TERADATA MASTER CLOUD SERVICE AGREEMENT

This Teradata Master Cloud Service Agreement, including any exhibits or documents referenced in it, (the "Agreement") contains the terms and conditions that govern access to and use of the Teradata Cloud Service ("Teradata Cloud Service"). This Agreement is made by, as applicable, Teradata Operations, Inc. if the Customer is in the United States of America, or, either (i) Teradata International Sales Limited, or (ii) another local Teradata entity designated in the applicable Order, if the Customer is outside the United States of America (each "Teradata") and you or the entity you represent ("Customer"). For any conflict between the terms of this Agreement and an Order, the terms of the Order shall take precedence. Notwithstanding the foregoing, any pre-printed terms in a purchase order, invoice, or other transaction document shall have no binding effect.

1. TERADATA CLOUD SERVICE.

1.1. *Provision of Teradata Cloud Service*. Teradata, or its Affiliate, shall provide Customer and its Affiliates' access to the Teradata Cloud Service, subject to the terms and conditions set forth in this Agreement and as described further in the Teradata Cloud Service Description. Teradata grants to Customer a nonexclusive, nontransferable worldwide right to access the Teradata Cloud Service (whether by Customer, its Affiliates, or other persons acting on their behalf) during the Teradata Cloud Service Term. Other than as expressly set forth in this Agreement, no license or other rights in or to the Teradata Cloud Service or Teradata intellectual property are granted to Customer, and all such licenses and rights are hereby expressly reserved.

1.2. *Restrictions*. The Teradata Cloud Service will be limited (e.g., available data space, processing power, number of concurrent users) as set out in the applicable Order. Customer shall not (i) modify, copy or create derivative works based on the Teradata Cloud Service or Teradata intellectual property; (ii) exceed the limitations agreed to in an Order unless otherwise agreed to by the parties in writing; (iii) access or use the Teradata Cloud Service to perform competitive analysis without Teradata's prior written consent; (iv) disassemble, reverse engineer, or decompile, or otherwise attempt to extract any of the source code of the Teradata Cloud Service, or access it with the intent to build a competitive product or service, or copy or substantially copy any ideas, features, functions or graphics of the Teradata Cloud Service; or (v) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share or otherwise commercially exploit or make the Teradata Cloud Service available to any third party unless otherwise permitted in a binding reseller or distributor agreement between Customer and Teradata.

1.3. *Use Guidelines*. Customer shall use reasonable care not to: (i) use the Teradata Cloud Service for any unlawful, infringing, defamatory or fraudulent purpose, (ii) send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs, (iii) knowingly interfere with or disrupt the integrity or performance of the Teradata Cloud Service; (iv) attempt to gain unauthorized access to the Teradata Cloud Service or its related systems or networks; (v) violate, or encourage the violation of, the legal rights of others; or (vi) use the Teradata Cloud Service to engage in, promote or encourage illegal activity.

1.4. *Cloud Service Description*. The Teradata Cloud Service Description (or "Cloud Service Description") is Teradata's standard description for the Teradata Cloud Service in effect at the time of the applicable Order. Teradata may make modifications to the Teradata Cloud Service Description immediately if a modification is required by applicable law, or necessary to improve security, performance, functionality, availability, or reliability of the Teradata Cloud Service. In addition, Teradata may modify the Teradata Cloud Service Description from time to time and will make the most current version thereof available through the Teradata Cloud Service portal. If a modification to the Cloud Service Description materially reduces the features or functions of the Teradata Cloud Service on a general basis, then Teradata will allow Customer to cancel the relevant Order(s) and receive a pro-rated refund of the fees for Teradata Cloud Service covered by the affected Order(s).

2. TERADATA RESPONSIBILITIES. In addition to its other responsibilities set forth in this Agreement, Teradata shall comply with all local, state, federal, and international laws, regulations and government orders applicable to operating the Teradata Cloud Service including those regarding export controls, privacy, and security.

3. CUSTOMER RESPONSIBILITIES. Customer is responsible for the activities of, and effects caused by, anyone who Customer allows to use the Teradata Cloud Service. Customer is also responsible for ensuring that its users comply with this Agreement and the Teradata Cloud Service Description. Customer shall provide secure connectivity to access or transfer data to the Teradata Cloud Service. Unless otherwise specifically covered in the Teradata Cloud Service Description or this Agreement, Customer is solely responsible for determining whether the Teradata Cloud Service ordered will meet its business requirements; data integration; providing standard extracted, transformed, cleansed data for loading into the Teradata Cloud Service; business intelligence development, support and operations; logical and physical data modeling; application development, support and operations; application performance; data quality; having reasonable security processes, tools and controls for systems and networks interacting with the Teradata Cloud Service; making its own elections regarding backup storage and alternative computing capabilities and business processes in the event that the Teradata Cloud Service is unavailable; and reporting incidents via the Teradata Cloud Service Management portal. In addition, Customer shall ensure that the security capabilities in the Teradata Cloud Service, and Customer's use of such security capabilities, fully meet its business needs and its obligations or requirements to protect its data (including encrypting columns containing sensitive information). Customer shall comply with all local, state, federal, and international laws, regulations, and government orders applicable to Customer's use of the Teradata Cloud Service, including those regarding export controls, privacy, and security. Under certain Teradata Cloud Service offers, Customer contracts directly with the Cloud Platform provider for the Site and related services that will host the Teradata Cloud Service. If Customer chooses such a Teradata Cloud Service, (i) Customer shall maintain the highest tier of support offered by the Cloud Platform provider for the Term of the Teradata Cloud Service, and (ii) Customer will look solely to the Cloud Platform provider with respect to any problems or claims related to the Cloud Platform.

4. FEES AND PAYMENT.

4.1. *General*. Except as otherwise specifically provided herein, fees are non-refundable, Customer shall also pay all taxes (including without limitation sales, use, excise, value added, and gross receipts) levied on an Order, except taxes based on Teradata's net income. In order to provide and support the Teradata Cloud Service, Teradata shall monitor and collect information on Customer's use of the system.

4.2. *Orders Placed Directly with Teradata*. Unless otherwise stated in the applicable Order, Customer will pay invoices to Teradata within 30 days after the date of invoice. Teradata will be entitled to charge late fees on amounts properly due under an Order and which are set forth in a correct invoice if Customer fails to pay the amounts when due. Late charges will be the lower of 1.5% per month of the unpaid amount, or any applicable limit imposed by law.

4.3. *Orders Placed Through Cloud Platform Marketplace*. Unless otherwise stated in the applicable Order, Customer will pay for Teradata Cloud Service through Customer's marketplace account. If parts of the Teradata Cloud Service cannot be paid through the Customer's marketplace account, Customer will pay invoices directly to Teradata within 30 days after the date of invoice. Teradata will be entitled to charge late fees on amounts properly due under an Order and which are set forth in a correct invoice if Customer fails to pay the amounts when due. Late charges will be the lower of 1.5% per month of the unpaid amount, or any applicable limit imposed by law.

5. SUSPENSION OF SERVICE. In addition to any other rights or remedies of Teradata, Teradata may, i) upon 10 days' advance written notice, discontinue access to or suspend the Teradata Cloud Service provided to Customer without liability to Customer, if any payment owed to Teradata has not been paid per the terms of this Agreement and such failure to pay has not been cured during the notice period, or ii) immediately discontinue access to or suspend the Teradata Cloud Service in order to protect the Teradata Cloud Service from hacking or other cyber-attack or other material adverse impact to the Teradata Cloud Service or other systems or data.

6. **AVAILABILITY REQUIREMENT**. The Teradata Cloud Service shall have an availability target as defined in the applicable Service Availability section of the Teradata Cloud Service Description and Order. Remedies for failure to meet the availability target shall also be set out therein.

7. WARRANTIES.

7.1. Each party warrants that it will use reasonable efforts to meet its responsibilities set out in this Agreement. Teradata warrants that: (i) it owns or otherwise has sufficient rights to the Teradata Cloud Service to grant the rights granted under this Agreement, and (ii) the Teradata Cloud Service will substantially conform to the Teradata Cloud Service Description. Claims under this warranty must be made in a writing detailing the nature of the breach within 30 days of breach.

7.2. Customer's exclusive remedies for breach of the warranties in this Section shall be as follows: Teradata shall have 30 days to cure the breach by repairing or replacing the Teradata Cloud Service. If repair or replacement of the Teradata Cloud Service is not possible within such period, Customer may terminate its access rights to the defective Teradata Cloud Service by providing written notice of termination to Teradata. Customer shall then be entitled to receive a refund of the prepaid fees for the Teradata Cloud Service pro-rated as of the date Customer provided notice of the breach

7.3. The Teradata Cloud Service is not intended to be used for High Risk Activities. Any use of the Teradata Cloud Service for High Risk Activities by the Customer will be at the Customer's own risk, and the Customer will be solely liable for the result of any failure of the Teradata Cloud Service when used for High Risk Activities. "High Risk Activities" means activities where the failure of the Teradata Cloud Service could lead to death, serious personal injury, or severe environmental or property damages.

7.4. TERADATA MAKES NO WARRANTY THAT THE TERADATA CLOUD SERVICE WILL BE UNINTERRUPTED, AVAILABLE AT ANY PARTICULAR TIME, ERROR-FREE, FREE OF HARMFUL COMPONENTS, OR THAT ANY DATA, INCLUDING CUSTOMER'S DATA OR THIRD-PARTY DATA, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT AS EXPRESSLY PROVIDED HEREIN, TERADATA MAKES NO REPRESENTATIONS, PROMISES OR WARRANTIES RELATED TO THE TERADATA CLOUD SERVICE OR TO TERADATA'S PERFORMANCE UNDER THIS AGREEMENT. EXCEPT FOR THE WARRANTIES EXPRESSLY STATED HEREIN, TERADATA DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THOSE REGARDING MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. TERADATA DOES NOT WARRANT THAT THE TERADATA CLOUD SERVICE WILL YIELD ANY PARTICULAR BUSINESS OR FINANCIAL RESULTS, OR THAT DATA, REPORTS OR ANALYSIS WILL BE TOTALLY ACCURATE.

8. **LIMITATION OF LIABILITY.** EXCEPT FOR A CUSTOMER'S OBLIGATION TO PAY ALL FEES OWED UNDER THIS AGREEMENT, IN NO EVENT SHALL EITHER PARTY'S LIABILITY HEREUNDER EXCEED THE TOTAL AMOUNT TO BE PAID FOR THE TERADATA CLOUD SERVICE UNDER THE INDIVIDUAL ORDER AT ISSUE FOR THE 12 MONTHS OF SERVICE IN WHICH THE CLAIM OCCURRED.

9. EXCLUSION OF DAMAGES.

9.1. NEITHER PARTY OR ITS AFFILIATES, EMPLOYEES, CONTRACTORS OR SUPPLIERS, WHEN ACTING IN SUCH CAPACITY WITH RESPECT TO THIS AGREEMENT, WILL BE LIABLE TO THE OTHER OR ITS AFFILIATES, EMPLOYEES, CONTRACTORS OR SUPPLIERS, WHEN

ACTING IN SUCH CAPACITY WITH RESPECT TO THIS AGREEMENT FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES, INCLUDING INDIRECT LOSS OF PROFITS, REVENUE, TIME, OPPORTUNITY OR DATA, WHETHER IN AN ACTION IN CONTRACT, TORT, PRODUCT LIABILITY, STRICT LIABILITY, STATUTE, LAW, EQUITY OR OTHERWISE. FOR CLARITY, IN ANY ACTION BY TERADATA TO RECOVER PAYMENT OF FEES OWED BY CUSTOMER PURSUANT TO A PRICE SET FORTH ON AN ORDER, THE PROFITS AND REVENUE INCLUDED IN THE PRICE ARE AGREED TO BE DIRECT LOSSES.

9.2. Notwithstanding the above provisions of Sections 8 and 9, a party's liability for:

i) personal injury, including death, will be unlimited to the extent caused by its negligence or willful misconduct;

ii) physical damage to tangible real or personal property will be the amount of direct damages, to the extent caused by its negligence or willful misconduct, up to 1 million dollars;

iii) the obligation to defend and indemnify for intellectual property infringement claims under Sections 10.1 and 10.2 are not limited by Sections 8 and 9;

iv) breach of data security or data protection obligations will be the amount of direct damages, to the extent caused by Teradata, up to 1 million dollars; or

v) intentionally violating the other's intellectual property rights or intentionally breaching the confidentiality provisions of Section 14 of this Agreement is not limited by Sections 8 and 9.

10. INDEMNIFICATION.

10.1. *Teradata Indemnification*. Teradata will defend Customer against any claim, demand, suit or proceeding made or brought against Customer by a third party alleging that the Teradata Cloud Service infringes or misappropriates such third party's intellectual property rights (each, a "Claim Against Customer"), and will indemnify and hold harmless Customer from Teradata's share of any damages, attorney fees and costs finally awarded against Customer as a result of, or for amounts paid by Customer under a settlement approved by Teradata in writing of, a Claim Against Customer. Customer must promptly give Teradata written notice of the Claim Against Customer; give Teradata sole control of the defense and settlement of the Claim Against Customer (except that Teradata may not settle any Claim Against Customer unless it unconditionally releases Customer of all liability); and give Teradata all reasonable assistance, at Teradata's expense.

i) In handling any claim relating to infringement of intellectual property, Teradata may obtain, at no additional charge to Customer, the right for Customer to continue using the Teradata Cloud Service at issue or replace or modify it so that it becomes non-infringing. If Teradata is unable to reasonably secure those remedies, and if Customer must discontinue use of an infringing Teradata Cloud Service then, in addition to providing the defense and indemnification set forth above, Teradata will also refund any unused prepaid fees for the infringing Teradata Cloud Service.

ii) Teradata's indemnification in Section 10.1 does not apply to the extent that the alleged infringement is caused by: use of a Teradata Cloud Service in connection with goods, computer code, or services not furnished as part of, the Teradata Cloud Service; or Teradata's compliance with Customer-specific designs or specifications. Section 10.1 represents Teradata's exclusive liability and Customer's sole remedy for third party claims related to infringement of intellectual property rights by the Teradata Cloud Service.

10.2. *Customer Indemnification*. Customer will defend Teradata against any claim, demand, suit or proceeding made or brought against Teradata by a third party alleging that any Customer Data infringes or misappropriates such third party's intellectual property rights, or to the extent caused by Customer's use of the Teradata Cloud Service in breach of the Agreement, the Teradata Cloud Service Description, Order or applicable law (each a "Claim Against Teradata"), and will indemnify Teradata from Customer's share of any damages, attorney fees and costs finally awarded against Teradata as a result of, or for any amounts paid by Teradata under a settlement approved by Customer in writing of, a Claim Against Teradata. Teradata must promptly give Customer written notice of the Claim Against Teradata; give Customer sole control of the defense and settlement of the Claim Against Teradata (except that Customer may not settle any Claim Against Teradata unless it unconditionally releases Teradata of all liability); and give Customer all reasonable assistance, at Customer's expense.

10.3. *Mitigation*. The party seeking indemnification under this Agreement shall have a duty to use reasonable efforts to mitigate damages and other costs and losses.

11. TERM AND TERMINATION.

11.1. *Term*. This Agreement commences on the Effective Date and shall continue in effect for the term of all applicable Orders for Teradata Cloud Service. Each Teradata Cloud Service Order becomes effective on the Order Effective Date, but the Teradata Cloud Service Term specified in an Order does not begin until the Cloud Service Availability Date.

11.2. *Termination for Breach*. Either Customer or Teradata may terminate an affected Order under this Agreement as a result of a material breach of this Agreement or the relevant Order by the other party: if (i) such party provides written notification to the other party of the material breach, and (ii) such material breach is not cured within 30 days of notification. Either party may terminate an Order and this Agreement if the other party is adjudged bankrupt, placed in receivership, becomes insolvent, or is unable to carry on business in the normal course and is unable to cure the foregoing within 30 days.

11.3. *Effect of Termination*. In the event of termination or expiration of an Order under this Agreement for any reason, Customer's access and use of Teradata Cloud Service and Customer's rights under that Order shall cease. Teradata will hold the relevant Teradata Cloud Service Site in a suspended state for 30 days following termination, after which period, that site will be deleted. Teradata will assist with moving data from a Site, upon mutual agreement on the terms, scope of services and fees for such assistance. If Customer rightfully terminates this Agreement for breach, Customer shall then be entitled to receive a refund of the prepaid fees for the Teradata Cloud Service pro-rated as of the date Customer provided notice of the breach. Sections 7, 8, 9, 10, and 14 through 22 shall survive any expiration or termination of this Agreement.

12. PUBLICITY. Each party shall have the right to state that the other party is a customer/supplier including in conference calls and to place the other party's logo on publicly available lists of its customers/suppliers. Each party grants to the other a license to the use of the other's name and logo as contemplated by the purpose of this exhibit in accordance with any logo usage guidelines provided by the first party. The parties will jointly issue a mutually agreed press release describing the general type of products Customer has acquired, the nature of the intended deployment of the Teradata Cloud Service, anticipated business benefits, and Teradata's differentiators, and include a quote from both parties. After successful implementation of the initial Teradata Cloud Service, Customer will, upon request by Teradata, participate in four of the following activities: customer video, written customer story, analyst report, reference calls, media opportunities, social network opportunities, or other mutually agreed activities. After successful implementation of the initial Teradata Cloud Service, Customer has the option to join Teradata's Peer Advantage Program. Unless otherwise agreed in writing or as set out in this Section, neither party will mention or refer to the other with respect to any data warehouse or analytics product, function or usage.

13. FORCE MAJEURE. Neither party will be responsible for any failure or delay in its performance under this Agreement due to acts of God or government, civil commotion, military authority, war, riots, terrorism, strikes, fire, or other causes beyond its reasonable control.

14. CONFIDENTIALITY.

14.1. *Generally*. Each party accessing Confidential Information of the other party agrees to use reasonable efforts to prevent the disclosure of such accessed Confidential Information of the other to third parties and its employees who do not have a need to know it, but may disclose it for confidentiality-protected financial, legal, security, compliance and/or tax reviews, advice, disclosures and audits. Each party will protect the Confidential Information of the other party with the same degree of care it exercises relative to its own Confidential Information, but not less than reasonable care. The disclosing party will use reasonable efforts to mark or otherwise designate information as confidential prior to disclosure. Customer's data values stored in or processed by computers, personal individually identifiable information, customer records/lists, financial/account records, employee records, medical/health records, business plans, pricing, software in human-readable form (e.g., source code), logical data models, and any other information that reasonably should be understood by the receiving party to be confidential will be considered Confidential Information whether or not marked as such. Upon the disclosing party's written request, the receiving party will destroy all full or partial copies of Confidential Information that it has in its control.

14.2. *Confidentiality Term*. Confidentiality obligations under this Agreement with respect to Customer Data stored in or processed by computers, personal individually identifiable information, customer records/lists, financial/account records, employee records, medical/health records, business plans, security information, software in human-readable form (*e.g.,* source code), and data models, will continue indefinitely. Otherwise, confidentiality obligations under this Agreement will end 2 years after termination of this Agreement.

14.3. *Exclusions to Confidentiality Provisions*. The obligations of the parties in respect of the Confidential Information of the other party shall not apply to any material or information that is or becomes a part of the public domain through no act or omission by the receiving party; is independently developed by employees or consultants of the receiving party without use or reference to the Confidential Information of the other party; or is disclosed to the receiving party by a third party that, to the receiving party's knowledge, was not bound by a confidentiality obligation to the other party. Personally identifiable information shall not lose its status as Confidential Information because it may be in the public domain. If Confidential Information is demanded by a lawful order from any court or lawful authority, the recipient agrees (to the extent permitted by such order) to notify the discloser promptly of the receipt of any such order; provide the other with a copy of such order; and to provide reasonable assistance to the discloser (at the disclosing party's expense in the case of reasonable out-of-pocket expenses) to object to such disclosure.

14.4. *Confidentiality and Contractors*. Each party may disclose Confidential Information to its Affiliates subject to the confidentiality terms of this Agreement, and to its contractors (such contractors which may include the Cloud Platform providers), who have a need to know the Confidential Information related to performance under this Agreement, and which agree in writing to confidentiality obligations consistent with this Agreement. Each party is responsible for any breach of these provisions by such Affiliates and contractors to which it provided the other party's Confidential Information.

14.5. *Other Confidentiality Agreements*. This Section shall control and supersede the terms of any non-disclosure or confidentiality agreement executed between the parties for Confidential Information concerning, related to, or stored in the Teradata Cloud Service.

15. DATA PROCESSING AND SECURITY. The parties agree to the Data Processing Terms set out in Exhibit A to this Agreement.

15.1. *Right to Process Data*. Customer represents and warrants that it owns or otherwise controls all the rights to Customer Data and that use of Customer Data does not violate any provision in this Agreement.

15.2. *Data Security Generally.* Teradata will have in place throughout the term of this Agreement security measures consisting of administrative, physical, and technical measures for: (i) maintaining industry-standard firewall protection for the Teradata Cloud Service systems, (ii) applying, on a reasonable schedule after release, patches to the Teradata Cloud Service system, (iii) employing commercially reasonable efforts to scan the Teradata Cloud Service systems for viruses and malware, and (iv) limiting employee and subcontractor access to the Teradata Cloud Service systems and facilities to authorized individuals who have a need-to-know and whose access privileges shall be revoked promptly upon their termination by Teradata.

15.3. *Data Breach*. Either party will inform the other as soon as practicable upon learning of a data breach on the Teradata Cloud Service involving Customer Data. The parties shall coordinate with each other to investigate the data breach and Teradata agrees to reasonably cooperate with Customer in Customer's handling of the matter, including, without limitation, assisting with any investigation and making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards. Each party will use reasonable measures in keeping with IT security industry standard practices to prevent a recurrence of any data breach as soon as practicable.

15.4. *Audit*. On an annual basis, certain components of the Teradata Cloud Service will undergo an AICPA Service Organization Controls (SOC 2) review, statement on Standards for Attestation Engagements No. 18 (SSAE18) SOC 1 review, PCI DSS validation, a HIPAA audit, and an ISO 27001:2013 audit of its Information Security Management System (ISMS), as well as an independent penetration test. Auditor and penetration test findings will be addressed in accordance with Teradata's policies. Upon customer request, Teradata will share the most recent SOC 1 report, SOC 2 report, ISO 27001:2013 certification, PCI DSS 3.2 Attestation of Compliance (AOC), and HIPAA Security Assessment reports. The scope of these audits and assessments is detailed in the Cloud Service Description.

16. NOTICES. Notice to the other party to this Agreement shall be in writing (including email sent to a designated address or number) and sent by personal delivery or commercial courier and shall be deemed provided on first receipt. Teradata will send notices to Customer at the address on the top of this Agreement and to any other address designated by Customer in writing; Customer will send notices to__________. Teradata at law.notices@teradata.com and/or 17095 Via del Campo, San Diego, CA 92127, Attn: General Counsel/Notices.

17. ASSIGNMENT. Neither party may assign, transfer, or delegate any of its rights, duties, or obligations hereunder, in whole or in part, without the prior written consent of the other party. Notwithstanding the foregoing, either party may assign this Agreement to an Affiliate, or in connection with a merger, reorganization, reincorporation, consolidation or other transfer to such Affiliate.

18. GOVERNING LAW; DISPUTES. New York law will govern the interpretation and enforcement of this Agreement and Orders under it; however, the Federal Arbitration Act will govern all issues of arbitrability. In the event of a claim, controversy, or dispute arising out of or related to this Agreement, an Order or the Teradata Cloud Service or other service, each party agrees to give the other prompt notice of such, and both agree to meet and confer promptly to engage in good faith discussions to try to resolve the matter. Any such controversy, claim or dispute which is not resolved through the procedure set forth above within 30 days will be resolved by arbitration before a sole mutually-agreeable arbitrator who is an attorney with experience in cloud computing under the then-current Commercial Arbitration Rules of the American Arbitration Association. The duty and right to arbitrate will extend to any employee, officer, director, shareholder, agent, affiliate, supplier, or contractor of a party to the extent such right or duty arises through a party or is related to this Agreement, an Order and/or the Teradata Cloud Service or other service. There shall be no right or authority for any claims to be arbitrated as a class member in any purported class or representative proceeding. The decision and award of the arbitrator will be final and binding, and the award rendered may be entered in any court having jurisdiction thereof. The arbitrator is directed to hear and decide potentially-dispositive motions in advance of the hearing-on-the-merits by applying the applicable law to uncontested facts and documents. The arbitration will be held in the United States headquarters city of the party not initiating the claim. Except to the extent, if any, elected in writing by the claiming party, the obligation to arbitrate hereunder will not apply to claims for misuse or infringement of a party's intellectual property; and, a claiming party may seek an injunction in court to prevent misuse or infringement of its intellectual property pending the appointment of an arbitrator. The arbitrator will enforce the terms of this Agreement and the order(s) at issue and will have no authority to award any damages in excess of the limitations and exclusions set forth in this Agreement or in an applicable order. Neither party may bring a claim more than 2 years after the underlying cause of action first accrues or the party bringing the claim, using reasonable care, first discovers or should have discovered the underlying facts giving rise to the claim, whichever is later.

19. EXPORT CONTROLS. Customer acknowledges that the products and any and all related materials are subject to the export restrictions and controls imposed by the United States Export Administration Regulations ("EAR") and expressly agrees to abide by all such export restrictions and controls, including, but not limited to, ensuring that (1) all products will be used only for civil purposes and not for nuclear, chemical or biological weapons, missile technology or other military purposes and (2) all products will be used only for Customer's internal use and (3) it will not sell, export, re-export, transship, loan or otherwise transfer or grant access to the products to any person for any purpose, including without limitation, Belarus, Cuba, Iran, North Korea, Russia, Sudan and Syria or to any nationals or citizens thereof, or to persons listed on the Denied Party List maintained by the United States Department of Commerce, Bureau of Industry and Security, the United States Office of Foreign Asset Control and the United States Department of State, or to any person otherwise prohibited pursuant to the EAR.

20. AUTHORITY. The individual executing this Agreement by, as applicable, signing such document, or clicking the "Create Contract" or similar button with a link to these terms, represents that he or she is duly authorized and has the authority to enter into this Agreement on behalf of the Customer.

21. GENERAL. If any provision of this Agreement is held to be illegal, invalid, or unenforceable, it will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remaining provisions will remain in full force and effect. Failure to enforce any provision of this Agreement shall not constitute a waiver of future enforcement of that or any other provision. This Agreement and any exhibits or documents referenced, or related Orders constitute the entire understanding between the parties solely with respect to Teradata's provision of Teradata Cloud Service. Any modifications to this Agreement must be in writing and signed by both parties, and, if applicable, such changes shall expressly supersede Teradata's standard contract for the Teradata Cloud Service accessible on the marketplace of such Cloud Platform. With respect to execution of this Agreement and any order, Customer and Teradata agree that a facsimile or electronic copy of either party's signature shall be considered a binding, original signature of each party. This Agreement shall bind the parties, their successors, heirs, and assigns to the extent permitted hereunder. In all matters relating to this Agreement, Customer and Teradata shall act as independent contractors. Teradata may use contractors, resellers and/or suppliers to fulfill its obligations, but in such event, Teradata will assure that they are bound to the same obligations as Teradata to the same extent as Teradata would be if it had provided the service at issue directly to Customer.

22. DEFINITIONS.

Affiliate: Any entity which directly or indirectly controls, is controlled by, or is under common control with the subject entity.

Cloud Platform: Cloud infrastructure and services provided by the cloud provider identified in the applicable Order or upon "click thru" acceptance of an order through that provider.

Confidential Information: All proprietary information disclosed by one party to the other related to the disclosing party, this Agreement, Teradata's products or services, or an Order, including, without limitation, technologies, methodologies, business plans, business records, requests for proposals ("RFPs"), requests for information ("RFIs"), responses to RFPs and/or RFIs, bids, pricing, and discussions regarding potential future business between the parties.

Customer Data: All data uploaded by Customer to the Teradata Cloud Service through the Cloud Platform.

Effective Date: This Agreement takes effect on the earlier of (i) when Customer clicks a "Create Contract" check box or similar button that includes a link to these terms on the marketplace of such Cloud Platform if applicable; or (ii) the last signature date of the first fully executed Order between the parties governed by this Agreement (the "Effective Date"). Once this Agreement becomes effective, it shall govern all subsequent Teradata Cloud Service Orders regardless of whether the Order is placed directly or through the Cloud Platform provider's marketplace.

Order: An order under which Teradata provides access to Teradata Cloud Service.

Service Availability Date: The date that Teradata informs Customer that Teradata has completed set up of the Teradata Cloud Service for Customer.

Teradata Cloud Service Description (or Service Description): Teradata's standard description for the Teradata Cloud Service in effect at the time of the applicable Order or as modified from time to time as set out in Section 1.4.

Teradata Cloud Service: Customer's electronic access to Teradata software and services as specifically described in the applicable Order entered into by the parties and the Service Description. If the Customer has chosen to contract directly with the Cloud Platform provider for the Site, Teradata Cloud Service excludes the Cloud Platform infrastructure (including related services such security and operations) provided by such Cloud Platform provider to Customer under an independent agreement.

Teradata Cloud Service Site (or Site): As applicable, either (i) each Cloud Platform provisioned under this Agreement or (ii) if the Customer has chosen to contract directly with the Cloud Platform provider, the Cloud Platform infrastructure provisioned independently by Customer.

Teradata Cloud Service Term (or Cloud Service Term): The period agreed to in an Order during which Teradata will provide access to the Teradata Cloud Service to Customer.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by signing below or by agreeing to terms via the Cloud Platform provider marketplace.

Exhibit A

Data Processing Attachment

This Data Processing Attachment ("DPA") forms part of the TERADATA MASTER CLOUD SERVICE AGREEMENT between Customer as Data Controller and Teradata as Data Processor. That agreement shall collectively be referred to below as the "Agreement".

1. Definitions

1.1 "*Data Protection Laws and Regulations*" means any legislation and/or regulation implementing or made pursuant to it which amends, replaces, re-enacts, implements, consolidates or derogates from any of it, and all other applicable laws relating to Processing of Personal Data and privacy that may exist in any relevant jurisdiction, including, the General Data Protection Regulation ("GDPR") (Regulation (EU) 2016/679), the California Consumer Privacy Act of 2018 (CCPA) where applicable, the guidance and codes of practice issued from time to time by Data Protection Authority, other data protection supervisory authorities relevant to Customer, the European Commission, the Article 29 Working Party and the European Data Protection Board.

1.2 "*Personal Data Breach*" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.3 "*Sub-processor*" shall mean a Data Processor processing data on behalf of a Data Processor.

1.4 All other capitalised terms shall have the meaning given to them in the General Data Protection Regulation.

2. Data Processing

2.1 In the course of rendering the contractual services Teradata may from time to time access Customer's Personal Data. Such services may include all or any of maintenance and support services, managed services or consultancy services. Access by Teradata to such Customer Personal Data is rare and limited in its extent. If such access to Customer's data qualifies as Processing under the Data Protection Laws and Regulations the parties acknowledge and agree that regarding such Processing, Customer is the Controller and Teradata is the Processor.

2.2 The parties shall each comply with their respective obligations under the Data Protection Laws and Regulations. Customer shall, in its acquisition of the services, process Personal Data only in accordance with the requirements of Data Protection Laws and Regulations.

2.3 Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Teradata shall inform Customer immediately if, in Teradata's opinion, an instruction from Customer violates Data Protection Laws and Regulations.

2.4 Teradata shall only process Personal Data on behalf of and in accordance with Customer's documented instructions for the purposes of (i) Processing in accordance with the Agreement (ii) Processing to comply with other documented reasonable instructions provided by Customer.

2.5 Subject-matter, duration nature and purpose of the Processing and the type of Personal Data and categories of Data Subjects are defined in the Agreement. Teradata's Privacy Policy can be viewed on Teradata's website www.teradata.com.

2.6 Data subjects.

The Personal Data processed concern the following categories of data subjects:

- Controller's customers

- Controller’s prospects
- Controller’s website visitors
- Controller’s employees and contractors
- Controller’s suppliers
- Controller’s other contacts

2.7 Categories of data.

The Personal Data processed concern the following categories of data:

- email addresses
- mobile number
- landline number
- last name, first name
- postal address
- date of birth
- information showing the
- opening of received emails
- clicks of links within the received emails
- IP addresses
- financial information
- online behaviour
- marital status and dependants
- pictures, videos
- geo data
- purchase behaviour and history

3. Data Subjects’ Rights Requests

3.1 Teradata shall, to the extent legally required, promptly notify Customer if Teradata receives a request from a Data Subject to exercise one or more of the Data Subject's rights as defined within chapter III GDPR (33-36) (“DSR Request”).

3.2 Taking into account the nature of the Processing, Teradata shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a DSR Request under Data Protection Laws and Regulations.

3.3 To the extent Customer, in its use of the services, does not have the ability to address a DSR Request, Teradata shall, upon Customer’s request, provide commercially reasonable efforts to assist Customer in responding to such a DSR Request, to the extent Teradata is legally required to do so and the response to such DSR Request is required under Data Protection Laws and Regulations. Except where such is prohibited, Teradata may make a reasonable charge for the provision of such assistance.

4. Data Protection Impact Assessments

Teradata shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with a Supervisory Authority, required under Data Protection Laws and Regulations, in each case solely in relation to Processing of Personal Data by Teradata, and at all times taking into account the nature of the Processing and information available to

Teradata. Except where such is prohibited, Teradata may make a reasonable charge for the provision of such assistance.

5. Personal Data Breach Notification

5.1 Either party shall notify the other without undue delay after becoming aware of a Personal Data Breach. Teradata shall provide Customer with sufficient information to allow Customer to meet any obligations to notify a Supervisory Authority of the Personal Data Breach and/or communicate the Personal Data Breach to Data Subjects under the Data Protection Laws and Regulations.

5.2 Teradata shall make reasonable efforts to identify the cause of a Personal Data Breach and take those steps as Teradata deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Teradata’s reasonable control.

5.3 Teradata’s obligations herein shall not apply to incidents that are caused by Customer.

6. Sub-Processing

6.1 Sub-processors used by Teradata to provide its contractual services, including their geographical location are published in Teradata’s List of Affiliates, available upon request and/or accessible in Teradata’s then-current 10-K Exhibit 21 (@ www.sec.gov, current version accessible here[1]) and also include the Cloud Platform provider for the relevant Cloud Platform in the Applicable Order.

6.2 Teradata has entered into a written Data Processing Agreement based on the Standard Contractual Clauses as issued by the European Commission with each Sub-processor.

6.3 Teradata shall be liable for the acts and omissions of its Sub-processors to the same extent Teradata would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the MA.

7. Security

7.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Teradata shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Personal Data, as set forth in Teradata’s Technical and Organisational Measures. Teradata regularly monitors compliance with these measures. Teradata will not materially decrease the overall security of the services during the term of the MA.

7.2 Teradata will have in place throughout the term of the Agreement security measures consisting of administrative, physical, and technical measures for: (i) maintaining industry-standard firewall protection for the Teradata Cloud Service systems under its control, (ii) applying, on a reasonable schedule after release, patches to the Teradata Cloud Service systems under its control, (iii) employing commercially reasonable efforts to scan the Teradata Cloud Service systems under its control for viruses and malware, and (iv) limiting employee and subcontractor access to the Teradata Cloud Service systems and facilities under its control to authorized individuals who have a need-to-know and whose access privileges shall be revoked promptly upon their termination by Teradata.

[1] https://www.sec.gov/Archives/edgar/data/816761/000081676118000007/tdc123117exhibit21.htm.

8. DELETION OR RETURN OF PERSONAL DATA

8.1 Teradata shall, without undue delay, delete the Personal Data upon termination/expiry of the Agreement or upon Customer's request. Teradata may retain Personal Data to the extent required by applicable laws and only to the extent and for such period as required by the applicable laws and always provided that Teradata shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

8.2 Teradata shall return Personal Data to Customer in accordance with the procedure and timeframe specified in the MA.

9. AUDITS AND INSPECTIONS

Teradata shall make available to Customer all information necessary to demonstrate compliance with the Data Protection Laws and Regulations applicable to Teradata's Processing of Personal Data under this Agreement and shall allow for and contribute to audits by Customer or a third-party auditor mandated by Customer in relation to the Processing of Personal Data, but only to the extent required by the Data Protection Laws and Regulations applicable to Teradata's Processing of Personal Data under this DPA. For example, under GDPR, Customer would only have the right to conduct an audit if the documentation provided by Supplier (e.g., independent SOC audit report) did not contain the information necessary to establish Supplier's compliance with GDPR and the scope of any such audit would be limited to only that information necessary to establish Supplier's compliance with GDPR not already provided by Supplier. Where an applicable Data Protection Law and Regulation does not require Supplier allow audits, Customer would have no right to audit.