



EXHIBIT B: DATA PROCESSING AGREEMENT

This Data Processing Agreement (“DPA”) forms part, and shall become an Addendum, to the Agreement between Selligent and Client. By signing this DPA, Client agrees and accepts the terms of this DPA, on behalf of itself, and to the extent required under applicable Data Protection Law and Regulations, in the name of and on behalf of its Authorized Affiliates. For the purpose of this DPA, the term “Client” shall include Client and Authorized Affiliates, unless the context indicates otherwise.

1. **PURPOSE.** Pursuant to the Agreement, Client shall provide Personal Data to Selligent. The parties agree to comply with the following provisions with respect to any Personal Data transferred to or processed or accessed by Processor pursuant to or in connection with the Agreement.

2. DEFINITIONS.

2.1 “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control”, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the concerned entity.

2.2 “**Authorized Affiliate**” means any Client’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to a Sales Order between Client and Selligent, but has not signed its own Sales Order with Selligent and is not a “Client” as defined under this DPA.

2.3 “**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

2.4 “**Client**” means the entity that is a party to the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Sales Orders.

2.5 “**Client Data**” means what is defined in the Agreement as “Client Data”.

2.6 “**Controller**” means (i) the entity which determines the purposes and means of the Processing of Personal Data and/or (ii) any “Business” as defined under the CCPA.

2.7 “**Data Protection Law and Regulation(s)**” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area (“EEA”) and their member states,

Switzerland and the United Kingdom, the United States and its states, including the CCPA, applicable to the Processing of Personal Data under the Agreement.

- 2.8** “**Data Subject**” means (i) the identified or identifiable person to whom Personal Data relates; and/or (ii) any “Consumer” or “Individual” as defined by any Data Protection Law and Regulation.
- 2.9** “**Data Subject Rights**” means those rights identified in Data Protection Law and Regulations that are granted to Data Subjects.
- 2.10** “**GDPR**” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- 2.11** “**Personal Data**” means (i) any Client Data that directly or indirectly identifies a natural person, or, with respect to those countries where relevant, a legal person; (ii) any “Personal Information” of a “Consumer” as those terms are defined under the CCPA; and (iii) any Personal Information of an individual as that term is defined under any data protection law and regulation.
- 2.12** “**Privacy Shield Framework**” means the EU-US and/or Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce.
- 2.13** “**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such a collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, deletion, or destruction. “Process”, “Processed” and “Processes” shall be interpreted accordingly.
- 2.14** “**Processor**” means (i) the entity that Processes Personal Data on behalf of the Controller and/or (ii) any “Service Provider” as defined in the CCPA.
- 2.15** “**Selligent**” means Selligent, Inc.¹, acting on behalf of itself, and to the extent required under applicable Data Protection Law and Regulations, in the name of the Selligent Affiliates. A list of the Selligent Affiliates is attached in [Schedule 1](#) of this DPA.
- 2.16** “**Standard Contractual Clauses**”, “**SCCs**”, or “**SCC**” means the European Commission standard contractual clauses for the transfer of Personal Data to a Processor established in a third country which

¹ A corporation incorporated under the laws of the State of Delaware, USA, with offices at 9 Lea Avenue, Nashville, Tennessee, 37210 (USA)

does not ensure an adequate level of data protection, as approved by Commission Decision 2010/87/EU (Controller to Processor transfers) as amended, replaced or repealed from time to time.

- 2.17** “**Sub-processor**” means any person appointed by or on behalf of Selligent to Process Personal Data on behalf of Client in connection with the Agreement.
- 2.18** “**Supervisory Authority**” means either (as applicable): (i) an independent public authority which is established by an European Union Member State pursuant to Article 51 of the GDPR; or (ii) the California Attorney General.
- 2.19** “**User**” means an individual expressly authorized by Client to use the Services and to whom Client has supplied a user identification and password. Users may include Client’s employees, agents (third-party service providers), independent contractors, or subcontractors.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

3. ROLES OF THE PARTIES.

- 3.1 Controller and Processor.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Client (including for the avoidance of doubt Authorized Affiliates, as the case may be) is the Controller and Selligent is the Processor with respect to Personal Data that Selligent Processes pursuant to the Agreement.
- 3.2 Authorized Affiliates.** Client enters into this DPA on its own behalf and, to the extent applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Selligent and each of such Authorized Affiliates subject to Section 9 of this DPA. For the avoidance of doubt, where an Authorized Affiliate becomes a party to this DPA, to the extent required under the Data Protection Law and Regulations, it is bound by its obligations as Controller. Unless otherwise prescribed by the Data Protection Law and Regulations, any right will be exercised by Client as party to the Agreement on behalf of an Authorized Affiliate and such rights exercised by Client as party to the Agreement shall be exercised in a combined manner for all of its Authorized Affiliates and not separately for each of them.

4. PROCESSING OF PERSONAL DATA.

- 4.1 Subject-matter of the Processing.** The subject-matter of the Processing is the performance of the Services pursuant to the Agreement. The content of the Processing, the types of Personal Data Processed and the categories of Data Subjects concerned by the Processing are further detailed in Schedule 2 of this DPA. The parties agree that the Processing of Personal Data by Processor is a valid business purpose for the duration of the Agreement, unless otherwise agreed in writing or provided in Section 4.2.
- 4.2 Provision of Personal Data by the Controller.** It is up to Client’s sole discretion to monitor what Personal Data is transferred to and uploaded on the Selligent Platform and to assess whether the technical and organizational measures implemented by Selligent provide the appropriate level of protection of its Personal Data on the Platform. Client shall comply with the requirements of Data Protection Law and Regulations in its use of the Services, Processing of Personal Data and in any instruction for the Processing of Personal Data. Client instructs Selligent (and authorizes Selligent to instruct each sub-processor) to: (i) Process Personal Data, including but not limited to by disclosing such data to sub-processors and other third parties; (ii) transfer Personal Data to any country or territory subject to Section 7; and (iii) engage any sub-processors subject to Section 6. Client is and will at all relevant times remain duly and effectively authorized to give the instruction in this sentence.

Client is solely responsible:

- a) for the accuracy, quality, integrity, legality, reliability and appropriateness, and, in general, the content of Personal Data transferred to and stored in the Platform, or generated and used by the Services;
- b) for the use of a secured communication protocol when submitting the Personal Data on the Selligent Platform (such as FTPS, SFTP or HTTPS); and
- c) the means by which Client acquired Personal Data, and any applicable requirement to provide notice to Data Subjects of the use of Selligent as Processor.

4.3 Processing of Personal Data by Selligent.

4.3.1 Clients Instructions. Selligent shall Process Personal Data only on behalf of and according to documented instructions of Client for the following purposes:

- a) Processing in accordance with the Agreement and any specific Sales Order or Statement of Work;
- b) Processing determined by the Users upon their use of the Services; and
- c) Processing upon other documented instructions provided by Client (e.g. via email) in line with the Agreement and consistent with the Services.

4.3.2 Selligent's use of Personal Data. Selligent shall not use the Personal Data for its own purposes or for the purposes of any third-party, and shall Process Personal Data in accordance with Data Protection Laws and Regulations, this DPA and the Agreement. Selligent shall not take any unilateral decisions about the use of the Personal Data or the length of time the Personal Data will be stored, except pursuant to statutory provisions or court or regulatory body decision that prescribe otherwise.

4.3.3 Processor's employees. Subject to Section 6 below, Selligent's employees who may have access to the Personal Data are limited to those employees performing Services in accordance with the Agreement, except prescribed otherwise by Data Protection Law and Regulations. The group of employees performing Services in accordance with the Agreement are listed in Schedule 2 of this DPA.

5. SECURITY OF PERSONAL DATA.

5.1 Security Measures. The Processor shall maintain appropriate technical and organizational measures designed to secure Personal Data (including to protect Personal Data against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Data). Subject to Section 5.2 below, details of such technical and organizational measures are available upon Client's written request, and are only provided for the purpose of demonstrating compliance with the Data Protection Law and Regulations. These measures are designed to provide a suitable and reasonable level of security, taking into account the state of the art, the costs of implementation, as well as the risks inherent in data Processing proposed by the Processor and the nature of the Personal Data.

5.2 Certifications and Audits. As of the date of execution of this DPA, Selligent has obtained the third-party certifications as described in Schedule 3 of this DPA. Upon Client's written request, not more than once per calendar year (unless requested by a Regulatory Authority), and subject to reasonable notice, Selligent will enable the Controller to supervise its compliance with provisions of Section 5.1 above by instituting an audit, subject to any confidentiality obligations owing to Selligent and any third-parties. Selligent will provide the necessary information and documentation and its reasonable cooperation with Client. The audit will be carried out in line with the requirements set out in the Selligent Support and Service Level Schedule. The costs of any such audit will be borne by Client, unless the audit reveals that the provisions of Section 5.1 have not been complied with in a material way, in which case the Processor

will bear the costs of the audit directly related to any noted material errors. In such case, the Processor will promptly develop a corrective action plan. It is agreed that Client will mitigate the burden of the audit for Selligent by combining, to the extent possible, several audit requests carried out on behalf of different Authorized Affiliates into one single audit.

5.3 Management and Notification of Personal Data Incidents. Selligent shall notify Client without undue delay after becoming aware of the accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Data, including Personal Data Processed by Selligent or its sub-processor(s) of which Selligent becomes aware (hereafter a “Personal Data Incident”). Selligent’s notification of or response to a Personal Data Incident under this Section 5.3 will not be construed as an acknowledgement by Selligent of any fault or liability with respect to the Personal Data Incident. Selligent will make reasonable efforts to identify the nature, scope and circumstances of such Personal Data Incident and take those measures as Selligent deems necessary and reasonable to be taken, to the extent within Selligent’s reasonable control and provide Client with sufficient information to allow Client to meet its obligations under Data Protection Laws and Regulations to report or inform Data Subjects and/or Supervisory Authorities of the Personal Data Incident. At Client’s written request, Selligent will reasonably cooperate with Client to enable Client to comply with the notification obligation, according to Section 11 of this DPA.

5.4 Confidentiality of Personal Data.

5.4.1 Confidentiality within the organization of the Processor. Processor shall ensure that Selligent’s employees having access to Personal Data are bound by contractual confidentiality obligations and are informed about the confidential nature of the Personal Data and the responsibilities arising from the Processing of Personal Data.

5.4.2 Confidentiality outside the organization of the Processor. Unless it has obtained Client’s prior written consent, Selligent is prohibited from granting any third-party access to the Personal Data, except and to the extent that it is necessary for the performance of the Services and in accordance with Section 6 below.

If Selligent receives a request or an order from a regulatory authority, a government agency, or a court (including but not limited to investigative, penal, or security institutions) to inspect or be provided with Personal Data belonging to the Controller (each an “Order”), then Selligent will, to the extent legally permitted, inform Client without undue delay of such Order. In dealing with the Order, Selligent will observe Client’s instructions (including an instruction to leave all or part of dealings with the Order to Client) and will provide all reasonably necessary cooperation. Should the Order prohibit Selligent from meeting its obligations pursuant to this Section, Selligent will promote the reasonable interests of Client and, in particular, will scrutinize any such Order to determine whether the Order is valid, legally binding and lawful and take all reasonable steps to reject or contest any Order that is not valid, legally binding and lawful.

6. SUB-PROCESSORS.

6.1 Client agrees that Selligent’s Affiliates are specifically authorized by Client to be retained as sub-processors and that Selligent and Selligent’s Affiliates may retain respectively third-party sub-processors in connection with the performance of the Services. Selligent Affiliates and country of location are listed in Schedule 1 of this DPA. Sub-processors whose services Selligent wishes to engage for Processing Personal Data will be selected with due care and diligence appropriate to the type and volume of Personal Data being processed.

6.2 Selligent or Selligent’s Affiliates will have in place a written agreement with any sub-processor it uses containing data protection obligations not less protective than those in this DPA with respect to the

protection of Personal Data to the extent applicable to the nature of the Services provided by such sub-processor. The agreement with sub-processor will provide that sub-processor agrees to only Process Personal Data (i) in a country that the European Commission has declared to have an “adequate” level of protection; (ii) on terms equivalent to the Standard Contractual Clauses, (iii) pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities, or (iv) pursuant to a compliant US-EU and/or US-Swiss Privacy Shield certification.

- 6.3** Selligent will notify Client in writing of its decision to engage or replace a sub-processor in due time, in order to give the Controller the opportunity to comment to such addition or change, and, as the case may be, to object in accordance with Article 28 of the GDPR. Client may object to a new sub-processor on a bona-fide and reasonable basis, by notifying Selligent in writing, not later than five (5) business days after receipt of Selligent’s notice, and in such event, the parties will meet to discuss the objections and agree on a reasonable solution acceptable to each of them. If no solution is found within ten (10) calendar days of Client’s objection, and subject to the new sub-processor not presenting the same level of technical and organizational measures as those previously in place, Client shall be entitled to terminate any such Sales Order or Statement of Work with respect to such Services that cannot be provided by Selligent without the use of the objected new sub-processor, and upon such termination, to a refund of any prepaid fees covering the remainder of the term for such specific Services, without any additional compensation being owed by any party. If Client does not terminate a Sales Order or Statement of Work because of the use of the objected new sub-processor, that sub-processor will be deemed to have been authorized by Client.
- 6.4** The sub-processors with country of location engaged by the Processor upon execution of this DPA are listed in Schedule 4 of this DPA.
- 6.5** Selligent will remain liable for the acts and omissions of its sub-processors to the same extent it would be liable under this DPA if performing itself the services of a sub-processor.

7. ONWARD TRANSFER OF PERSONAL DATA.

- 7.1 Hosting of Client Data.** Selligent Platform is located within the United States of America (USA).
- 7.2 Mechanisms for Transfer of Personal Data.** As of the execution of this DPA, Selligent, Inc. is certified under the EU-US and Swiss-US Privacy-Shield Frameworks and Client warrants that it is authorized to transfer the Personal Data to Selligent acting as Processor outside of the EU, and that such transfer of Personal Data is taking place only for the limited and specified purposes of providing the Services under the Agreement. Client warrants that it has undertaken all necessary steps to ascertain that Selligent’s technical and organizational measures are reasonable and appropriate steps designed to ensure the effective processing of Personal Data in a manner consistent with Data Protection Laws and Regulations. By entering into this DPA, in each case where such transfer as referred to above would be prohibited by Data Protection Law and Regulations in the absence of the Standard Contractual Clauses established pursuant to the EU Commission Decision 2010/87/EU of 5 February 2010, Client hereby grants Selligent power of attorney to enter, in the name of and on behalf of Client, into these Standard Contractual Clauses, deemed incorporated herewith by reference.

In the event that the Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of

precedence: (a) the Standard Contractual Clauses as set out in this section; and (b) Swiss-US Privacy Shield Framework self-certifications.

The Controller agrees that for Support Services purposes, support may be provided, when necessary, by a Selligent Affiliate within the United Kingdom or EEA.

In case any permitted use of the Services by a Client to an Authorized Affiliate results in a transfer of Personal Data outside the European Union, the EEA, and their member states, Switzerland and the United Kingdom, Client and such Affiliate shall comply with all Data Protection Law and Regulations applicable to transfers of Personal Data outside the European Union, the EEA, and their member states, Switzerland and the United Kingdom.

- 8. DATA SUBJECT'S RIGHTS.** Client is responsible for responding to a data subject's exercise of their Data Subject Rights (each a "Data Subject Request") using its own access to the relevant Personal Data. To the extent Client, in its use of the Services, cannot itself access such relevant Personal Data, Selligent shall, upon Client's request, use commercially reasonable efforts to assist Client in accessing such relevant Personal Data, to the extent Selligent is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations.

Selligent will, to the extent legally permitted, promptly notify Client if Selligent receives a Data Subject Request directly from a Data Subject. Selligent will not respond to such request except on the documented instructions of Client or as required by applicable law.

- 9. LIABILITY FOR BREACHES UNDER THIS DPA.** EACH PARTY'S AND ALL OF ITS AFFILIATES' LIABILITY, TAKEN TOGETHER IN THE AGGREGATE, ARISING OUT OF OR IN CONNECTION WITH THIS DPA, AND ALL DPAS BETWEEN AUTHORIZED AFFILIATES AND SELLIGENT, WHETHER IN CONTRACT OR TORT, SHALL BE SUBJECT TO THE LIABILITY LIMITATIONS SET FORTH IN THE AGREEMENT AND ANY REFERENCE TO A PARTY'S LIABILITY IN THE AGREEMENT SHALL BE DEEMED TO BE A REFERENCE TO THE AGGREGATE LIABILITY OF SUCH PARTY AND ALL OF ITS AFFILIATES.

10. TERM AND TERMINATION OF THIS DPA.

- 10.1** This DPA will become effective upon its signing by both parties (the "DPA Effective Date"). Unless earlier terminated, this DPA will terminate upon the termination of the Agreement.

- 10.2** In the event that changes in law or regulation render performance of this DPA impossible or commercially unreasonable, or if any modification to this DPA is required to comply with a material change in any Data Protection Law and Regulations, Selligent will provide Client with an addendum to this DPA to address such impossibility, commercial unreasonableness or material change. If Client does not agree to such addendum in the time required, either party may by notice to the other, terminate the Agreement and this DPA on notice, without liability to either party.

- 10.3** At the request of Client or upon the termination of the DPA (regardless of the reasons for such termination), Selligent will ensure that, at Client's option:

a) the Personal Data is made available to Client or to a subsequent service provider in accordance with the Agreement entered into by the parties. Such request must be notified by Client in writing at the latest by the effective date of termination or expiration of the Agreement. Processor will return to Client its data through FTPS or SFTP within fifteen (15) calendar days of such request. All complaints relating to the return of the data must be notified to Selligent in writing within ten (10) calendar days of the return. The format in which such data will be returned will be Selligent format or any other format that can be read on industry standard software; or

b) destroy all of the Personal Data that has been provided to it, as well as all Personal Data it has Processed, to the extent allowed by applicable law and in accordance with the recognized standards for data destruction, and provide the Controller with written confirmation of such destruction.

10.4 After the termination of the DPA, Selligent will not retain any copies of the Personal Data, except for that relating to any agreed technical back-up procedures or to the extent legally required.

11. INFORMATION AND ASSISTANCE. Selligent will reasonably provide Client with the information and assistance necessary to allow Client (as Controller) to:

- a) make notification of Personal Data Incidents to Supervisory Authorities and any other data protection governmental authorities with respect to Personal Data processed as a consequence of the Services;
- b) take the appropriate technical and organizational measures to ensure the security and safety of Personal Data;
- c) undertake data protection impact assessments or seek prior consultation with the data protection authorities; and
- d) observe rights of data subjects according to section 8 of this DPA.

Selligent reserves the right to charge a reasonable administrative fee which shall be proportional to the effort required to provide Client with this information and assistance. Any such fee shall be communicated beforehand and shall not be set at a level which results in the fee working prohibitively with regard to Selligent's obligation to comply with the commitments in the first paragraph of this Section.

12. MISCELLANEOUS.

12.1 This DPA supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this DPA, including any prior data processing addenda entered into between Selligent and Client. Except as specifically set forth in this DPA, all terms of the Agreement remain in full force and effect. In the event of any conflict or inconsistency between the content of this DPA and the Agreement, this DPA shall prevail.

12.2 None of the provisions of this DPA should prevent any party to be compliant with any applicable law or regulation. In the event of any conflict, the relevant provision of this DPA shall not be applied.

IN WITNESS WHEREOF, each of the Parties hereto, intending to be legally bound, has caused the Agreement to be executed by its duly authorized representative as of the date indicated below.

FOR SELLIGENT, INC.:

FOR _____:

By: _____

By: _____

Name: Karthik Kripapuri

Name: _____

Title: CEO

Title: _____

Date: _____

Date: _____

Schedule 1 – Selligent Affiliates

Selligent Benelux NV
Kempische Steenweg 305 box 401
3500 Hasselt (Belgium)
Belgian Crossroad Bank 0478.839.312
Selligent International SA
Avenue de Finlande 2 box 2
1420 Braine L'Alleud (Belgium)
Belgian Crossroad Bank 0652.992.518
Selligent France SA
20 Place des Vins de France RCS
75012 Paris (France)
RCS Paris B 391 206 554
Selligent GmbH
Herzogspitalstraße 24
80331 München (Deutschland)
HRB 197488
Selligent Iberica S.L.U
Calle Enrique Granados 86-88
Planta 3 °
08008 Barcelona (España)
CIF B-66-577.669
Selligent Ltd
Second Floor, 45 Folgate Street
London E1 6BX (United Kingdom)
Company Number: 06398867
Selligent Italy
Via Copernico 38
20125 Milano (Italia)
Register number 02763630346
Selligent Inc
9 Lea Avenue
Nashville, Tennessee, 37210 (USA)

Schedule 2 – Details of Processing

The Controller shall decide, in its sole discretion, what Personal Data is transferred to and stored on the Selligent Platform. While the Controller is responsible for deciding what data to submit, it typically may concern:

- The following categories of Data Subjects:
 - a) Prospects, Clients, Business Partners; and
 - b) Clients' users; and

Note: Information regarding children below the age of 16 and/or 13 years old, depending on applicable domestic privacy legislation, shall not be processed by the Controller on the Platform.

-
- The following types of Personal Data:
 - a) Contact information including first name, last name, e-mail address;
 - b) Information that a Client or Prospect has entered in a form;
 - c) Other information relevant to customer surveys and/or offers;
 - d) Behavioral and navigation data, such as which sites of the controller or mails viewed, in what order and at which time; and
 - e) Analytical and profiling data.

As part of the Services under the Agreement, Selligent will provide Client with access to and usage of the Selligent Platform for the purpose of executing omnichannel campaign to engage both anonymous and identified consumers via e-mail, mobile, social, website optimization, call center, SMS, direct mail, in-store and other channels.

The nature of the processing includes uploading, creating and updating personal data, executing omnichannel campaigns to engage with data subjects through different channels, optimizing campaigns & customer experience and analytics.

The Processor merely provides services, usage concepts, data storage space and interfaces. The definition of the Services is described in the Agreement entered into between the Processor and the Controller.

Selligent's employees may have access to Personal Data to the extent necessary to perform the Services under the Agreement. This concerns typically SaaS Operations and DevOps teams, Support Services team, dedicated employees in charge of Client relationship who may consult the use of the Platform by the Client for the purposes of providing advices.

Client DPO Information:

Name: _____

Email Address: _____

Phone Number: _____

Schedule 3 – Selligent, Inc. Certifications

- a) ISO 27001
- b) ISO 27018
- c) EU-US and Swiss-US Privacy-Shield Framework Certifications

Schedule 4 – List of sub-processors that may have access Personal Data

- Datacenter(s)
- Cloud service provider(s)
- Support provider(s)
- Content delivery network provider(s)
- IT infrastructure Provider(s)
- Operating System Provider(s)
- Application or Software Provider(s)

The details of sub-processing activities and the identity and country of location of each sub-processor is available in the Privacy section of the online help page on Selligent Platform .