herein.

Terms

1. Accenture and Customer agree that this is a binding agreement for Cloud Services (as further detailed in the SOW) (**Cloud Service**).
2. All Cloud Services ordered pursuant to this Agreement are subject to ultimate acceptance by SAP (or its Affiliates), and once accepted shall be non-cancellable, non–revocable, and non-transferable.

USE OF CLOUD SERVICES

3. Customer's use of the Cloud Service is at all times governed by and subject to the documents in effect as of the effective date of this Agreement applicable to the Cloud Service, as follows: i) Product-specific supplement terms (**Supplement**); ii) Support Policy for SAP Cloud Services iii) Service Level Agreement for SAP Cloud Services

   iv) Personal Data Processing Agreement for SAP Cloud Services (**DPA**) v) General terms and conditions for SAP Cloud Services (UK) (**GTC**).

Jointly the **"SAP Terms"**.

All references in the Supplement(s) to "Services" mean "Cloud Service", and "Named Users" mean "Authorised Users".

4. Copies of the SAP Terms may be found at http://www.sap.com/about/agreements.html. Customer acknowledges that it has had the opportunity to read the SAP Terms.
5. Customer acknowledges and accepts that it is required to sign a Cloud EULA Acceptance form for Cloud Services (EULA Acceptance) (as between Customer and SAP), which shall incorporate the SAP Terms in order to use the Cloud Service.
6. Customer will not be permitted access to the Cloud Service until it provides Accenture with a duly signed EULA Acceptance.
7. SAP may, at its discretion, decline to grant Customer a license to use the Cloud Service, in which case this Agreement shall be terminated with immediate effect.

FEES

8. In consideration for the procurement and delivery of the Cloud Service Customer shall pay Accenture the fees stated in the SOW, which shall be invoiced quarterly in advance.

9. Subject to receipt of payment from Customer Accenture shall pay SAP for the delivery of the Cloud Service pursuant to its commercial arrangement directly with SAP. If Customer fails to pay any fee or other amount payable to Accenture by its due date the Cloud Service may, at Accenture or SAP's discretion, suspend or stop providing the Cloud Service.
10. Customer shall pay all invoices net thirty (30) days from date of each invoice.
11. All fees set forth herein do not include VAT and are in GB Pounds (£). Customer is responsible for payment of its own taxes in connection with this Agreement.
12. Accenture reserves the right to increase the fees for the Cloud Service upon 3 months' notice prior to the beginning of each Renewal Term by a sum which shall not exceed the percentage increase in the Retail Price Index in the preceding contract year. Not raising fees shall not be deemed a waiver of Accenture's rights to increase fees.

Subscription term

13. The Cloud Service shall be delivered during the period specified in the SOW (**Initial Term**), unless terminated sooner in accordance with the SAP Terms.
14. Unless stated otherwise in the Supplement or the SOW, after the Initial Term, the subscription term for the relevant Cloud Service shall be automatically extended for subsequent periods of one year (each a **Renewal Term**).
15. Auto-renewal will not occur if Customer notifies Accenture in writing of its intention not to renew at least 100 days in advance of expiration of the then current Initial or Renewal Term.

Excess use

16. Customer's use of the Cloud Service is subject to the terms of the Agreement, including the usage metrics specified in the SOW. Any use of the Cloud Service that exceeds this scope will be subject to additional fees. Fees accrue from the date the excess use began. Customer will execute an additional Cloud Service Agreement to cover subscriptions for additional usage metrics and their volume. Accenture may invoice and the Customer will pay for excess used based on SAP's price list on the date that the excess usage began in any event.

General

17. Notwithstanding any provision of the SAP Terms, nothing shall affect Accenture's right to collect fees owed in connection with this Agreement.
18. Unless otherwise set out in this Agreement, all prices and other terms and conditions contained in this Agreement relate to this Agreement alone, and will not apply to any other Agreement or to any use of any software or subscription in excess of Customer's permitted use under this Agreement.
19. Save in relation to clause 17 above, where the terms of this Agreement conflict with the SAP Terms with regard to Customer's right to use the Cloud Services, the SAP Terms will prevail.
20. The Agreement constitutes the entire and exclusive agreement between the parties with respect to the Cloud Services identified in the SOW and supersedes any and all prior agreements and understandings, whether written or oral, that may exist between the parties with respect to the subject matter of this Agreement or any part thereof. The parties agree that no side agreements exist.
21. Roadmap information, RFP, Statement of Directions, or other forward looking presentations are not part of any agreement with Accenture and/or SAP; and neither Accenture nor SAP has any obligation to pursue any course of business outlined in those materials or to develop or release any functionality mentioned in that material. That material and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice.
22. The Agreement shall be governed by and construed in accordance with the laws of England.
23. Customer warrants that the person signing this Agreement and the EULA Acceptance is duly authorised and has full legal capacity to bind Customer.

Signed for and on behalf of Customer:	**Signed for and on behalf of Accenture UK Limited:**
……	……
Print Name: ……...	Print Name: ……...
Position: ……..……...	Position: ……..……...
Date: ……..…….....	Date: ……..…….....

11. Data Ingestion Terms Addendum

[Due to constraints in uploading multiple documents, we have consolidated these into one document. This document will apply to all offerings where data ingestion is in scope]

1. **Agreement.** This is an attachment ("Attachment") to the Statement of Work [insert SOW name and/or number] dated [insert date] ("SOW") under the Agreement between the parties dated [insert date]

("Agreement"). Capitalized terms in this Addendum have the same meanings as in the Agreement or in the additional definitions in section 8 below, as applicable. In the event of a conflict between the terms and conditions of this Addendum and the terms and conditions of either the Agreement or the SOW, the terms and conditions of this Addendum will govern.

2. **Platform.** Accenture will use the Platform hosted in the cloud by Accenture's Cloud Service Vendor (CSV) in connection with the services described in the SOW.

3. **Client Content.** Client grants to Accenture a non-exclusive license to use the Client Content in connection with the services, including importing such Client Content into the Platform and processing such Client Content via the Platform. Accenture will use the Client Content for the purpose of providing the services. Reasonable and appropriate technical and organizational security measures intended to safeguard Client Content against accidental, unauthorized or unlawful access, loss, damage or destruction ("Security Standards") will be implemented, and Accenture will provide Client with details of such Security Standards upon request.

   Provided Accenture complies with the Security Standards, Accenture will not be liable in the event of a Security Incident. Notwithstanding anything to the contrary in the Agreement or the SOW, a Security Incident shall not be deemed to be a violation of Accenture's confidentiality obligations. Client has collected and shall maintain and handle all Client Personal Information contained in Client Content in compliance with all applicable data privacy and protection laws, rules and regulations. Client authorizes Accenture to process Client Personal Information in accordance with the Data Processing and Security Addendum. Client warrants that it has provided all required notices, has a lawful basis and/or obtained all required consents and/or authorizations, and registrations to disclose and transfer any Client Personal Information to Accenture and for the use of such Client Personal Information in manner contemplated by this Addendum and the relevant SOW. Client warrants that Client provides Client Content that complies with all applicable laws and that such Client Content does not infringe the intellectual property rights of any third party. Client will promptly notify Accenture of any failure to comply with these requirements and will defend, indemnify, and hold harmless Accenture and its Affiliates from and against any Losses arising out of or relating to any claim arising out of such failure. Client also agrees not to deliver any files to be included in Client Content that contain viruses, malicious files or other harmful code or any other similar software that may access or damage the operation of the Platform, the Outputs or another's computers. Client is solely responsible for the accuracy and content of Client Content. Client consents to the processing of Client Content in, and transfer of Client Content into, the CSV data centres. Accenture's licensors are third party beneficiaries under the terms of this Addendum for enforcement purposes.

4. **Ownership.** Client may retain all Outputs that Accenture creates for Client using the Platform and Client may use such Outputs for Client's internal business purposes in perpetuity. Client is responsible for obtaining any underlying software (such as Tableau Reader) that may be necessary to display the content of the Outputs on Client's computer. As between Client and Accenture, Accenture owns all intellectual property rights in the Platform and in any improvements, enhancements and derivative works thereof. As between Client and Accenture, Client owns all intellectual property rights in the Client Content.

5. **Disclaimer.** The Outputs are made available "as is" without warranty of any kind, whether express, implied or statutory. Accenture, its Affiliates and its licensors make no representations and provide no warranties of any kind, whether express, implied, statutory or otherwise, regarding the Outputs. Accenture, its Affiliates and its licensors expressly disclaim all warranties, express, implied, statutory or otherwise, including any implied warranties of satisfactory quality, fitness for a particular purpose, or non-infringement, any warranties arising out of any course of dealing or usage of trade, and any warranties of fitness for high-risk activities. These disclaimers shall only apply to the extent permitted by applicable law. Client acknowledges that Accenture does not control the transfer of data over the internet or any public telecommunications network, and so cannot be responsible for any loss or corruption of Client Content during such transmission.

6. **Limitation of Liability.** Accenture's liability with respect to Client Content and the Outputs is subject to the same limitation of liability as provided for in the Agreement and the SOW, as applicable.
7. **Reservation of Rights.** All rights not expressly granted to Client are reserved to Accenture and its licensors. The Platform, including any underlying hardware or other infrastructure, may be provided by Accenture, Accenture Affiliates, or third-party subcontractors under contract to Accenture.
8. **Business Contact Information.** Each party consents to the other party using its Business Contact Information for contract management, payment processing, service offering, and business development purposes related to this Agreement and such other purposes as set out in the using party's global data privacy policy (copies of which shall be made available upon request). For such purposes, and notwithstanding anything else set forth in this Addendum with respect to Client Personal Information in general, each party shall be considered a controller with respect to the other party's Business Contact Information and shall be entitled to transfer such information to any country where such party's global organization operates.
9. **Definitions.**
    - **Client Content** means all content, materials, data and information that is provided by or on behalf of Client for processing, analysis and display via the Platform.
    - **Client Personal Information** means Client-owned or controlled personal information (i.e. which names or identifies a natural person) provided to Accenture by or on behalf of Client in connection with this Addendum, in the form of Client Content. Unless prohibited by applicable Data Privacy Laws, Client Personal Information shall not include information or data that is anonymized, aggregated, de-identified and/or compiled on a generic basis and which does not name or identify a specific person.
    - **Consents** means all necessary consents, permissions, notices and authorizations necessary for Accenture to provide the AIP, including any of the foregoing from Client employees or third parties; valid consents from or notices to applicable data subjects; and authorizations from regulatory authorities, employee representative bodies or other applicable third parties.
    - **Data Privacy Laws** all applicable laws, regulations and regulatory guidance in relation to the processing or protection of Personal Information, as amended from time-to-time, including but not limited to, Regulation (EU) 2016/679 of 27 April 2016, General Data Protection Regulation ("GDPR").
    - **CSV** means the Cloud Service Vendor, Amazon Web Services.
    - **Losses** means any claims, damages, losses, liabilities, costs and expenses (including reasonable legal fees).
    - **Outputs** means downloadable files consisting of visualizations, charts, graphs, reports or other data displayed or produced via the Platform but excluding software and Client Content.
    - **Platform** means a hosted analytics solution used by Accenture to provide the services, as detailed in the applicable CCN. Platform includes any modifications, enhancements, additions, extensions, translations and derivative works of Platform or its any of its components, any programming code and other associated technologies related to Platform. Platform does not include Client Content or any Client-provided proprietary or third-party software;
    - **Security Incident** means a failure by Accenture to comply with the Security Standards, where such failure results in the unauthorized access to or acquisition of any unencrypted record in Accenture's control containing Client Content in a manner that renders misuse of the Client Content reasonably possible. For the avoidance of doubt, Security Incident does not include any of the following that results in no unauthorized access to Client Content or to any Accenture or CSV systems storing Client Content: (a) pings and other broadcast attacks on firewalls or edge servers, (b) port scans, (c) unsuccessful log-on attempts, (d) denial of service attacks, (e) packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers), or (f) similar incidents.

AGREED TO BY:
ACCENTURE (UK) LIMITED

By: _____

Name: _____

Title: _____

Date: _____

AGREED TO BY:
Client: _____

By: _____

Name: _____

Title: _____

Date: _____

12. ServiceNow Terms and Conditions

ServiceNow Schedules

https://www.servicenow.com/schedules.html

ServiceNow Subscription Agreement

https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/servicenowsubcription-service-agreement.pdf

13. Accenture Sales Contract

[Due to constraints in uploading multiple documents, we have consolidated these into one document. In the event of resale of third-party products these terms and conditions would apply]

This Accenture Sales Contract ("Agreement") dated _____, 20__ (the "Effective Date") is made by and between Accenture (UK) Limited ("Accenture") and _____ ("Client") and will govern Client's purchase of Products and Services (both defined below) from Accenture (each a "Party" and collectively, the "Parties") in the United Kingdom.

1. **Products and Services Resale**. Accenture and Accenture Affiliates (as defined below) have relationships with third party product and services vendors ("Third Party Suppliers"). Accenture resells the Third Party Supplier's products ("Products") and/or services ("Services"). All Products and Services are provided subject to the Third Party Supplier's applicable terms, which shall constitute an agreement between Client and the Third Party Supplier only, and not Accenture. Third Party Suppliers are independent contractors and shall not be deemed Accenture Affiliates or employees, agents, subcontractors, authorized representatives, partners or joint venturers of Accenture. An Accenture Affiliate is any entity, whether incorporated or not, that is under common control with Accenture. As used in this definition, "control" (and variations thereof) shall mean the existing ability, whether directly or indirectly, to direct the affairs of another by means of ownership, contract or otherwise.
2. **Sales Quotations.** Products and Services purchased by Client hereunder will be listed on the sales quotation(s) issued by Accenture to Client (each, a "Sales Quotation"). Accenture will order the Products and Services specified on each Sales Quotation that has been accepted by both Client and Accenture. Client accepts a Sales Quotation by signing the Sales Quotation or by issuing a purchase order for the Products or Services listed in the Sales Quotation. Accenture confirms its acceptance of a Sales Quotation to the extent that Accenture orders Products or Services pursuant to such Sales Quotation. Any term, condition or proposal submitted by Client in a purchase order or otherwise (whether orally or in writing) that is inconsistent with or in addition to the applicable Sales Quotation or the terms and conditions of this Agreement will be of no force or effect, unless otherwise agreed in writing.
3. **Prices and Payment.** Accenture will invoice Client in the primary local currency of Accenture (unless stated otherwise in the Sales Quotation). Client agrees to pay as invoiced the total purchase price for the Products and Services agreed in the Sales Quotation, plus Taxes (as defined in Section 4) and applicable delivery and insurance charges. Payment in full is due within 30 days of an invoice date. Interest on any payment past due will accrue at the lower of the rate of 1.5% per month or the maximum rate allowed by law. Client will be responsible for Accenture's costs of collection for any payment default, including, but not limited to, court costs, filing fees and reasonable attorneys' fees.
4. **Taxes.** Applicable taxes will be billed as a separate item on invoices and any taxes paid on behalf of Client by Accenture will be identified on the applicable invoice. In addition to the purchase price, the Client shall pay or reimburse Accenture for all sales, use, property and all other similar taxes, including tax costs incurred by Accenture arising from transactions to purchase the Products and Services, local fees or charges imposed by any federal, state or local government for Products and/or Services provided under this Agreement, even if imposed by law upon Accenture or Accenture's employees, excluding taxes based upon the income or property of Accenture and taxes based upon the payroll of Accenture's employees (collectively "Taxes"). Client will reimburse Accenture for any deficiencies, interest or penalties relating to taxes that are Client's responsibility under this Agreement. If Client is required to withhold or deduct any Taxes from any payment, Client shall be required to "gross up" the amount of such payment and shall pay the total amount reflected on the invoice. The Client agrees to pay such Taxes unless the Client has provided Accenture with a direct pay permit or valid exemption certificate for the applicable jurisdiction. The Parties will cooperate in good faith to minimize Taxes to the extent legally permissible including, if available, acceptance of electronic delivery of software products with no media backup.
5. **Delivery and Risk of Loss.** Shipment and delivery of Products and Services will be in accordance with the applicable terms and conditions of the Third Party Supplier. All orders are subject to the availability of underlying Products and Services. For hardware, title and risk of loss will each pass to Client from Accenture immediately after being transferred to Accenture from the Third Party Supplier.

6. **Order Changes, Cancellations and Returns.** Any order changes, cancellations or returns of Products or Services will be governed by the applicable Third Party Supplier policies. Client will be responsible for any fees, penalties or other amounts a Third Party Supplier charges Accenture as a result of any order change, cancellation or return by Client.

7. **Disclaimer of Warranty.** Warranty remedies offered by the Third Party Supplier, or remedies under applicable law, are the Client's sole and exclusive remedies. This Section shall not be construed to limit any of Client's rights or remedies it may have against the applicable Third Party Supplier in an agreement between Client and such Third Party Supplier***. All Products and Services are provided by Accenture on an "as is" basis without warranty of any kind from Accenture or Accenture Affiliates, including any implied warranties of fitness for a particular purpose, merchantability, or otherwise arising out of, or relating to, the Products and Services.***

8. **Limitation of Liability.** This Section shall not be construed to limit any of Client's rights or remedies it may have against the applicable Third Party Supplier in an agreement between Client and such Third Party Supplier or under law. Except for each Party's confidentiality obligations, the sole liability of either Party to the other (whether in contract, tort or delict, negligence, strict liability in tort, by statute or otherwise) for any and all claims in any manner related to this Agreement or the Products or Services resold will be payment of direct damages, not to exceed (in the aggregate) an amount equal to the total fees received by Accenture for the Product or Service in the applicable Sales Quotation giving rise to the claim or, in the case of subscription Services, the total fees paid under the applicable Sales Quotation giving rise to the claim. In no event will either Party be liable for any: (i) consequential, incidental, indirect, special or punitive damage, loss or expenses or business interruption, loss of data, lost business, lost profits or lost savings, or (ii) loss or claim arising out of or in connection with Client's implementation of any conclusions or recommendations made by Accenture. Nothing in this Section 8 shall operate to limit or exclude a Party's liability for: (a) death or personal injury caused by the Party's negligence or that of its employees or agents; or (b) fraud or fraudulent misrepresentation; or (c) any other liability that cannot be limited or excluded by law.

9. **Confidential Information.** Each Party may be given access to information that relates to the other's business activities, which is identified by the disclosing Party as confidential information or which a reasonable person would deem to be confidential ("Confidential Information"), and access to the names and contact information regarding a Party's personnel, officers, and director, vendors and customers ("Business Contact Information"). Business Contact Information is not considered Confidential Information. Confidential Information and Business Contact Information may only be used by the receiving Party as reasonably needed to perform its obligations and activities permitted under this Agreement, including disclosure to Third Party Suppliers for pre-sales and post-sales activities and record-keeping. The receiving Party agrees to protect the Confidential Information and Business Contact Information of the disclosing Party using a reasonable standard of care. Each party shall be considered a data controller with respect to the other party's Business Contact Information and shall be entitled to transfer such information to any country where such Party, its global organization and Affiliates operate.

10. **Termination and Survival.** Either Party may terminate this Agreement at any time, without cause or penalty, upon 10 business days' prior written notice. However, any Sales Quotation accepted by both Parties prior to the date of termination will remain in effect and continue to be governed by the terms and conditions of this Agreement. The Parties agree that all terms and conditions of this Agreement that by their sense or nature should be deemed to survive termination of this Agreement will survive termination.

11. **Governing Law and Venue.** This Agreement will be governed by the substantive laws of England, without giving effect to any choice of law rules. The United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement. Both Parties specifically agree to submit to the exclusive jurisdiction of, and venue in, English Courts, in any dispute arising out of or relating to this Agreement.

12. **Compliance with Laws**. Each Party will retain responsibility for compliance with all federal, state and local laws and regulations applicable to their respective businesses. Each Party will comply with all applicable export control and economic sanctions laws and regulations, including without limitation those of the United States of America, with respect to the export or re-export of U.S.-origin or other local-origin goods, software and technical data, or the direct product thereof, and each Party agrees to abide by all such regulations in respect of all information supplied by or on behalf of the other Party.

13. **Miscellaneous.** The relationship between Accenture and Client is that of independent contractors and not that of employer/employee, partnership or joint venture. Except for payment obligations, neither Party will be responsible for any delays in delivery or failure to perform that may result from any circumstances beyond that Party's reasonable control. If any part of this Agreement is found by a court of competent jurisdiction to be invalid, illegal or unenforceable, all other parts will still remain in effect. Notices to be provided under this Agreement must be in writing and sent to the address set forth in the applicable purchase order, or as otherwise provided by the Parties. This Agreement and any Sales Quotation supersedes and replaces any previous communications, representations or agreements regarding the purchase of Products or Services from Accenture and may be signed in separate counterparts, each of which will be deemed an original, and together constitute the entire agreement between the Parties.
14. **Implementation in Other Countries.** The Parties agree that Accenture's and Client's respective rights, benefits and/or obligations under this Agreement may be extended to any Accenture Affiliate and Client affiliate in another country through a Local Country Agreement executed by such local Client affiliate and local Accenture Affiliate, provided that the addition of any such country does not violate any applicable export laws and regulations. The Parties intend that such agreement will not modify the terms of this Agreement except to the extent necessary to reflect local business conditions and legal requirements. Such local business conditions and legal requirements shall include, without limitation, the use of local currency, local law and venue. The Parties agree that any modifications made by an amendment to this Agreement shall apply to each Local Country Agreement in effect at the time of such amendment and that come into effect thereafter, and intend to update their respective local affiliates on modifications that affect local legal requirements.
15. **Rights of Third Parties**. The Contracts (Rights of Third Parties Act) 1999 shall not apply to this Agreement or any Sales Quotation.

The Parties hereto have executed this Agreement by their duly authorized representatives as of the Effective Date.

AGREED TO BY:	**AGREED TO BY:**
Client:	**ACCENTURE (UK) LIMITED**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

14. Power Virtual Agent (PVA) Terms and Conditions

This is the current disclaimer for using the PVA Bot for Medical Automated Replies, however, similar and relevant disclaimers would apply if and when the PVA is used in other industries.

The bot topics and related guidance in this blogpost are samples and may be used with Microsoft Power Virtual Agents for dissemination of reference information only. The samples are not designed or intended to be substitutes for professional medical advice, diagnosis, treatment, or judgment and should not be used as such.

The samples should not be used for emergencies and they do not support emergency communications. Microsoft does not warrant that the samples, or any materials provided in connection with the samples, will be sufficient for any medical purposes or meet the health or medical requirements of any person. The samples are not intended or made available for use as medical devices, clinical support, diagnostic tools, or other technology intended to be used in the diagnosis, cure, mitigation, treatment, or prevention of disease or other conditions, and no license or right is granted by Microsoft to use the samples for such purposes. You bear the sole responsibility for any use of the samples, including incorporation into any product or service intended for medical or clinical use, and for providing end users with appropriate warnings about using your crisis response bot.

https://powervirtualagents.microsoft.com/en-us/blog/building-a-crisis-faq-bot-using-power-virtual-agents/

15. Data Processing and Security Addendum

[This document includes the data privacy provisions which apply to all Services described in the preceding documents]

This Data Processing and Security Addendum ("**Addendum**") describes the responsibilities of the parties with respect to the processing and security of any Client Personal Data in connection with the Services provided under any [SOW/Service Order] under the Agreement. This Addendum is subject to the terms and conditions of the [Master Services Agreement] ("**Agreement**") dated _____ between _____("**Client**") and Accenture (UK) Limited ("**Accenture**") and will be deemed part of the Agreement. Terms not defined below shall have the meaning set forth in the Agreement. In the event of a conflict between the Agreement and this Addendum, this Addendum shall prevail.

1. **Definitions**. (a) "Business Contact Information" means the names, mailing addresses, email addresses, and phone numbers regarding the other party's employees, directors, vendors, agents and customers, maintained by a party for business purposes as further described in Section 9 below.

   (b) "Client Personal Data" means client-owned or controlled personal data provided by or on behalf of Client to Accenture or an Accenture affiliate or subcontractor for processing under an [SOW/Service Order]. Unless prohibited by applicable Data Protection Laws, Client Personal Data shall not include information or data that is anonymized, aggregated, de-identified and/or compiled on a generic basis and which does not name or identify a specific person.

   (c) "Consents" includes all necessary consents, permissions, as well as notices and authorizations necessary for the processing or onward transfer by Accenture of Client Personal Data which is required to perform the Services, including the transfer of Client Personal Data outside of the country of origin and any of the foregoing, as applicable, from employees or third parties; valid consents from or notices to applicable data subjects; and authorizations from regulatory authorities, employee representative bodies or other applicable third parties;

   (d) "Data Protection Laws" means all applicable data protection and privacy Laws that apply to the processing of personal data under a particular [SOW/Service Order], including, as applicable, General Data Protection Regulation 2016/679 (GDPR), Federal Data Protection Act of 19 June 1992 (Switzerland), UK Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR), and any US state or federal laws or regulations pertaining to the collection, use, disclosure, security or protection of personal data, or to security breach notification, e.g., California Consumer Privacy Act of 2018 ("CCPA") and California Privacy Rights Act of 2020 ("CPRA").

   (e) "Information Security Incident" means a breach of Accenture's security leading to the accidental or unlawful destruction, loss, alteration or unauthorized acquisition, disclosure, misuse or access to unencrypted Client Personal Data transmitted, stored or otherwise processed by Accenture.

   (f) "Subprocessors" means Accenture Affiliates and third parties authorized under the terms of this Addendum to have access to and process Client Personal Data in order to provide a portion of the Services.

   (g) The terms "controller," "data subject," "de-identification," "personal data," "process," "processing," "processor," "pseudonymize," "sale," "service provider" and "supervisory authority" as used in this Addendum have the meanings given to any equivalent terms in the applicable Data Protection Laws, as relevant.

2. **Roles of the Parties; Compliance with Data Protection Laws**.

   (a) Each party will comply with the requirements of the Data Protection Laws as applicable to such party with respect to the processing of the Client Personal Data.

   (b) Client warrants to Accenture that it has and will maintain all necessary rights (including lawful legal basis), licenses and Consents to provide the Client Personal Data to Accenture for the processing to be performed in relation to the Services and agrees that Client shall be responsible for obtaining all necessary Consents or identifying the appropriate legal basis for the processing, and providing all necessary notices, as required under the relevant Data Protection Laws in relation to the processing of the Client Personal Data.

(c) Accenture will process the Client Personal Data only in accordance with Client's documented processing instructions as set forth in the Agreement, including this Addendum and the applicable [SOW/Service Order], unless otherwise required by law.

(d) If Accenture is acting as a subprocessor in relation to any Client Personal Data (i.e., the data owner/controller is an entity other than Client), Client warrants to Accenture that Client's instructions with respect to the Client Personal Data have been authorized by the applicable data owner/controller, including the appointment of Accenture as a subprocessor.

(e) Except as otherwise set forth in the applicable [SOW/Service Order], (i) Accenture is a service provider and/or processor with respect to the Client Personal Data; and (ii) Client is an owner / controller or service provider / processor, as applicable, of the Client Personal Data.

(f) The applicable [SOW/Service Order] shall set out (i) the subject matter and duration of the processing; (ii) the nature and purpose of the processing; and (iii) the type of personal data and categories of data subjects involved.

(g) Accenture will promptly notify Client if Accenture determines, in its reasonable business judgment, that a Client processing instruction violates any applicable Data Protection Law (provided that nothing herein shall require Accenture to provide legal or regulatory advice or monitor Data Protection Laws as they apply to Client). In such event, the parties will work together in good faith to resolve such issue in a timely manner. In no event will either party be required to perform any activity that violates any applicable Data Protection Law. If Client requires that Accenture follow a processing instruction despite Accenture's notice that such instruction may violate an applicable Data Protection Law, Client will be responsible for all liability for all claims and damages arising from any continued processing in accordance with such instruction.

3. Disclosure and Use of Data.

(a) When providing or making available Client Personal Data to Accenture, Client shall only disclose or transmit Client Personal Data that is necessary for Accenture to perform the applicable Services.

(b) Following expiration or termination of the provision of Services relating to the processing of Client Personal Data, or at Client's request, Accenture shall (and shall require that its sub-processors) promptly and securely delete (or return to Client) all Client Personal Data (including existing copies), unless otherwise required or permitted by applicable laws. Unless otherwise agreed, Accenture will comply with any Client deletion instruction as soon as reasonably practicable and within a maximum period of 180 days.

(c) All Accenture personnel, including subcontractors, authorized to process the Client Personal Data shall be subject to confidentiality obligations and/or subject to an appropriate statutory obligation of confidentiality.

(d) Client expressly acknowledges and agrees that, in the course of providing the Services, Accenture may anonymize, aggregate, and/or otherwise de-identify Client data ("**De-Identified Data**") and subsequently use and/or disclose such De-Identified Data for the purpose of research, benchmarking, improving Accenture's offerings generally, or for another business purpose authorized by applicable Data Protection Law provided that Accenture has implemented technical safeguards and business processes designed to prevent the re-identification or inadvertent release of the De-Identified Data.

4. Security Obligations.

(a) Each party shall implement appropriate technical and organizational security measures to safeguard Client Personal Data from unauthorized processing or accidental loss or damage, as further described in **Attachment 1** to this Addendum ("**Data Safeguards**") and the applicable [SOW/Service Order].

(b) Taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Data, as well as the likelihood and severity of risk to individuals, Accenture's implementation of and compliance with the security measures set forth in **Attachment 1** and the applicable [SOW/Service Order] is designed to provide a level of security appropriate to the risk in respect of the processing of the Client Personal Data.

5. **Additional Accenture Responsibilities**.

   (a) **Documentation, Audits and Inspections**. Accenture shall make available to Client information reasonably requested by Client to demonstrate Accenture's compliance with its obligations in this Section and submit to audits and inspections by Client (or Client directed third parties) in accordance with a mutually agreed process designed to avoid disruption of the Services and protect the confidential information of Accenture and its other clients. As required by applicable law, Accenture shall inform Client if, in Accenture's opinion, any Client audit instruction infringes upon any applicable Data Protection Law. Client shall be solely responsible for determining whether the Services and Accenture's security measures as set forth in **Attachment 1** and the applicable [SOW/Service Order] will meet Client's needs, including with respect to any Data Protection Laws.

   (b) **Data Subject and Supervisory Authority Requests**. As required by law and taking into account the nature of the Services provided, Accenture shall:

      (i) provide assistance to Client as reasonably requested with respect to Client's obligations to respond to requests from Client's data subjects as required under applicable Data Protection Laws.

      Accenture will not independently respond to such requests from Client's data subjects, but will refer them to Client, except where required by applicable Data Protection Law; and

      (ii) provide assistance to Client as reasonably requested if Client needs to provide information (including details of the Services provided by Accenture) to a competent supervisory authority, to the extent that such information is solely in the possession of Accenture or its Subprocessors.

   (c) **Privacy / Data Protection Impact Assessments**. As required by law and taking into account the nature of the Services provided and the information available to Accenture, Accenture shall provide assistance to Client as reasonably requested with respect to Client's obligations to conduct privacy / data protection impact assessments with respect to the processing of Client Personal Data as required under applicable Data Protection Laws.

6. **Subprocessors**. Client generally authorizes the engagement of Accenture's Affiliates as Subprocessors as identified in the list attached to the Agreement or any applicable [SOW/Service Order], and specifically authorizes the engagement of third parties as Subprocessors as identified in the applicable [SOW/Service Order]. Accenture shall contractually require (including via EU SCCs or via intra-company agreements with respect to Affiliates as applicable) any such Subprocessors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder. Accenture shall remain fully liable for the performance of the Subprocessors. Accenture shall provide Client with written notice of any intended changes to the list of authorized Subprocessors or any intended appointment of a new third party Subprocessor and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes / appointment. If Client's objection is based on anything other than the proposed Subprocessor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. Any disagreements between the parties shall be resolved via the contract dispute resolution procedure.

7. **Cross-Border Transfers of Client Personal Data**.

   (a) **Transfers of EEA/Swiss Data**.

      Subject to subsection (d) below, the parties shall rely on the EU Standard Contractual Clauses for the transfers of personal data to third countries pursuant to Regulation (EU) 679/2016, adopted by the EU Commission by its Implementing Decision (EU) 2021/914 of 4 June 2021 (the "**EU SCCs**") to protect Client Personal Data being transferred from a country within the European Economic Area ("**EEA**") and/or Switzerland to a country outside the EEA/Switzerland that is not recognized as providing an adequate level of protection for personal data. The parties will cooperate in good faith to agree on and execute the appropriate module of the EU SCCs to be used based on the data transfer occurring under the applicable [SOW/Service Order].

   (b) **Transfers of UK Data**. Subject to subsection (d) below, the parties shall rely on the EU Standard Contractual Clauses for the transfers of personal data to processors established in third countries, dated 5 February 2010 (2010/87/EU) as amended from time to time by the Information's

Commissioner Office (the "**UK SCCs**") to protect Client Personal Data being transferred from the United Kingdom (UK) to a country outside the UK not recognized as providing an adequate level of protection for personal data. Where the transfer relies on the UK SCCs, the Client, acting as data exporter, shall execute, or shall procure that the relevant Client entities execute, such UK SCCs with the relevant Accenture entity or a third-party entity, acting as a data importer.

(c) **Transfers of non-EEA/Swiss/UK Data** In the event that Client Personal Data is to be transferred outside the country of origin in connection with the provision of Services under the Agreement and this country is not located within the EEA, Switzerland or the United Kingdom, the parties will work together expeditiously and in good faith to establish the appropriate transfer mechanism to be implemented, as required by applicable Data Protection Law.

(d) **Accenture BCR-P**. If and when Accenture's Binding Corporate Rules for Processors are approved, the parties shall rely on such Binding Corporate Rules for Processors to cover any cross-border transfer of Client Personal Data to Accenture, provided that Accenture (i) maintains the applicable approval of its Binding Corporate Rules for Processors for the duration of the applicable [SOW/Service Order]; (ii) promptly notifies Client of any subsequent material changes in the Binding Corporate Rules for Processors or such approval; and (iii) downstreams all of its applicable data protection obligations under its Binding Corporate Rules for Processors to Subprocessors by entering into appropriate onward transfer agreements with any such Subprocessors.

(e) **Transfer Mechanism.** In the event that the transfer mechanisms agreed by the parties herein are amended, replaced, or cease to be authorized as a means to provide "adequate protection" with respect to transfers of Client Personal Data, the parties will work together expeditiously and in good faith to establish another valid transfer mechanism and/or implement supplementary measures as needed to establish appropriate safeguards for such data. Any impacts on the terms of the Agreement and the provision of the Services caused by such new requirements will be addressed by the parties in accordance with Section 10 below.

8. **Information Security Incidents**. Accenture shall maintain procedures to detect and respond to Information Security Incidents. If an Information Security Incident occurs which may reasonably compromise the security or privacy of Client Personal Data, Accenture will promptly notify Client without undue delay. Accenture will cooperate with Client in investigating the Information Security Incident and, taking into account the nature of the Services provided and the information available to Accenture, provide assistance to Client as reasonably requested with respect to Client's breach notification obligations under any applicable Data Protection Laws.

9. **Use of Business Contact Information**. Each party consents to the other party using its Business Contact Information for contract management, payment processing, service offering, and business development purposes, including business development with partners, and such other purposes as set out in the using party's global data privacy policy (copies of which shall be made available upon request). For such purposes, and notwithstanding anything else set forth in the Agreement or this Addendum with respect to Client Personal Data in general, each party shall be considered a controller with respect to the other party's Business Contact Information and shall be entitled to transfer such information to any country where such party's global organization operates.

10. **Changes in Laws**. In the event of (i) any newly enacted Data Protection Law, (ii) any change to an existing Data Protection Law (including generally-accepted interpretations thereof), (iii) any interpretation of a new or existing Data Protection Law by Client, or (iv) any material new or emerging cybersecurity threat, which individually or collectively requires a change in the manner by which Accenture is delivering the Services to Client, the parties shall agree upon how Accenture's delivery of the Services will be impacted and shall make equitable adjustments to the terms of the Agreement and the Services in accordance with the Change Control Procedures.

11. **Relationship with Other Agreements.** For avoidance of doubt and without prejudice to the rights of any data subjects thereunder, this Addendum and any EU SCCs (or other data transfer agreements) that the parties or their affiliates may enter into in connection with the Services provided pursuant to the Agreement will be considered part of the Agreement and the liability terms set forth in the Agreement will apply to all claims arising thereunder.

Attachment 1 to Data Processing and Security Addendum - Data Safeguards

These data safeguards ("Data Safeguards") set forth the security framework that Client and Accenture will follow with respect to protecting Client Data in connection with the [Agreement/SOW]. In the event of a conflict between these Data Safeguards and any terms and conditions set forth in the Agreement, the terms and conditions of these Data Safeguards shall prevail.

I. Security Standards

1. **General Obligations.** Each party will:

- maintain and comply with globally applicable standards, policies and procedures intended to protect data within their own respective environments (e.g., systems, networks, facilities) and such standards will govern and control in their respective environments;
- comply with the other party's standards when accessing or operating within the other party's environments; and
- provide timely notice of any changes to such standards that may materially degrade the security of the Services.

2. Client Standards. Client's applicable security standards are as set out in the SOW.

3. Accenture Standards. Accenture's applicable security standards are as set out online, accessible here: https://www.accenture.com/client-data-safeguards.

II. Vulnerabilities in Client Systems. Unless otherwise expressly agreed in the Agreement or applicable SOW, and except with respect to vulnerabilities caused by Accenture's breach of its obligations under the Agreement or applicable SOW, Client is responsible to remediate any vulnerabilities in Client Data or Client systems at Client's cost. Client may engage Accenture to perform such remediation on Client's behalf pursuant to a project SOW. For clarity, such remediation activities pursuant to a project SOW are not considered "Services" under any other SOW. In the event Client fails to remediate a security vulnerability in Client Data or Client systems, Accenture will not be liable for the consequences resulting from such security vulnerability, including a data security breach, except to the extent such security vulnerability resulted from Accenture's breach of its obligations under the Agreement or applicable SOW.

III. Remote Work. In addition to performing Services from those Accenture and Client Locations specified in the SOW, Accenture personnel may perform the Services or any portion of the Services remotely, provided that performing remotely does not (i) adversely impact Accenture's ability to perform its obligations under the Agreement; or (ii) require any increase to the Fees.

For Services provided on a remote basis, any contractual requirements to provide physical and environmental security controls (e.g., secure bays; security guards; CCTV) at the Accenture service locations will not apply to remote work locations. In addition, where Accenture personnel are required to access Client systems from a remote work location, such access will only occur using devices and access points approved by Client in accordance with SOW.