ADDENDUM TO AGREEMENT FOR CLOUD ID SERVICE PROVIDERS

This Addendum to Agreement for Cloud ID Service Providers is entered into as of the last date of signature listed on an applicable, fully executed Service Order Form (the "Effective Date"), by and between the customer listed on the same fully executed Order Form for Cloud ID Services ("Customer" or "Service Provider") and Enhanced Telecommunications, Inc. d/b/a ETI Software Solutions ("Company" or "ETI"), a Georgia corporation, with offices at 6065 Atlantic Blvd., Norcross, GA 30071., and Enhanced Telecommunications, Inc. d/b/a ETI Software Solutions, a Georgia corporation ("Reseller" and together with Customer, the "Parties" and each individually, a "Party"). The terms of this Cloud ID Addendum supplement and form a part of any service agreement, order or other terms and conditions between Reseller and Customer pursuant to which Customer receives Cloud ID services through Reseller (collectively, the "Agreement"). In the event of any conflict between the Agreement and this Cloud ID Addendum, this Cloud ID Addendum will prevail pertaining solely to the use of Cloud ID Services.

WHEREAS, Pursuant to the Agreement, Customer has engaged Reller to procure certain Services (defined below) from Cloud ID on Customer's behalf;

WHEREAS, Under updated terms and conditions, Cloud ID now requires that all parties granted access and/or use of the Services must agree in writing to certain terms and conditions, as contained Reseller's updated agreement with Cloud ID (the "Reseller Agreement");

WHEREAS, The intent of this Cloud ID Addendum is to pass through to Customer such required terms from the Reseller Agreement; and

WHEREAS, The terms of this Cloud ID Addendum govern only the use of Cloud ID Product by Customer; and

WHEREAS, The Parties now desire to supplement the Agreement with such terms.

NOW, THEREFORE, in consideration of the terms and conditions set forth in this Cloud ID Addendum and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

1. DEFINITIONS.

1.1 "Account Information" means information about User accounts that is provided by Customer or Users in connection with the Services.

1.2 "Active User" means a Subscriber who successfully authenticates and/or receives an authorization response to use the Service to access Content or a Connected-Service within a calendar month. Active Users are identified via the unique or opaque identifier provided by Customer when the Subscriber authenticates their identity via the Service or receives an authorization response from Customer or Cloud ID.

1.3 "Affiliate" means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. The term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract, or otherwise.

1.4 "Cloud ID Addendum" means this Cloud ID Addendum, including the attached Order Form, Service Schedule, Service Level Agreement, Scope of Requirements, and Data Processing Addendum. In the event of a conflict among these documents, the terms of the Cloud ID Addendum will be determined by giving preference in descending order of control to (1) this Cloud ID Addendum; the Data Processing Addendum, the Scope of Requirements, the Service Level Agreement, and the Service Schedule.

1.5 "Authorized User" means an employee, consultant, contractor, or agent of Customer authorized to access and use the Service on behalf of Customer for administrative purposes only pursuant to the rights granted to Customer pursuant to this Cloud ID Addendum.

1.6 "Cloud ID Platform" means Cloud ID's modular identity management platform that offers a single integration point for participants in an on-line access control framework.

1.7 "Cloud ID Property" means (i) the Cloud ID Marks; (ii) the Cloud ID Technology; (iii) the Service; (iv) Cloud ID's Confidential & Proprietary Information; and (v) all Intellectual Property Rights or other proprietary rights in and to any of the foregoing.

1.8 "Cloud ID Technology" means Cloud ID's proprietary technology, including without limitation, hardware designs, algorithms, software, software and user-interface designs, architecture, documentation (both printed and electronic), network designs, know-how, trademarks, patents, trade dress, methodologies, trade secrets, confidential information, and any related intellectual property rights throughout the world (whether owned by Cloud ID or licensed to Cloud ID from a third party), used in the Service or incorporated into any deliverables, and any derivatives, improvements, enhancements, or extensions of any of the foregoing, conceived, reduced to

practice, or developed whether alone or jointly with others by Cloud ID or Customer.

1.9 "Confidential & Proprietary Information" means all information that relates to past, present, and future research, development, financial, operations, clients, Users, and business activities of a Party or its subsidiaries or Affiliates, and any software, technology, systems, procedures, algorithms, computer programs, data and information which a Party's employees, consultants or agents may construct or acquire possession or knowledge of by reason of their performance of rights or obligations, including, without limitation, Third Party Proprietary Information. Confidential Information will exclude information that: (i) was known to the receiving Party without restriction on disclosure or use before disclosure by the disclosing Party; (ii) is or becomes information within the public domain (through no fault of the receiving Party); (iii) is independently developed by the receiving party without reference to or knowledge of confidential information; (iv) is rightfully received from third parties not subject to an obligation or confidence to the disclosing Party; or (v) the release of which is pre-approved by the disclosing Party in writing.

1.10 "Connected-Service" means a service offering made available by a Service Provider and accessible via the Internet by authenticated Users, including but not limited to (i) apps, tools, and services such as account management, WiFi hotspots, webmail; and (ii) any logos, trademarks, service marks, meta data, or other materials made available therewith.

1.11 "Content" means programming or a service offering made available by a Content Provider and accessible via the Internet by authenticated Users, including but not limited to (i) digital streaming content, including, but not limited to movies, television programs, video programming, music, audio, games, images, graphics, statistics, text, and other multimedia content; and (ii) any logos, trademarks, service marks, meta data, or other materials made available therewith.

1.12 "Content Provider" means any individual, entity, or organization (i) engaged in the creation, licensing, and distribution of Content; (ii) that operates platforms or services that deliver Content directly to its own Subscribers, typically through subscription-based or ad-supported models; or (iii) enters into commercial agreements with other Content Providers or Service Providers, thereby enabling the distribution of its Content to the Subscribers of these third-party platforms or services, and such agreements may include, but are not limited to, syndication arrangements, licensing partnerships, or white-label distribution deals, ensuring that the Content is accessible across multiple platforms and Subscriber bases.

1.13 "Customer" means the named Customer on the applicable order form.

1.14 "Customer Content" means any data, Content, Marks, or Confidential & Proprietary Information of Customer: (a) that may be disclosed to Cloud ID in conjunction with the use or performance of the Service; (b) that may be generated by or displayed to Users in conjunction with Customer's use of the Service; or (c) that is generated or embedded on Customer's Digital Properties or its version of the Service.

1.15 "Customer Materials" means the materials, domain names, Customer Content, Account Information, User subscription data, and other information or content provided by Customer to Cloud ID as required by the Cloud ID Addendum or reasonably necessary to provide the Service or perform the Services.

1.16 "Customer Systems" means the Customer's information technology infrastructure, including Digital Properties, computers, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Customer or through the use of third-party services.

1.17 "Data Protection Addendum" means the attached Exhibit E, which set forth a Data Protection Addendum among the Parties.

1.18 "Data Protection Laws" means all data privacy and security laws, rules and regulations in any jurisdiction applicable to the Service provided pursuant to this Cloud ID Addendum and/or other obligations set forth in this Cloud ID Addendum, and as more specifically defined in the Data Protection Addendum.

1.19 "Digital Property" or "Digital Properties" means a digital property such as a web page, mobile site, video digital property, video player, application, retailer page, etc.

1.20 "Effective Date" has the meaning set forth in the preamble of this Cloud ID Addendum.

1.21 "Federated Directory of Content Providers" means Cloud ID's then-current federated directory of Content Provider partners, which (as of the Effective Date) is set forth on that certain Federated Content Provider Addendum attached as Exhibit D.

1.22 "Fees" means Onboarding Fees, Monthly Platform Fees, Professional Service Fees, and any other fees due Reseller pursuant to this Cloud ID Addendum or related Order Form for the Service or Services.

1.23 "Intellectual Property Rights" means any and all registered and unregistered rights granted, applied for, or otherwise now or hereafter in existence under or related to any patent, copyright, trademark, trade secret, database protection, or other intellectual property rights laws, and all similar or equivalent rights or forms of protection, in any part of the world.

1.24 "Law" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree, or other requirement of any federal, state, local, or foreign government or political subdivision thereof, or any arbitrator, court, or tribunal of competent jurisdiction.

1.25 "Marks" means existing and subsequently-developed, legally valid and protectable logos, trademarks, service marks, trade names, logos, slogans, trade dress, and domain names.

1.26 "Order Form" means a document, pursuant to which Customer orders Cloud ID Service and specific Services from Reseller.

1.27 "Party" or "Parties" means Customer and Reseller, individually or collectively.

1.28 "Person" means an individual, corporation, partnership, joint venture, limited liability entity, governmental authority, unincorporated organization, trust, association, or other entity.

1.29 "Production" means an environment in which the Service is live for Customer's use.

1.30 "Provider" means a Content Provider or a Service Provider, as applicable.

1.31 "Scope of Requirements" means the attached Exhibit A-1 to the Order Form, which sets forth the scope of requirements for onboarding the Service.

1.32 "Service" means the Cloud ID authentication service described in the Order Form and Service Schedule, which enables Users to authenticate their entitlement to use certain content of a Content Provider based on their service relationships with a Service Provider.

1.33 "Service Level Agreement" means the attached Exhibit C, which sets forth the service levels for the Service.

1.34 "Service Package" means the type of Service package that the Customer orders via the Order Form, i.e., Essential Package, Advanced Package, or Ultimate Package.

1.35 "Service Provider" means Customer.

1.36 "Services" means the services described in the Order Form and Service Schedule, which are in addition to the Service, such as integration services, professional services, and technical support services.

1.37 "Service Schedule - Description of Service and Services" or "Service Schedule" means the attached Exhibit B, which sets forth a description of the Service and Services set forth in the Order Form.

1.38 "Subscriber" means an individual customer (identified by a Customer supplied account ID) of Customer that subscribes to (as applicable) Content or a Connected-Service pursuant to which Customer has authorized the use of the Service for such person.

1.39 "Technology Property" or "Technology Properties" means any mutually agreed digital device, application, or technology on which Users will be able to authenticate and authorize through the Service pursuant to the Service Schedule, which will include, but not be limited to, applications and websites of Customer or a Provider, and may include smart phone or tablet applications, Smart TVs, or other mutually agreed upon devices, applications, or technologies.

1.40 "Term" has the meaning set forth in below in the Term section.

1.41 "Third Party Proprietary Information" means any confidential or proprietary information of a third party that a Party is obligated, under a contractual or legal confidentiality obligation, to maintain confidential and/or the use or disclosure of which is governed by licensing, confidentiality or other written agreements with a third party.

1.42 "User" means an Authorized User or Subscriber.

2. SERVICE DELIVERY, AND USE

2.1 Service. Subject to and condition on Customer's compliance with the terms and conditions of this Cloud ID Addendum, Reseller shall deliver to Customer the Service described in the applicable Order Form and Service Schedule mutually agreed-to or acknowledged by the Parties. Except as otherwise specified, only Users may access and use the Service, during the Term, and on a non-exclusive, non-transferable basis. Customer may only use the Service for its internal business purposes. Each Party shall provide the other with reasonable cooperation, assistance, information, and access as may be lawful and necessary to initiate and thereafter provide Customer and its Users with access and use of the Service (such as, for example, developing any content, user interfaces or appearance specific to the Service contracted for by Customer). Customer agrees that Cloud ID may, in its sole and absolute discretion and without cost to Customer and minimal impact to Users, change data centers used in providing the Service.

2.2 Service Package Upgrade. Customer may upgrade the Service Package anytime during the Term by providing Reseller with at least one hundred (100) days prior, written notice. Upon the upgraded Service Package going into Production, Customer shall commence incurring and paying Fees applicable to such upgraded Service Package per the terms of the Order Form until the end of the Term.

2.3 Technical Support. Reseller will deliver the Service at the levels of performance and provide Customer with technical support services in accordance with the Service Level Agreement.

2.4 Limitations. Neither Cloud ID, nor Reseller, will be responsible for or liable in connection with any failure of the Service due to or resulting from: (a) any Customer Materials or Customer Systems; (b) negligent or intentional acts or omissions of Customer, its Affiliates, or any Person acting under the control and direction of Customer; (c) telecommunications or equipment failures outside of Cloud ID or Reseller's facilities or control; (d) scheduled maintenance; (e) use of the Service in a way that is not authorized or intended;

or (f) unauthorized access, breach, or other hacking by third parties of Cloud ID or Reseller's systems which occurs notwithstanding Cloud ID or Reseller's implementation of reasonable security procedures.

2.5 Data. As between Cloud ID, Customer and Reseller, Customer shall own all Account Information. Unless otherwise agreed to by Customer in advance and in writing, Cloud ID and Reseller shall not disclose to third parties or use any Account Information except as reasonably necessary to perform its obligations under this Agreement or to comply with any legal or regulatory requirement. To avoid uncertainty, Customer acknowledges and agrees that Cloud ID and Reseller may disclose aggregate measures (not personally identifiable information) of multiple Cloud ID clients' (as opposed to Customer specific measures) Users and Service usage and performance derived from Account Information to Cloud ID investors and other Cloud ID clients or potential clients for the purposes of permitting such persons to evaluate potential business relationships with Cloud ID, to maintain and improve the Service, or to develop relationships with or obtain investments from investors.

3. CUSTOMER RESPONSIBILITIES.

3.1 Customer Cooperation. Customer acknowledges that implementation and the continuing performance of the service and some Services may depend on Customer providing cooperation, assistance, information, and access to Cloud ID. If Customer fails to timely provide any of the foregoing, then Cloud ID and Reseller will not be liable for any resulting delay or failure in the Service's performance.

3.2 Customer Materials and Customer Systems. Customer will provide the Customer Materials and Customer Systems to Cloud ID as reasonably requested in connection with delivering the Service, or which Customer and Cloud ID agree should be integrated with the Service. Customer shall obtain, operate, and maintain in good working order the security and functionality of all Customer Systems needed for Users to connect to, access, or otherwise use the Service.

3.3 Provision of Test Accounts. Customer agrees to supply, upon Reseller's request, test accounts that Reseller may use to test (in test environment and Production) all Service releases. The number of test accounts provided and the specific attributes of these accounts will be determined in Reseller's reasonable discretion by the overall functionality that must be tested. These accounts will be maintained by Customer throughout the Term for the testing of regular Service releases and monitoring of Service functionality in Production. As account profiles change and functionality is added, Customer will provide additional test accounts or modify existing test accounts as requested by Reseller. Customer understands and agrees that without the test accounts, Reseller is not able to properly test the Service and Customer's specific implementation thereof.

4. LICENSE; INTELLECTUAL PROPERTY.

4.1 License Grant by Customer. Customer hereby grants to Cloud ID, and authorizes Reseller to grant on its behalf, a nonexclusive, non-transferable, worldwide and royalty-free right and license during the Term to use, reproduce, distribute, perform and display the Customer Materials provided to Cloud ID or Reseller, solely in connection with the Service and in a form approved by Customer (such approval not to be unreasonably withheld or delayed).

4.2 Ownership of Cloud ID Property. Except for the limited rights and licenses expressly granted in this Cloud ID Addendum, Cloud ID shall retain all right, title, and interest in and to the Cloud ID Property. Neither Customer nor Reseller shall use any Cloud ID Property, except as specifically provided in the Cloud ID Addendum. Any Cloud ID Technology used to deliver the Service will be installed, accessed and maintained only by or for Cloud ID and no license therein is granted to Customer or Reseller. Neither Customer nor Reseller may use and neither obtains any interest in the Cloud ID Property, except as expressly permitted by the licenses provided in the Cloud ID Addendum, and Cloud ID retains all right, title and interest in and to the Cloud ID Property. Customer shall comply, at Cloud ID's cost, with all reasonable request of Cloud ID to protect Cloud ID's rights with respect to Customer's use of the Cloud ID Property.

4.3 Restrictions Related to Cloud ID IP. Except as specifically permitted in this Cloud ID Addendum, neither Customer nor Reseller shall, directly or indirectly: (a) use any Cloud ID Property to create or make available any product, software, or service that is similar to the Service; (b) decompile, disassemble, reverse engineer or use any similar means to attempt to discover the source code of the Service or the trade secrets therein, or otherwise circumvent any technological measure that controls access to the Service; (c) encumber, transfer, rent, lease, or time-share the Service (except with any Affiliate of Customer, subject to Cloud ID's prior written consent) , or use them in any service bureau arrangement or otherwise for the benefit of any third party; (d) access, copy, distribute, manufacture, adapt, create derivative works of or otherwise modify the Service; (e) remove any proprietary notices; or (f) permit any third party to engage in any of the acts proscribed in clauses (a) through (e) above.

5. PERSONAL DATA

5.1 Personal Data. During the Term of this Cloud ID Addendum (and for any applicable period thereafter related to obligations related to this Cloud ID Addendum), each Party shall comply with all Data Protection Laws, as well as the terms and conditions of the Data Protection Addendum.

6. TERM AND TERMINATION.

6.1 Term. This term of this Cloud ID Addendum shall commence as of the Effective Date and shall continue thereafter in full force and effect for a period that is specified in the Order Form ("Term").

6.2 Termination for Cause. In addition to any of its other remedies, Reseller may terminate this Cloud ID Addendum: (a) if the Customer materially breaches any provision of the Cloud ID Addendum and the Customer fails to cure such breach within fifteen (15)

days after receiving written notice of such breach from the Reseller; or (b) immediately upon written notice to the Customer if (i) there is a material breach by the Customer that is incapable of cure, (ii) there is an assignment that is made by the Customer for the benefit of creditors, (iii) a receiver, trustee in bankruptcy or similar officer shall be appointed to take charge of any or all of such Customer's property or if a voluntary or involuntary petition under federal bankruptcy laws or similar state statutes is filed against the Customer, or (iv) the Customer dissolves or fails to operate in the ordinary course of business.

6.3 Effects of Termination. Upon any expiration or termination of this Cloud ID Addendum, all rights and obligations of the Parties shall cease, except that: (a) all obligations that accrued prior to the effective date of termination (including without limitation, all payment obligations) shall survive termination; and (b) each Party shall destroy or return to the other party all of the other's Confidential & Proprietary Information in its possession or under its control

6.4 Survival. All obligations of payment incurred or due through the date of expiration or earlier termination of this Cloud ID Addendum, and each of the provisions in Sections 2.5, 4, 5, 6.3, 6.4, 7.2, and 8, will survive the expiration or earlier termination of this Cloud ID Addendum.

7. REPRESENTATIONS AND WARRANTIES; DISCLAIMER OF WARRANTIES.

7.1 Customer Representations and Warranties. Customer represents and warrants to Reseller that, during the Term: (a) Reseller and Customer have all rights necessary to enter into and perform this Cloud ID Addendum and to grant the limited rights and licenses granted in this Cloud ID Addendum including, without limitation, all necessary consents and rights in the Customer Materials; (b) the use of any Customer Materials under this Cloud ID Addendum will not violate (i) Customer's obligations under any other agreement or to any third party, (ii) any applicable laws or regulations, or (iii) any privacy policies covering any Customer Materials; (c) the Customer Materials are not defamatory, obscene, or otherwise unlawful and do not infringe or interfere with any intellectual property, contract, right of publicity, or any other proprietary right of any individual or entity; (d) Customer will maintain throughout the Term a privacy policy on Customer's Digital Properties that make the Service available to Users that is compliant with all applicable laws, and (e) Customer will not make any representation or warranty concerning the Service or Services to any User or third party that is inconsistent with this Cloud ID Addendum.

7.2 DISCLAIMER OF WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS OTHERWISE SPECIFICALLY SET FORTH IN THIS AGREEMENT, THE SERVICE AND SERVICES ARE PROVIDED "AS IS", WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND CLOUD ID AND RESELLER SPECIFICALLY DISCLAIM AND MAKE NO WARRANTY, WHETHER EXPRESS OR IMPLIED, REGARDING THE SERVICES, INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, AND CLOUD ID AND RESELLER DO NOT WARRANT OR MAKE ANY REPRESENTATION REGARDING THE ACCURACY, ADEQUACY OR COMPLETENESS OF THE SERVICE OR SERVICES OR THE RESULTS TO BE OBTAINED FROM THE USE OF THE SERVICE OR SERVICES. CLOUD ID AND RESELLER DO NOT WARRANT THAT THE SERVICE OR SERVICES WILL MEET THE REQUIREMENTS OR EXPECTATIONS OF CUSTOMER OR THOSE OF ANY THIRD PARTY AND, IN PARTICULAR, CLOUD ID AND RESELLER DO NOT WARRANT THAT THE SYSTEM WILL BE ERROR FREE OR WILL OPERATE WITHOUT INTERRUPTION. NO ORAL OR WRITTEN ADVICE GIVEN BY CLOUD ID OR RESELLER OR AN AUTHORIZED REPRESENTATIVE OF CLOUD ID OR RESELLER WILL CREATE A WARRANTY WITH RESPECT TO THE SERVICE OR SERVICES. EXCEPT FOR CLOUD ID OR RESELLER'S FAILURE TO COMPLY WITH THE TERMS SET FORTH IN THIS AGREEMENT, CUSTOMER, UNDERSTANDS AND AGREES THAT CUSTOMER'S USE OF THE SERVICE AND SERVICES ARE AT CUSTOMER'S SOLE DISCRETION AND RISK. CUSTOMER ACKNOWLEDGE AND AGREE THAT THIS DISCLAIMER OF WARRANTIES WAS SPECIFICALLY BARGAINED FOR AND ARE ACCEPTABLE TO CUSTOMER AND THAT CUSTOMER'S WILLINGNESS TO AGREE TO THIS DISCLAIMER OF WARRANTIES IS MATERIAL TO RESELLER'S DECISION TO ENTER INTO THIS CLOUD ID ADDENDUM. THIS DISCLAIMER OF WARRANTIES WILL BE ENFORCEABLE TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

8. LIMITATIONS OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE LIABILITY OF CLOUD ID AND/OR RESELLER TO THE CUSTOMER, IF ANY, AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM OF ANY KIND WHATSOEVER ARISING OUT OF OR RELATING TO THE SERVICE, SERVICES AND/OR THIS CLOUD ID ADDENDUM, REGARDLESS OF THE LEGAL THEORY, INCLUDING, WITHOUT LIMITATION, IF BASED ON BREACH OF CONTRACT, NEGLIGENCE, INFRINGEMENT OF ANY THIRD PARTY RIGHTS, PRODUCT LIABILITY, INDEMNITY, SUBROGATION, OR CONTRIBUTION, SHALL NOT EXCEED THE ACTUAL COMPENSATION PAID TO RESELLER BY CUSTOMER FOR WHICH A CLAIM ARISES DURING THE THEN IMMEDIATELY PAST TWELVE (12) MONTHS . WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, UNDER NO CIRCUMSTANCE WILL CLOUD ID AND/OR RESELLER BE LIABLE TO THE CUSTOMER FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND WHATSOEVER, INCLUDING, WITHOUT LIMITATION, REIMBURSEMENT OR DAMAGES ON ACCOUNT OF DAMAGES FOR SUBSTITUTE SERVICE OR SERVICES, LOSS OF USE, LOSS OF PROFITS, LOSS OF GOODWILL, LOSS OF PRIVACY, LOSS OF DATA, LOSS OF OPPORTUNITY, OR OTHER INTANGIBLE LOSSES (EVEN IF CLOUD ID HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES). EACH PARTY ACKNOWLEDGES AND AGREES THAT THIS LIMITATION OF LIABILITY WAS SPECIFICALLY BARGAINED FOR AND IS ACCEPTABLE TO EACH PARTY AND THAT A PARTY'S WILLINGNESS TO AGREE TO THIS LIMITATION OF

LIABILITY IS MATERIAL TO EACH PARTY'S DECISION TO ENTER INTO THIS CLOUD ID ADDENDUM. THIS LIMITATION OF LIABILITY WILL BE ENFORCEABLE TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

9. GENERAL PROVISIONS.

9.1 Modification. This Cloud ID Addendum may be modified from time to time by Reseller as required by Cloud ID, without materially changing the bargained value of the applicable order form, and binding with notice to Customer.

9.2 Confidential Information of the other Party.

9.3 Notices. All notices provided under this Agreement must be in writing, delivered to the address set forth on the signature page to this Agreement (or such other address as set forth in this Agreement for the applicable type of notice or such other address as a Party provides to the other Party pursuant to the terms of this section), and will be deemed to have been duly given (a) when received, if personally delivered; (b) the day after being sent, if sent for next day delivery by a nationally-recognized overnight delivery service; or (c) when recipient confirms reception of such communication, if transmitted by facsimile or e-mail.

9.4 Prevailing Party Attorneys' Fees. The prevailing party in any legal proceeding or proceeding seeking injunctive relief arising out of or related to this Agreement will be entitled to an award of their reasonable attorney's fees and costs (including, without limitation, all taxable and non-taxable costs, and all fees and costs to determine the amount of fees and costs to be awarded) incurred prior to any such legal proceeding or proceeding seeking injunctive relief, as well as at all levels of trial and appeal, and including expert fees and costs.

9.5 Headings. Headings are for convenience only and shall in no way affect interpretation of the Agreement.

[Exhibits to Follow]

Exhibit B

SERVICE SCHEDULE - DESCRIPTION OF SERVICE AND SERVICES

1. SERVICE

(a) **Service.** On behalf of and through Reseller, Cloud ID shall provide Customer with the Service and Services set forth in the Order Form and further described in this Service Schedule. Specifically, Customer desires to provide a subset or all of their Subscribers, or a subset or all of its partners and their subscribers, the ability to consume their partners Content or other licensed content via the Internet, either directly or through commercial agreements with Content Providers, pursuant to the Subscriber's agreement with Customer. Cloud ID will provide a Service whereby the criteria of eligibility for Subscribers will be determined from data provided by Reseller, on behalf of Customer, to Cloud ID, combined with data received by Cloud ID from Content Providers. This determination will be used to enable authorized Subscribers to access relevant Content, including distribution by Customer to Content Providers under commercial agreements between Customer and such Content Providers, subject to the terms and conditions of the Cloud ID Addendum.

(b) **Service Level Agreement.** Cloud ID will provide the Service consistent with the Service Level Agreement.

(c) **Limitations.** In addition to those limitations set forth in the Cloud ID Addendum, Customer authorizes Reseller to represent and, agree on its behalf, that it acknowledges and agrees that Cloud ID will not be responsible for, nor liable in connection with (i) the quality, functionality, or availability of the Content; (ii) the quality, functionality, or availability of a Content Provider's Connected-Services or interconnection endpoints, including any interruptions or performance issues arising from such Connected-Services; (iii) any willful or negligent acts or omissions by the Reseller, Customer, other Content Providers, or Service Providers; (iv) incorrect or incomplete data provided by Reseller, Customer, other Content Providers, or Service Providers; or (v) any issues reasonably outside of Cloud ID's control, including but not limited to, delays or failures resulting from external dependencies or system outages. Reseller, on behalf of Reseller and Customer, also acknowledges and agrees that Customer must maintain a valid legal agreement with any Content Provider involved in the distribution of Content. Cloud ID shall not be liable for any delays, interruptions, or other issues resulting from the establishment, renewal, or operational management of such agreements between Customer and the Content Providers.

2. CUSTOMER/RESELLER RESPONSIBILITIES

(a) **Rights to Content.** Customer authorizes Reseller to represent and agree on Customer behalfthat it shall ensure it has all rights and licenses necessary from all Content Providers with which it wishes Cloud ID to integrate its Cloud ID Platform (i) to allow Cloud ID to perform its obligations under this Service Schedule, and (ii) to allow Customer's Subscribers to access, view, or consume such Content or Connected-Services on the Technology Properties. Cloud ID shall not be obligated to begin integration of the Service related to any Content Provider with whom Customer does not yet have an agreement in place granting Customer such rights. If at any time during the Term, such rights or licenses terminate or are modified in any way that affects the Service provided to Customer, Customer shall as soon as commercially reasonable give notice of the same to Reseller, after Customer becomes aware of such termination or modification. In the event such rights or licenses are terminated, Customer will promptly modify its backend systems to disallow Customer's Subscribers from accessing, viewing or consuming Content on the Technology Properties using the Service. If such rights or licenses are modified, Customer and Reseller shall promptly make the necessary changes to comply with such modification. Cloud ID shall not have any liability to Customer or Reseller in the event Cloud ID disables the integration of the Service with the terminated Content Provider or with regard to terminated Content upon receipt of notice from Reseller indicating its rights or license with such Content Provider has terminated.

(b) **Content Entitlement.** Customer understand and agree that any authorization that occurs through the Service is based on Customer's data that identifies which Users are authorized to access certain Content online based on their subscription rights. Customer will ensure that Customer and Customer's Content Providers accurately maintain such data, provide Cloud ID continuous access to such data, and will not, at any time, permit access to Content to any Users who are not entitled to such access. Cloud ID agrees that, as between Cloud ID, Reseller and Customer, such data is owned by Customer, and Cloud ID shall only have the right to use such data to fulfill Cloud ID's obligations under the Cloud ID Addendum. Customer and Reseller shall also ensure that each Content Provider provides Cloud ID the necessary Content data and assistance to perform the integration with such Content Provider, and that the data provided by each Content Provider is accurate.

(c) **Compliance with Content Provider Requirements.** Content Providers may, from time to time, require Cloud ID to pass through to Customer through Reseller certain requirements in order to allow the integration of such Content Provider's data with the Cloud ID Platform. To the extent a Content Provider has specified any such requirements to Cloud ID, Cloud ID will provide the Customer through Reseller a separate attachment to the Cloud ID Addendum specifying such Content Provider requirements. If Customer wishes to allow their Subscribers access to such Content, such attachment will be executed by Cloud ID and Reseller and become a part of the Cloud ID Addendum. If compliance with this provision causes Cloud ID to incur any cost, then Reseller shall pay or reimburse Cloud ID for such costs.

(d) **Determination of Launch Dates.** Cloud ID and Reseller shall work together to determine a target date for the Service to first become operational and the integration timeframes for each of the Content Providers. Customer and Reseller agrees not to commit to an integration date for any Content Provider without Cloud ID's input and written agreement. Notwithstanding the foregoing, Customer and Reseller shall begin integration work with Cloud ID no more than sixty (60) days after the Effective Date.

(e) **Changes to Integration Parameters.** Reseller acknowledges and agrees that any changes to the initial integration specifications must be mutually agreed to by Cloud ID and Reseller and communicated by Reseller to Cloud ID in writing at least sixty (60) days before the date that such change is to take effect.

3. REMOVAL OF PROVIDERS.

(a) **Right to Remove Individual Content Providers.** Cloud ID shall have the right to suspend or disable any integration with any Content Provider upon prior notice to Reseller (which will be passed to Customer): (i) if Cloud ID reasonably believes the use of the Content Provider's data would result in the violation of third party intellectual property rights or otherwise expose it to potential legal liability; (ii) if the integration with the Content Provider is causing the Cloud ID Platform or the Service to malfunction; or (ii) if Cloud ID's right to integrate with such Content Provider otherwise ceases. In each case, Cloud ID will provide Reseller as much notice as is reasonably practical in such circumstances.

4. CLOUD ID MEDIA CONNECT SERVICE

Basic Integration Approach

The integration of Cloud ID Media Connect with any additional websites or applications of Customer must be approved in writing by Cloud ID.

Cloud ID will provide integration of Customer's authorized Content Providers that are in the Federated Directory of Content Providers using the most recent versions of authentication protocols. Cloud ID reserves the right to refuse non-standard integrations and to request the Content Provider to comply with the authentication and authorization standards.

Media Connect Service Introduction

Media Connect for Content Providers enables a Content Provider to develop new sales channels with Content Provider partners. This functionality is done by authenticating Users to the identities registered with the Content Provider and authorizing if the User's paid package gives them entitlement to the content.

Essential Package Features

Authentication and Authorization

- **Federated:**
  - Proxied authentication with Content Providers – Allowing Users to log in with their existing MVPD credentials, normalized so the authentication artifacts are returned to the CP in homogenous format.
  - Content Provider Pickers **–** Makes available all the data to create a picker where Users can select their MVPD to log in.
  - AuthZ - single entitlement lookup **–** An API that indicates to the CP if a User has a package that includes the content they are trying to access.
  - Multi AuthZ - Package Entitlement Lookup **–** Extending on the single check, this API can check if a User has the entitlement to access multiple content sources in one request.
- **Fraud Management & Reporting**
  - **Monitoring & Alerting** – 24/7/365 monitoring and automated alerting to ensure a Cloud ID customer's identity services stay up and running.
  - **Basic Reporting** – One report sent per month showing the following metrics:

- Unique MAUs for a given period
- Number of AuthN and AuthZ requests for a given period

Advanced Package Features

Authentication and Authorization

- **Concurrency Monitoring:** Per User– Configure and enforce the number of concurrent streams per User belonging to specific MVPD.

Ultimate Package Features

Authentication and Authorization

Lifecycle Management:

- **Self-Serve End Use Management –** A Cloud ID portal for Users to manage all their identity details.
- **Head of Household Management –** A primary User of a household can manage the identity of other Users and even bless other Users with the same administrative privilege.
- **Administrative User Management –** Customer service agents and other administrators can utilize this portal to aid Users in solving their identity issues.
- **User / Credential Interactions:**
- **Storage** – Cloud ID can be the storage mechanism and source of truth for User and credential data.

5. ADDITIONAL DETAILS

a. General Overview:

i. Act as authentication integration aggregator to Customer's Technology Properties. Customer's Technology Properties include, but may not be limited to, Customer's applications including:

- Websites
- Android smart phones and tablets
- Apple iPhone and iPad (iOS)
- Connected TVs with Amazon Fire TV, Apple TV and Roku

ii. Provide access to login pages as described below to support the above, branded as requested by Customer to Reseller.

iii. Answer authorization queries regarding Content and services to which an authenticated User is entitled based on their current active subscription with Customer and Provider.

iv. Provide to Customer via Reseller authentication and authorization information related to both individual User accounts and the household account as needed and as possible given the account information available from Content Providers.

v. Integrate with the Content Provider systems for both authentication (username/password) and authorization (User subscription) to verify User subscription information.

vi. Provide additional User data to Customer via Reseller, such as parental control settings, as provided by the Content Provider, if applicable. Integration of the Services with Customer's Technology Property.

b. Cloud ID will integrate the Customer's Technology Properties into the Cloud ID Platform such that when Customer initiates a request utilizing SAML or other secure authentication and authorization integration technology and protocols, the Content Provider's login pages will be presented to the User. Such login page will be hosted by the Content Provider, including possible co-branding with the Customer's logo and Content Provider's logo.

c. Upon successful login, the Cloud ID Platform generates a secure response and redirects the User to the Customer Technology Property. The Customer Technology Property receives the secure response with the opaque identifier that the Content Provider provided for the User and any other required information sent by the Content Provider.

d. After authentication, the Customer Technology Property can then issue an authorization call directly to the Cloud ID Platform to confirm that the User's subscription contains the required products; the typical case will confirm that the User is authorized to access the requested Content or Connected-Service. Depending on the response, the Customer Technology Property may allow access to the Content or Connected-Service, or display an agreed upon message that might be an error message or an up-sell message.

e. Aggregated API Integration with the Cloud ID Platform:

i. For the purposes of authentication and authorization, the Customer and Content Provider will integrate with Cloud ID Platform API Interface. Cloud ID and Reseller will mutually agree to the appropriate authentication integration method, but regardless of such integration method. Customer and Reseller will be insulated from the specifics of the secure communication with each Content Provider. Only the integration between the Customer and the Cloud ID Platform will be necessary.

f. Content Provider Provision of Account Information:

i. The Content Provider must provide Cloud ID Platform APIs the following Account Information and other items to facilitate the provision of the Services:

- Opaque or unique identifiers for each User which allows to map the event to the Content Provider's Subscriber;
- Subscriber's, OS, device type or user-agent;
- Subscriber's IP;
- authorization information for Customer's Content, such as what Content a User has access to, if any;
- parental controls information; and
- any other information required to comply with Customer's rules regarding the availability of the Content to their Subscribers.

g. Protection of User and Provider Information:

h. The username and password are protected by the Content Provider by having them entered in the Content Provider login page only. The individual User will be identified to the Customer as a machine generated opaque ID generated by Cloud ID or the Content Provider and will remain anonymous. No personally identifying information shall be passed.

Exhibit C

SERVICE LEVEL AGREEMENT

1. GENERAL.

1.1 SLAs. Cloud ID directly or via Reseller shall provide the Service consistent with the service levels set forth in this Service Level Agreement (each, an "SLA") twenty-four (24) hours a day, seven (7) days a week, three hundred sixty five (365) days a year.

1.2 Exclusions. The SLAs exclude events resulting from failures of a Provider or other third party provider hosting or delivery systems, Customer authentication and authorization systems, acts of God, war, acts by civil or military authorities, energy shortages, or other causes beyond Cloud ID's reasonable control, whether or not similar to the foregoing (collectively, the "SLA Exclusions").

1.3 Contact Information. Cloud ID Contact Information:

(a) Technical Service Support: 866.535.8286 or tss@synacor.com

(b) Network Operations Center: 800.716.8347 or noc@synacor.com

2. MONITORING AND REPORTING In an effort to detect potential problems before impacting API Availability (as defined below), Cloud ID will, upon receipt of appropriate test accounts from Customer, continuously monitor the status of Cloud ID's systems using both automated and manual tools employed in Cloud ID's 24 by 7 network operations center. Customer acknowledges and agrees that such monitoring is not fully possible without the appropriate test accounts.

3. API AVAILABILITY.

3.1 API Evaluation. API Availability (as defined below) will be evaluated on a monthly basis by Cloud ID.

3.2 API Availability.

(a) **Definitions**.

i. "API Availability" means that the Service is Fully Functional on a 99.9% average in a calendar month.

ii. "API Unavailability" means the failure of the Service to be available consistent with the API Availability.

iii. "Fully Functional" means the Service is continuously operable, available, and responsive to Users without significant delay or malfunction.

iv. "Security Intrusion" means a network or system intrusion, including, without limitation, a denial of service attack or other unauthorized access or malicious code affecting a network or system ("Security Intrusion").

(b) **Exclusions**. API Availability excludes:

i. downtime or degradation attributable to maintenance;

ii. the inability of Users to access Content or a Connected Service as a result of such Users' Internet or network connection;

iii. impediments affecting the path (route) traveled in accessing Cloud ID's systems, except for those facilities owned, operated or maintained by Cloud ID or by a third party on behalf of Cloud ID;

iv. downtime or degradation resulting from bugs in third-party software or content not caused by Cloud ID;

v. the inability of Providers to update or deliver Content or a Connected Service due to circumstances not within Cloud ID's control;

vi. downtime or degradation attributable to a Security Intrusion;

vii. downtime or degradation attributable to problems with Customer-provided data API's, authentication mechanisms, or similar services;

viii. downtime or degradation attributable to Provider, a vendor retained by Customer or a Provider, or other third party

providers performing maintenance on Content or a Connected Service, APIs, or otherwise that may affect Cloud ID's API Availability; and

ix. the SLA Exclusions.

(c) **Third Party Maintenance by or on behalf of Customer**. If Customer or Reseller is provided notice of any Provider performing maintenance which could affect the Service, then Reseller, on Customer's behalf where Customer has notified Reseller, shall promptly notify Cloud ID in advance or immediately upon becoming aware of such maintenance taking place.

3.3 Calculation. Due to Cloud ID's distributed architecture and redundancy, it is likely that API Unavailability. may only affect a subset of the total User base. Therefore, API Unavailability will be calculated based upon the percentage of Users who are experiencing API Unavailability compared to Customer's total User base. For example, if ten percent (10%) of the User base is experiencing API Unavailability for thirty (30) minutes during a thirty (30) day month, then the API Unavailability for that month is based on three (3) minutes of unavailability for an API Unavailability of 99.99%.

3.4 Credits. If Reseller, on behalf of Customer, makes a written request to Cloud ID within thirty (30) days of the end of the month in which Cloud ID failed to meet the API Availability, then the API Availability credits set forth below will be applied to Customer's account for such month ("Credit"). To the extent possible, a Credit will be applied during the billing period following the month in which such Credit is incurred and shall be detailed as a separate line item on the invoice.

(a) **Credit Calculation**. A Credit of one percent (1%) of the Monthly Platform Fees owed by Customer under the Cloud ID Addendum in the applicable month, plus an additional one percent (1%) of such Monthly Platform Fees for every increment of 0.1% by which API Availability fails to meet the API availability percentage, up to a maximum of fifty percent (50%) of the Monthly Platform Fees which would otherwise have been payable by Customer to Cloud ID for the applicable month.

(b) **Chronic API Unavailability**. If Cloud fails to meet the API Availability during the time periods set forth below, then in addition to the applicable Credits, Customer shall have the right to terminate the Cloud ID Addendum upon thirty (30) days written notice to Cloud ID:

i. three (3) or more separate occasions, each lasting eight (8) or more hours, over the course of any rolling three-month period;

ii. twenty-four (24) hours aggregated over any rolling thirty (30) day period of time;

iii. sixty-four (64) hours aggregated over any rolling ninety (90) day period of time.

4. CUSTOMER CHANGES OR ACTIONS.

4.1 Changes. Customer acknowledges that it or third party providers may have the ability to take actions or make changes which can adversely affect the performance of the Service. In some cases, Cloud ID may be able to mitigate the risk of the actions or changes if Customer provides notice to Cloud ID via Reseller in advance of the change. Cloud ID will not be responsible for any downtime, degradation or other SLA-related problems that were caused, in whole or in part, by the change. Cloud ID makes no representation or warranty that any Customer or Provider change will be successful and Cloud ID shall have no liability for any changes or modifications by Customer or any third party. Customer should always provide a reasonable amount of notice to Cloud ID via Reseller before taking any actions or making any changes that may adversely affect the performance of the Service, as the case may be, and Cloud ID reserves the right to require a postponement of any actions that it believes requires mitigation before deployment. Degradation in performance resulting from Customer or third party provider changes will not be covered by the SLA.

4.2 Service.

Action / Change	***Risk***	***Cloud ID Mitigation***	***Required Notification***
Changes to Cloud ID-facing API's and data exchange mechanisms.	If login or Customer data API's change, consumers may be unable to log in or access the Service.	Cloud ID will need to change all integration code, perform Unit and Regression testing, and then release the code to the Production servers. This is normally a four to eight week process.	Notification is requested a minimum of eight weeks prior to implementation.
Changes to Customer's network.	Variable risk depending on scope of change.	Cloud ID's network team will assess the impact of the	Cloud ID requires 72 hours' notice of maintenance or

		change.	testing that may have an impact on access to the Service.
Changes / configurations to Name Service	Access to service may be disrupted; variable risk depending on scope of change.	Cloud ID's network team will assess the impact of the change.	A minimum of three days' notice is needed for consultation
Changes or renewals for certificates used in the Cloud ID/Customer integration	Access to service may be disrupted; variable risk depending on scope of change.	Cloud ID's systems team will assess the impact of the change.	A minimum of four weeks' notice is needed for consultation

5. SECURITY.

5.1 Security Team. Cloud ID's security team proactively evaluates network security risk, develops and implements policies and incident prevention programs, educates management and staff about security policies, and handles computer security incidents.

5.2 System Intrusion. In the event of a System Intrusion, affected parties will be notified and a solution will be implemented. Notification will occur upon confirmation by Cloud ID's security team that there was a bona fide System Intrusion.

5.3 Network Security. Cloud ID maintains network firewalls and intrusion detection devices to prevent unauthorized access to the network infrastructure and systems. Network attacks such as denial-of-service attacks are logged. Cloud ID will notify Customer when such attacks are verified.

6. MAINTENANCE WINDOWS.

6.1 Scheduled Maintenance Windows. Cloud ID reserves one or more windows, for weekly application revision/infrastructure maintenance, should the need for such maintenance arise. Typically, Cloud ID conducts scheduled maintenance in a three (3) hour window from 2:00 AM to 5:00 AM Eastern Time every Monday and application maintenance during a four (4) hour window from 3:00 AM Eastern Time to 7:00 AM Eastern Time every Tuesday. However, Cloud ID may move or add scheduled maintenance windows, as necessary. During these scheduled maintenance windows and any extensions thereof, the system and services may be unavailable to Customer and Users. Scheduled maintenance windows and extensions thereof are not counted against API Availability percentages.

6.2 Emergency Maintenance Notification. In the event that emergency maintenance is required outside of scheduled maintenance windows and such emergency maintenance will have a material adverse effect on Users, Cloud ID will make reasonable efforts to notify Reseller, who will then notify Customer, about the emergency maintenance window. Notification will be based on practicality and the degree of adverse effect on the applicable Service or availability thereof.

7. CUSTOMER SUPPORT PROCEDURES.

7.1 Incident Management.

(a) **Tier 1** – Reseller will provide first level support to Users, consisting of (i) handling questions from Users regarding customer/technical support, order processing, and use of the Service; and (ii) accepting and responding to problem calls from Users relating to the Service as set out in Cloud ID Addendum; (iii) supporting User devices and underlying Customer Systems and architecture; (iv) providing notification to Cloud ID of changes, maintenance, outages of underling systems that may affect Service.

(b) **Tier 2/Tier 3** – Cloud ID will provide second level support to Reseller and only interact with a Customer with the approval and cooperation of Reseller, consisting of (i) accepting and responding to problem escalations reported by Users or other representatives of Customer with regard to problems that cannot be resolved by Customer or Reseller, (ii) resolving reported problems as set forth in the Cloud ID Addendum, and (iii) providing notification to Reseller of changes, maintenance, outages of underlying systems that may affect Service.

(c) Cloud ID will provide Reseller with the following for Customer:

i. Technical support offered in English.

ii. Email address for submitting Tier 2 level support incidents to Cloud ID.

iii. Phone support twenty-four (24) hours a day, seven (7) days a week, three hundred sixty five (365) days a year.

7.2 Priority. Reseller (with the Customer) will estimate the priority of an incident at the time the incident is reported. The priority can change at any time during the process. Incidents will be categorized by product category, with the following priority definitions:

(a) "Priority 1" or "(P1)" means that the Service is substantially non-operational such that it causes severe commercial impact and there are no known workarounds.

(b) "Priority 2" or "(P2)" means a problem with the Service that causes significant commercial impact which cannot be resolved (temporarily) by workarounds.

(c) "Priority 3" or "(P3)" means a non-critical problem or incident with the Service where Customer is able to continue to utilize the Service and a workaround is not available.

(d) "Priority 4" or "(P4)" means an incident that is not a P1, P2, or P3 incident, is non-critical, and for which an applicable workaround is available.

(e) "Support Response Time" means the elapsed time between the incident escalation by Reseller and the time within which Cloud ID begins support as verified by a verbal or email confirmation to Reseller.

Standard Support Response Times are as follows:

Incident Priority	Initial Cloud ID Response	System Fix or Workaround Implemented
P1	1 hour	24 hours
P2	2 hours	48 hours
P3	24 hours	2 weeks
P4	72 hours	Scheduled within the next appropriate release schedule

7.3 Incident Calls. Cloud ID will be responsible for the control and management of incident calls and assignment of priority and escalation to resources within Cloud ID in its sole and absolute discretion.

7.4 Non-Service Items. Non-Service impacting support escalations, such as feature requests, long-term improvements, documentation requests, general inquires, etc. are not covered by the resolution timelines.

7.5 Exclusions. Support Services do not cover (i) third party products, including the interface of the Service with the third party products; (ii) use of the Service with unsupported tools APIs, interfaces, or data formats other than those included with the Service and supported as set forth in the Documentation; (iii) any custom developments or integrations that were not provided as part of the Service by Cloud ID. Reseller may request assistance from Cloud ID for such problems, for an additional Professional Services Fee.

7.6 Escalation Path. The escalation process consists of the reporting, troubleshooting, diagnosis, and resolution processes. All incidents are assigned to a Cloud ID support engineer substantially in accordance with the standard support response times set forth above. However, Cloud ID may choose from time to time to handle issues outside of the escalation path indicated below if, in Cloud ID's reasonable judgment, such issues either need to be escalated more quickly or can be resolved without escalation.

Escalation Levels	Escalation Response Time	Cloud ID Contacts
Level 1	Cloud ID Technical Support Agents available 24 hours per day, 7 days per week for Cloud ID Issues; M-F for Cloud ID issues.	Cloud ID TSS Team tss@synacor.com
Level 2	Level 2 Support Contact should be contacted if the issue is not answered within 15 minutes.	Support Lead Jackson Tomei jackson.tomei@synacor.com
Level 3	Level 3 Support Contact should be contacted if the issue is not answered within 30 minutes from either Level 1 or Level 2.	Director Global Support Shashank Tewari

		shashank.tewari@synacor.com
Level 4	Level 4 Support Contact should be contacted if the issue is not answered within 60 minutes from Level 1, Level 2 or Level 3	SVP Operations Ian Mitchell imitchell@synacor.com

8. SOLE REMEDY. Reseller and Cloud ID's sole obligation, and Customer's sole remedy , for a violation of any SLA set forth in this Service Level Agreement is that Reseller with provide Customer any issuance of a Credit to Reseller from Cloud ID, or the right of Customer and/or Reseller to terminate the Cloud ID Addendum and Related Order Form for chronic API Unavailability, pursuant to the terms set forth in this Service Level Agreement.

EXHIBIT D

FEDERATED CONTENT PROVIDER ADDENDUM

ABS-CBN
AE Networks
Altitude Sports
AMC Networks
AT&T SportsNet
BEINSport
C-SPAN
Crown Media
Discovery, Inc.
Disney/ESPN
EPIX
Sinclair
FOX
Fuse
HBO
MASN
Marquee Sports
MLB Network
MLB.TV
AT&T SportsNet - MLB
ROOT SPORTS - MLB
AT&T SportsNet - MLB
MSGGO
Music Choice
NBCu
National Football League
NESN
News 12
Newsmax
NewsNation
NHL
Ovation
PAC12
REELZ
REVOLTTV
Showtime
Spectrum Sports
STARZ
Tennis Channel
The Weather Channel
Turner
TV5MONDE
TVOne
Univision
CBS
Paramount
Weather Channel
YES Network

EXHIBIT E

DATA PROCESSING ADDENDUM

Last Updated: April 18, 2025

For purposes of this Data Processing Addendum, the term Parties will include, Cloud ID, to the extent that Cloud ID is a Controller herein.

Pursuant to the Agreement, each of the Parties may act as a Controller (as defined below) with respect to Personal Data (as defined below) collected from its employees and/or customers. These same Parties may act as a Processor (as defined below) with respect to Personal Data collected from employees and/or customers of another party. The Parties agree to comply with the provisions of this Addendum with respect to the Processing (as defined below) of any and all Personal Data collected on behalf of or submitted by Controllers pursuant to the Agreement. The Parties also agree to comply with all applicable Data Protection Laws with respect to such Personal Data.

1. DEFINITIONS

For purposes of this Addendum, the following capitalized terms have the meanings set forth below. Capitalized terms used, but not defined, in this Addendum have the meaning ascribed to such terms in the Agreement:

1.1. "Appropriate Safeguards" means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time.

1.2. "Authorized Person" means a person or category of person that Controller authorizes Processor to allow to Process Personal Data, including employees and contractors of Controller, employees and contractors of Processor, and employees and contractors of Subprocessors.

1.3. "Business Purposes" means the services described in the Agreement or any other purpose specifically identified in Exhibit A.

1.4. "Controller" has the meaning ascribed to such term in the applicable Data Protection Laws.

1.5. "Data Breach" means any suspected, potential, or actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Personal Data. This shall include any use or disclosure of Personal Data not provided for by the Agreement or this Addendum.

1.6. "Data Subject" means an individual who is the subject of the Personal Data and to whom or about whom the Personal Data relates or identifies, directly or indirectly.

1.7. "Data Subject Request" means a request made by a Data Subject, user or other individual conferred rights under Data Protection Laws.

1.8. "Data Protection Laws" means, collectively, all applicable data privacy and security laws and their implementing rules and regulations, as amended or superseded from time to time, that exist at any time during the Term, including, without limitation, the (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (commonly referred to as the General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) the Swiss Federal Act on Data Protection; (iv) the United Kingdom General Data Protection Regulation, and the UK Data Protection Act 2018, as amended (the "UK GDPR"); (v) U.S. Data Privacy Laws; and (vi) other laws and their implementing rules and regulations that address the Processing of Personal Data or Personal Information.

1.9. "EEA" means the European Economic Area.

1.10. "Personal Data" or "Personal Information" have the meaning ascribed to such terms in the applicable Data Protection Laws, except that Personal Data as used in this Addendum will only refer to Personal Data which has been, or is intended to be,

Processed by a Processor pursuant to or in connection with the Agreement. For purposes of clarity, any reference in this Addendum to Personal Data or Personal Information includes reference to the other term or both terms, as applicable.

1.11. "Process", "Processed", or Processing" means the collection, accessing, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, sharing, disclosure, dissemination, alignment or combination, restriction, erasure, and destruction of Personal Data.

1.12. "Processor" has the meaning ascribed to such term in the applicable Data Protection Laws.

1.13. "Standard Contractual Clauses" means the controller to processor clauses (Module 2) and processor to processor clause (Module 3) for the transfer of Personal Data from the EEA to Processors established in non-EEA countries that do not provide an adequate level of data protection approved by the European Commission Implementing Decision of 4 June 2021, as currently set out at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914. Annex I, Annex II and Annex III to Exhibit A (each, an "Annex") sets forth information applicable to the Standard contractual Clauses.

1.14. "Regulatory Authority" means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

1.15. "Sub-Processor" has the meaning ascribed to such term in the applicable Data Protection Laws.

1.16. "U.S. Data Privacy Laws" means, collectively, all applicable U.S. state and federal data privacy and security laws and their implementing rules and regulations, as amended or superseded from time to time, that exist at any time during the Term. The terms "Consumer", "Contractor", "Service Provider", "Share", "Shared", "Sharing", "Sale", "Selling" and "Third Party" have the meaning ascribed to such terms in the applicable U.S. Data Privacy Laws.

2. ROLES OF THE PARTIES

2.1. The Parties agree that Controllers will determine the scope, purposes, and manner by which Personal Data may be processed by Processors. The Processors will Process Personal Data only as set forth in Controllers' written instructions. As such, pursuant to the Data Protection Laws, Controllers are the controllers and Processors are the processors. The Controllers retain control of the Personal Data and remain responsible for its compliance obligations under any Data Protection Laws, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Processors.

2.2. Processors acknowledge and agree that, under the terms of the Agreement, Processors receive or have access to Personal Data. Processors shall comply with the terms and conditions set forth in this Addendum when Processing Personal Data that is in their possession or control. Unless otherwise expressly stated herein, Processors shall fulfill all obligations set forth in this Addendum at Processors' sole cost and expense. Processors shall only Process Personal Data to fulfill the Business Purposes of the Agreement. Controller discloses the Personal Data to the Processors only for the limited and specified Business Purposes of the Agreement.

3. OBLIGATIONS OF THE PROCESSORS

3.1. Processors shall, with respect to Processing Personal Data on behalf of Controllers:

a) Process Personal Data only on documented instructions from Controllers. Processing includes any proposed transfers of Personal Data to a third party. Processors shall seek approval from Controllers, unless the transfer of Personal Data is required by a law to which Processors are subject, or if the transfer is otherwise permissible pursuant to this Addendum. If the Processors are legally required to transfer Personal Data, Processors shall inform Controllers of that legal requirement before Processing, unless that law prohibits such notification. Controllers' instructions on Processing may be specific instructions or standing instructions of general application in relation to the performance of Processors' obligations under any contract or agreement between the Parties.

b) Process Personal Data only in accordance with Data Protection Laws, the Agreement, and this Addendum.

c) Limit Processing of Personal Data to activities reasonably necessary and proportionate to achieve the Business Purposes or another compatible operational purpose. Therefore, Processors will rely on Controllers to provide notice

to individuals addressing Processors' use of Personal Data. If, however, the Business Purposes require the collection of Personal Data from individuals on Controllers' behalf, Processors shall provide notice to the individuals addressing Processors' use and collection methods. The notice shall comply with Data Protection Laws and Controllers shall pre-approve such notice. Processors shall not modify or alter the notice in any way without Controllers' prior written consent.

d) Keep and maintain, in accordance with Data Protection Laws, electronic records of all categories of Processing activities carried out on behalf of Controllers.

e) Ensure that Processors and Subprocessors Authorized Persons shall be subject to a strict duty of confidentiality by contract and by law, where applicable. Processors shall not permit any person not subject to strict confidentiality to Process Personal Data. Processors accept responsibility for any breach of this Addendum caused by the act, error, or omission of an Authorized Person of Processor or a Subprocessor.

f) Implement and maintain commercially reasonable measures with respect to the security of Processing Controllers' Personal Data and in compliance with this Addendum and Data Protection Laws.

g) Taking into account the nature of the Processing, assist Controllers by technical and organizational measures, insofar as this is possible, for the fulfillment of Controllers' obligation to respond to (i) any Data Subject Request, including but not limited to requests for access, rectification, erasure, opt-out and all similar requests, and will not respond to any such requests unless expressly authorized to do so by Controllers, or (ii) any complaint relating to the Processing of Personal Data by Processors. Processors will cooperate with Controllers with respect to any action taken relating to such request or complaint.

h) Assist Controller in ensuring compliance with the obligations under Data Protection Laws with respect to:

i) security of Processing;

ii) notifications to applicable Regulatory Authorities and Data Subjects in case of any Data Breach;

iii) data protection impact assessments (as such term is defined in Data Protection Laws); and

iv) consultation and communication with any Regulatory Authority in connection with legal and regulatory requirements imposed by Data Protection Laws.

i) Processors shall: (a) securely maintain Controllers' historical data. However, at Controllers' sole discretion, Processors shall delete or return all Personal Data, including copies to Controllers, unless Data Protection Laws require retention and storage of Personal Data and Processors so notify Controllers of such requirement; and (b) ensure that all third parties supporting Processors' Processing of Personal Data take the same action. Processors shall make available to Controllers all information necessary to demonstrate compliance with the obligations in this Addendum and allow for and contribute to audits, including inspections, conducted by Controllers or another auditor mandated by Controllers.

3.2. Processors shall immediately notify Controllers if, in their opinion, an instruction infringes Data Protection Laws.

3.3. Processors shall not unreasonably withhold, delay or condition their approval of any change to this Addendum requested by Controllers in order to ensure Controllers can comply with Data Protection Laws.

3.4. Processors are under no duty to investigate the completeness, accuracy, or sufficiency of any specific Controllers' instructions from an Authorized Person of Controller or the Personal Data other than as required under Data Protection Laws.

4. CONFIDENTIALITY

4.1. Processors shall:

a) keep and maintain all Personal Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure;

b) use and disclose Personal Data solely and exclusively for the Business Purposes, or to comply with the terms and conditions of the Agreement;

c) not use, sell, rent, share, transfer, distribute, or otherwise disclose or make available Controllers' Personal Data for Processors' own purposes or for the benefit of anyone other than Controllers, in each case, without Controllers' prior written consent;

d) use, transmit, store, and Process Personal Data only in the EEA, unless Section 7 of this Addendum is satisfied; and

e) not, directly or indirectly, disclose Personal Data to any person other than Authorized Persons, without prior written consent from Controllers, unless and to the extent expressly required by Data Protection Laws or as permitted by Section 5 of this Addendum.

4.2. In the event that Processors are legally required to disclose any portion of Controllers' Personal Data, Processors shall:

a) notify Controllers before such disclosure as soon as practicable after learning of such required disclosure;

b) furnish only that portion of Personal Data for which Processors' legal counsel reasonably believes Processors are legally required to produce and only in the manner legally required; and

c) exercise reasonable efforts to obtain assurance that confidential treatment will be accorded such Personal Data.

5. SUB-PROCESSORS

5.1. Controllers acknowledge that the provision of the services by Processors may require the use of Sub-Processors. Controllers hereby grant to Processors general authorization for sub-processing in order to support the performance of the services, including the use of data center operators, email service providers, providers of fraud detection/authenticity services and outsourced support providers, provided always that:

a) Processors shall keep Controllers informed of all Sub-Processors engaged in the provision of the services unless contractually prohibited from doing so. Upon request, for each Sub-Processor used, Processors shall provide: (i) the Sub-Processor's name, address, and contact information; (ii) the category of the Sub-Processor or type of services provided; and (iii) the categories of Personal Data disclosed to the Sub-Processor in the preceding 12 months.

b) Processors shall notify Controllers of any intended changes concerning the addition or replacement of Sub-Processors to the nominated contact, giving Controllers the opportunity to object to such changes on reasonable grounds based on non-compliance or a material risk of non-compliance by Controllers with Data Protection Laws or this Addendum.

c) Processors shall limit disclosure to Sub-Processor, to the extent practicable, to the minimum necessary to accomplish the intended purpose of such use, disclosure or request.

d) Obligations substantially no less protective of Personal Data in question than those set out in this Addendum shall be imposed on each Sub-Processor by way of a contract or other legally binding agreement, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of (i) this Addendum; and (ii) the Data Protection Laws. Where the Sub-Processor fails to fulfill the data protection obligations, Processors shall remain fully liable to Controllers for the performance of the Sub-Processor's obligations, subject to the terms of this Addendum.

e) Controllers may request that Processors audit a Sub-Processor or provide confirmation that such an audit has occurred to ensure compliance with its obligations imposed by Processors in conformity with this Addendum.

f) Processors are considered to control any Personal Data controlled by or in possession of its Sub-Processors.

g) The Processors enter into a written contract with the Sub-Processors that contain terms substantially the same as those set forth in this Addendum and provides Controller with copies of such contracts upon Controllers' written request. These written contracts shall automatically terminate on termination of this Addendum for any reason.

6. TECHNICAL/ORGANIZATIONAL MEASURES

6.1. In relation to the Processing of Personal Data, Processors shall implement and maintain, at their cost and expense, a suitable written information security program taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of Processing Personal Data, that is designed to:

a) ensure the security and confidentiality of Personal Data;

b) protect against any anticipated threats or hazards to the security or integrity of Personal Data;

c) protect against unauthorized disclosure, access to, or use of Personal Data;

d) ensure the proper disposal of Personal Data; and

e) ensure the compliance of all Authorized Persons of Processor and Authorized Persons of a Subprocessor.

6.2. Processors represent and warrant that their collection, access, use, storage, disposal and disclosure of Personal Data does and will comply with this Addendum and Data Protection Laws.

6.3. Technical and organizational measures are subject to technical advancements and future developments. Processors are, therefore, permitted to make use of adequate alternate measures in this respect. Such alternate measures may not, however, fall below the level of security stipulated in the Data Protection Laws for these measures. Substantive changes shall be properly documented and communicated to Controllers.

6.4. The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. Processors will therefore evaluate the measures as implemented in accordance with this Addendum on an on-going basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out herein.

6.5. Processors shall further provide Controllers (and their external auditors) with the results of any and all Processor Audits performed immediately prior to or during the term of the Agreement, including but not limited to AICPA Service Organization Controls (SOC) 2 Type II report and/or ISO 27001 certification.

7. INTERNATIONAL DATA TRANSFERS

7.1. Controllers acknowledge that the provision of the services under the Agreement may require the transfer or Processing of Personal Data in countries other than Controllers' country of domicile from time to time.

7.2. The provisions of this Addendum shall constitute Controllers' instructions with respect to international transfers for Processing in countries other than Controllers' country of domicile.

7.3. In the event of such international transfers, assuming there is no derogation that the Parties may rely on, the Parties shall complete all relevant details in and execute Standard Contractual Clauses or any other suitable data transfer mechanism recognized by a competent authority as an Appropriate Safeguard.

8. OBLIGATIONS OF CONTROLLERS

8.1. Controllers will ensure that all Personal Data disclosed or made available to Processors will have been collected or made available in accordance with Data Protection Laws, including with respect to any required information, transparency and consents, and that the collection, Processing and use of such Personal Data by Processors on behalf of Controllers in accordance with this Addendum will not result in any contravention of Data Protection Laws.

8.2. Controllers warrant and represent that: (a) all instructions given by them to Processors with respect to Personal Data shall at all times be in accordance with Data Protection Laws; (b) Controllers shall not unreasonably withhold, delay or condition their approval of any change to this Addendum requested by Processors in order to ensure the Processors (and each Sub-Processor) can comply with Data Protection Laws.

8.3. Controllers warrant that they have all necessary rights to provide the Personal Data to Processors for the Processing to be performed in relation to any contract or other agreement between the Parties. To the extent required by applicable Data Protection Law, Controllers are responsible for ensuring that any necessary Data Subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the Data Subject, Controllers are responsible for communicating the fact of such revocation to the Processors, and Processors remain responsible for implementing any Controller instructions with respect to the further Processing of that Personal Data.

9. REPORTING VIOLATIONS

9.1. Processors shall at all times have in place written procedures which enable them to promptly respond to Controllers about a Data Breach or security incident impacting the Controllers' Personal Data.

9.2. Processors shall in all cases notify Controllers, without undue delay (and in no event later than a period required under applicable Data Protection Laws) of any Data Breach or any breach of the specifications in this Addendum, and provide Controllers with details of any Data Breach. Processors shall at all times cooperate with Controllers, and shall follow Controllers' instructions with regard to any suspected or actual Data Breach, in order to enable Controllers to perform or assist in performing a thorough investigation into the Data Breach, to formulate a correct response, and to take suitable further steps with respect to the Data Breach.

9.3. Any notifications made to Controllers pursuant to this section shall contain:

a) a description of the nature of the incident, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

b) the name and contact details of the Processors' data protection officer or another contact point where more information can be obtained;

c) a description of the likely consequences of the incident; and

d) a description of the measures taken or proposed to be taken by Processors to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

9.4. It is recognized that, pursuant to Data Protection Laws, an obligation to provide information may exist in the event that Personal Data is lost or unlawfully accessed/disclosed. Therefore, Controllers should be notified of such incidents, regardless of the cause. This also applies to serious disruptions in operations or other irregularities in handling Controllers' Data. In cooperation with Controllers, Processors shall take appropriate steps to secure the data and mitigate possible negative effects on the affected parties.

10. DELETE, AMEND, TRANSFER DATA, PROOF OF DATA PROCESSING

10.1. Processors must promptly comply with any Controller request or instruction to provide, amend, transfer, or delete Personal Data, or to stop, mitigate, or remedy any unauthorized Processing. Should Controllers issue an instruction to Processors pursuant to this section, the Processors are hereby authorized and obligated to commence the amendment, transfer or permanent deletion without undue delay, unless Data Protection Laws require storage of the Personal Data.

10.2. Documentation which serves to provide proof that data Processing occurred properly and pursuant to contract shall be retained by Processors beyond the term of this Addendum in accordance with the appropriate retention schedules.

11. DATA SUBJECT REQUESTS, COMPLAINTS, AND THIRD PARTY RIGHTS

11.1. The Processors must notify the Controllers within thirty (30) days if it receives a request from a Data Subject to exercise any rights the individual may have regarding their Personal Data, such as access, correction, deletion, or to opt-out of or limit certain activities like sales, disclosures or other Processing actions.

11.2. The Processors must notify the Controllers immediately if they receive any other complaint, notice, or communication that directly or indirectly relates to the Personal Data or to either Part's compliance with the Data Protection Laws.

11.3. The Processor will give the Controller its full cooperation and assistance in responding to any complaint, notice, communication or Data Subject Request.

12. COOPERATION TO REMEDIATE

In the event that the transfer or Processing of Personal Data under this Addendum is no longer lawful or otherwise not permitted, the Parties agree to remediate the Processing in order to meet the necessary standards or requirements. If Processors are unable to remediate the Processing, then Controllers shall be entitled to terminate this Addendum without penalty.

13. NOTICES

All notices with respect to matters covered under this Addendum shall be sent to the nominated contacts herein:

To Cloud ID: Cloud ID, LLC
Attn: Legal Department
485 Sunset Blvd., Office #114
Hamburg, NY 14075
Email: legaldept@synacor.om

To Reseller: The name, address, and contact information as set forth in the Agreement.

14. GENERAL PROVISIONS

14.1. This Addendum is subject to the terms of the Agreement and is incorporated into and made a part of the Agreement.

14.2. Exhibit A and each Annex are hereby incorporated into and made a part of this Addendum. Any reference to this Addendum includes Exhibit A and each Annex.

14.3. This Addendum supersedes all previous communications, representations, understandings, and agreements, either oral, electronic, or written with respect to the subject matter of this Addendum.

14.4. Any amendment, change or other modification of this addendum requires the signed, written consent of both parties. The waiver of any provision of this Addendum requires the signed, written consent of the party providing such waiver, and such waiver only applies to the waiver and instance so consented to by such party.

14.5. If there is a conflict between the terms of this Addendum and the terms of the remaining part of the Agreement with respect the subject matter of this Addendum, then the terms of this Addendum prevail.

14.6. If there is a conflict between the terms of this Addendum and the terms of the Standard Contractual Clauses, then the terms of the Standard Contractual Clauses shall prevail.

[Remainder of this page intentionally left blank.]

EXHIBIT A

ANNEX I

A. LIST OF PARTIES

Data Exporter(s)	
Name, Address, Contact Person:	Set forth in the Agreement.
Activities relevant to the data transferred under these Clauses:	Processing of data for [describe activities].
Signature and date:	Signed and dated in the Agreement.
Role (controller/processor):	Controller
Data Importer(s)	
Name:	Cloud ID, LLC
Address:	485 Sunset Blvd., Office #114, Hamburg, NY 14075
Contact Person:	Name: Position: Contact Details:
Activities relevant to the data transferred under these Clauses:	[Describe activities].
Signature and date:	Signed and dated in the Agreement.
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred.	
Categories of personal data transferred.	
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	
Nature of the processing.	
Purpose(s) of the data transfer and further processing.	
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.	

For transfers to subprocessors, also specify subject matter, nature and duration of the processing.	*See chart below.*

Subprocessors:

Subprocessor(s)	***Address and contact person's name, position and contact details***	***Personal data processed***	***Nature of the processing***	***Duration of the processing***	***Location of processing***
Stripe	Name, email, phone, credit card, employee id number	Credit card payment	Electronic	One time	See this link: https://stripe.com/privacy.
AWS	Name, email, phone, employee id number	Storage	Electronic	For as long as data is stored.	U.S.
Sisense	Name, email, phone, employee id number	Data analytics	Electronic	For as long as data is stored.	U.S.
Suppliers	Name, email, phone, employee id number	Book corporate accommodations	Electronic and manual	For as long as data is processed and stored.	In Service Portal

C. COMPETENT SUPERVISORY AUTHORITY

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

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.	The Data Importer will comply with and implement the Information Security Obligations; physical, technical and organizational security measures, including those set forth in the Agreement, along with the schedules and exhibits to the Agreement.
For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.	The Data Importer will comply with and implement the Information Security Obligations; physical, technical and organizational security measures, including those set forth in the Agreement, along with the schedules and exhibits to the Agreement.

ANNEX III

LIST OF SUBPROCESSORS

The controller has authorized the use of the following sub-processors:	
Name:	See chart below.
Address:	See chart below.
Contact person's name, position, and contact details:	See chart below.
Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized):	See chart below.

Subprocessor(s)	***Address and contact person's name, position and contact details***	***Personal data processed***	***Nature of the processing***	***Duration of the processing***	***Location of processing***
Stripe	Name, email, phone, credit card, employee id number	Credit card payment	Electronic	One time	See this link: https://stripe.com/privacy.
AWS	Name, email, phone, employee id number	Storage	Electronic	For as long as data is stored.	U.S.
Sisense	Name, email, phone, employee id number	Data analytics	Electronic	For as long as data is stored.	U.S.
Suppliers	Name, email, phone, employee id number	Book corporate accommodations	Electronic and manual	For as long as data is processed and stored.	In Service Portal