acsense

Data Processing Addendum

This Data Processing Addendum (“**Addendum**”) forms an integral part of the Agreement between Customer and Empyrean Technologies Ltd. DBA Acsense ("**Company**") and applies to the extent that Company processes Personal Data, or has access to Personal Data, in the course of its performance under the Agreement.

Customer shall qualify as the Data Controller and Company shall qualify as the Data Processor, as this term is defined under Data Protection Law. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions

1.1. "**Agreement**" means the agreement as well as any order form or other purchasing document between customer and the Company which involves Company having access to or otherwise processing personal data of customer ("**Customer**");

1.2. "**Approved Jurisdiction**" means a member state of the EEA, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission.

1.3. "**CCPA**" means the California Consumer Privacy Act Cal. Civ. Code § 1798.100 et seq.

1.4. “**Data Controller**”, “**Data Processor**”, "**Personal Data Breach**" “**data subject**”, “**process**”, “**processing**” and "**sell**" shall have the meanings ascribed to them in the Data Protection Law. Where applicable, Data Controller shall be deemed to be a "Business", Data Processor shall be deemed to be a "Service Provider", and "data subject" shall be deemed to be a "Consumer" as these terms are defined under the CCPA.

1.5. **"EEA**" means those countries that are member of the European Economic Area.

1.6. **“Data Protection Law”** means any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security and/or the protection of personal data, including Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including the 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 (General Data Protection Regulation) ("**GDPR**") and the CCPA.

1.7. "**Personal Data**" means any information which (i) can be related to an identifiable individual, including any information that can be linked to an individual or used to directly or indirectly identify an individual, **and** (ii) supplied by Customer to Company pursuant to the Agreement or which Company generates, collects, stores, transmits, or otherwise processes on behalf of Customer in connection with the Agreement. Personal Data may include information which is related to Customer's end users, employees, contractors, suppliers and other third parties.

1.8. “**Security Measures**” mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Company's business, the level of sensitivity of the data collected, handled and stored, and the nature of Company's business activities.

1.9. **"Standard Contractual Clauses"** mean the standard contractual clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission Decision EC/2021/915: Commission Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

1.10. “**Sub-Processors**” mean any affiliate, agent or assign of Company that may process Personal Data pursuant to the terms of the Agreement, and any unaffiliated processor engaged by Company.

2. Compliance with Laws

2.1. Each Party shall comply with its respective obligations under the Data Protection Law.

2.2. Company shall provide reasonable cooperation and assistance to Customer in relation to Company's processing of Personal Data in order to allow Customer to comply with its obligations as a Data Controller under Data Protection Law.

2.3. Company agrees to notify Customer promptly if it becomes unable to comply with the terms of this

Addendum and take reasonable and appropriate measures to remedy such non-compliance.

2.4. Throughout the duration of the Addendum, Customer agrees and warrants that: (i) the processing of Personal Data by Customer, as well as any instruction to Company in connection with the processing of Personal Data, has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law; and (ii) Personal Data has been collected and transferred fairly and lawfully, pursuant to any applicable Data Protection Law, and that the concerned data subjects have been informed of the processing and transfer of Personal Data pursuant to this Addendum.

3. <u>Obligations under the CCPA</u>

3.1. Company shall not sell the Personal Data.

3.2. Company is prohibited from retaining, using or disclosing Personal Data for a commercial purpose other than providing the services to the Customer under the Agreement and from retaining, using or disclosing the Personal Data outside of the Agreement.

3.3. Company understands its obligations under this section and will comply with them.

4. <u>Processing Purpose and Instructions</u>

4.1. The subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, shall be as set out in the Agreement.

4.2. The duration of the processing under the Agreement is determined by the Parties, as set forth in the Agreement.

4.3. Company shall process Personal Data only to deliver the Services in accordance with Customer's written instructions, the Agreement and the Data Protection Law, unless Company is otherwise required by law to which Company is subject (and in such a case, Company shall inform Customer of that legal requirement before processing, unless that law prohibits such information disclosure on grounds of public interest).

4.4. Processing any Personal Data outside the scope of the Agreement will require prior written agreement between Company and Customer by way of written amendment to the Agreement and will include any additional fees that may be payable by Customer to Company for carrying out such instructions.

5. Reasonable Security and Safeguards

5.1. Company shall implement and maintain commercially reasonable and appropriate physical, technical and organizational security measures to provide a level of security appropriate to the risk represented by the processing and nature of such personal data and protect personal data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed; all other unlawful forms of processing; including (as appropriate): (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

5.2. To the extent that Company processes Special Categories of Data, the security measures referred to in this Data Protection Addendum shall also include, at a minimum (i) routine risk assessments of Company's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while "at rest" and during transmission (whether sent by e-mail, fax, or otherwise), and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone).

6. Personal Data Breach. Upon becoming aware of a Personal Data Breach, Company will notify Customer without undue delay and will provide information relating to the Personal Data Breach as reasonably requested by Customer. Company will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Personal Data Breach.

7. Security Assessments and Audits

7.1. Company shall, upon reasonable and written notice and subject to obligations of confidentiality, allow its data processing procedures and documentation to be inspected no more than once a year by Customer (or its designee) subject to a 30 days prior written notice in order to ascertain compliance with this Addendum. Company shall cooperate in good faith with audit requests by providing access to relevant knowledgeable personnel and documentation.

7.2. At Customer's written request, and subject to obligations of confidentiality, Company may satisfy the requirements set out in this section by providing Customer with a copy of a written report so that Customer can reasonably verify Company's compliance with its obligations under this Addendum.

8. Cooperation and Assistance

8.1. If Company receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement, including requests from individuals seeking to exercise their rights under Data Protection Law, Company will promptly redirect the request to Customer. Company will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Company is required to respond to such a request, Company will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so.

8.2. If Company receives a legally binding request for the disclosure of Personal Data which is subject to this Addendum, Company shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. Notwithstanding the foregoing, Company will cooperate with Customer with respect to any action taken pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data.

8.3. Upon reasonable notice, Company shall provide reasonable assistance to Customer in:

i. allowing data subjects to exercise their rights under the Data Protection Law;

ii. ensuring compliance with any notification obligations of Personal Data Breaches to the supervisory authority and communication obligations to data subjects, as required under Data Protection Law;

iii. Ensuring compliance with its obligation to carry out Data Protection Impact Assessments ("**DPIA**") or prior consultations with data protection authorities with respect to the processing of Personal Data. Any assistance to Customer with regard to DPIA or prior consultations will be solely at Customer's expense.

9. Use of Sub-Processors

9.1. Customer provides a general authorization to Company to appoint (and permit each Sub-Processor appointed in accordance with this section to appoint) Processors and/or Sub Processors in accordance with this section.

9.2. Company may continue to use those Processors and/or Sub Processors already engaged by Company as at the date of this Agreement, subject to Company in each case as soon as practicable meeting the obligations set out in this section. A list of the Company's current Sub Processors is attached as **Schedule 1**.

9.3. Company can at any time and without justification appoint a new Processor and/or Sub-Processor provided that Company provides seven (7) days' prior notice and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Processor and/or Sub-Processor's non-compliance with Data Protection Law. If, in Company's reasonable opinion, such objections are legitimate, Company shall either refrain from using such Processor and/or Sub-Processor in the context of the processing of Personal Data or shall notify Customer of its intention to continue to use the Processor and/or Sub-Processor. Where Company notifies Customer of its intention to continue to use the Processor and/or Sub-Processor in these circumstances, Customer may, by providing written notice to Company, terminate the Agreement immediately.

9.4. With respect to each Processor and/or Sub Processor, Company shall ensure that the arrangement between Company and the Processor and/or Sub Processor is governed by a written contract including terms which offer at least the same level of protection as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR.

9.5. Company will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Company to breach any of its obligations under this Addendum.

10. International Data Transfers. If Company is required to transfer personal data to a third country or an international organization under applicable laws, it shall inform Customer of that legal requirement before processing; If, subject to Customer's prior consent, Company processes personal data from the EEA in a jurisdiction that is not an Approved Jurisdiction, Company shall ensure that it has a legally approved mechanism in place to allow for the international data transfer ("EEA Transfer"), the terms set forth in Part 1 of Schedule 2 (EEA Cross Border Transfers) shall apply. If Company transfer's Personal Data from the UK

to other countries that is not an Approved Jurisdiction, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Company for the lawful transfer of personal data (as defined in the UK GDPR) outside the EEA or UK ("UK Transfer"), the terms set forth in Part 2 of Schedule 2 (UK Cross Border Transfers) shall apply; the terms set forth in Part 3 of Schedule 2 (Additional Safeguards) shall apply to an EEA Transfer and a UK Transfer. If Company intends to rely on Standard Contractual Clauses, the following additional terms will apply to Company: (i) if the Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the new or modified Standard Contractual Clauses shall be deemed to be incorporated into this DPA, will replace the then-current Standard Contractual Clauses, and parties will promptly begin complying with such Standard Contractual Clauses. Company will abide by the obligations set forth under the Standard Contractual Clauses for data importer and/or sub-processor as the case may be; (ii) If Company subcontracts any processing of personal data, Company will ensure that it has a legally approved mechanism in place to allow for the international data transfer, where relevant.

11. Data Retention and Destruction. Company will only retain Personal Data for the duration of the Agreement or as required from its obligations under the Agreement. Following expiration or termination of the Agreement, Company will delete or return to Customer all Personal Data in its possession as provided in the Agreement except to the extent Company is required under applicable law to retain the Personal Data (in which case Company will implement reasonable measures to prevent the Personal Data from any further processing). The terms of this Addendum will continue to apply to such Personal Data.

12. General

12.1. Any claims brought under this Addendum will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement.

12.2. In the event of a conflict between the Agreement (or any document referred to therein) and this Addendum, the provisions of this Addendum shall prevail.

12.3. Company may change this Addendum if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the Company as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's rights to use or otherwise process Personal

Data; or (iii) have a material adverse impact on Customer, as reasonably determined by Company.

12.4. If Company intends to change this Addendum under this section, and such change will have a material adverse impact on Customer, as reasonably determined by Company, then Company will use commercially reasonable efforts to inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

Company ______________________ [ ]

By: ______________________ By: ______________________

Title: ______________________ Title: ______________________

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Services to Customer;
2. Performing the Agreement, this DPA and/or other contracts executed by the Parties;
3. Acting upon Customer’s instructions, where such instructions are consistent with the terms of the Agreement;
4. Sharing Personal Data with third parties in accordance with Customer’s instructions and/or pursuant to Customer’s use of the Services (e.g., integrations between the Services and any services provided by third parties, as configured by or on behalf of Customer to facilitate the sharing of Personal Data between the Services and such third party services);
5. Complying with applicable laws and regulations;
6. All tasks related with any of the above.

Duration of Processing

Subject to any section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Company will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion where such data typically includes: The name, contact and employment information of Customer’s personnel.

Categories of Data Subjects

Customer may submit Personal Data to the Services which mostly includes, but is not limited to, Personal Data relating to the following categories of Data Subjects: Employees, agents, advisors, freelancers of Customer (who are natural persons).

List of Sub-Processors

Sub-processor Entity	**Brief Definition of processing**	**Location of the Data Center**
Amazon Web Services Inc.	Hosting and security analytics	EU Germany(Frankfort)
Okta	Service cloud - for Identity and access management	Cell (US)
Hubspot	Service cloud - Customer requirement and support ticketing process	HubSpot's product infrastructure is hosted on Amazon Web Services (AWS) in the United States East region
AppNiv technologies SRL	Customer Support Team	No data centers, AppNiv may access accSenSe utilizes for AWS while providing support, the team is located in Romania

SCHEDULE 2 – CROSS BORDER TRANSFERS

PART 1 – EEA Transfers

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to an EEA Transfer.

2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and Service Provider is the data processor of the Personal Data.

3. Module Three (Processor to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data processor of the Personal Data and Service Provider is a Sub-processor of the Personal Data.

4. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.

5. Option 2: GENERAL WRITTEN AUTHORISATION in ההבהClause 9 of the Standard Contractual Clauses shall apply, and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 4 of the DPA.

6. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.

7. In Clause 17 of the Standard Contractual Clauses, Option 1 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland.

8. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of the Republic of Ireland.

9. Annex I.A of the Standard Contractual Clauses shall be completed as follows:

   Data Exporter: Customer.

Contact details: As detailed in the Agreement.

Data Exporter Role:

Module Two: The Data Exporter is a data controller.

Module Three: The Data Exporter is a data processor.

Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data Importer: Service Provider.

Contact details: As detailed in the Agreement.

Data Importer Role:

Module Two: The Data Importer is a data processor.

Module Three: The Data Importer is a sub-processor.

Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

10. Annex I.B of the Standard Contractual Clauses shall be completed as follows:

The categories of data subjects are described in Schedule 1 (Details of Processing) of this DPA.
The categories of personal data are described in Schedule 1 (Details of Processing) of this DPA.

The Parties do not intend for Sensitive Data to be transferred.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing is described in Schedule 1 (Details of Processing) of this DPA.

The purpose of the processing is described in Schedule 1 (Details of Processing) of this DPA.

The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.

In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth at the link detailed in Section 4 of the DPA.

11. Annex I.C of the Standard Contractual Clauses shall be completed as follows:

    The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 7 above.

12. The Security Documentation referred to in the DPA serves as Annex II of the Standard Contractual Clauses.

13. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.

PART 2 – UK Transfers

1. This Part 2 is effective from the same date as the Standard Contractual Clauses.

Background:

2. This Part 2 is intended to provide appropriate safeguards for the purposes of transfers of Personal Data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation:

3. Where this Part 2 uses terms that are defined in the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland

4. This Part 2 shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

5. This Part 2 shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this DPA has been entered into.

7. In the event of a conflict or inconsistency between this Part 2 and the provisions of the Standard Contractual Clauses or other related agreements between the Parties, existing at the time the DPA is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

8. This Part 2 incorporates the Standard Contractual Clauses which are deemed to be amended to the extent necessary so they operate:

   a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and
   b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 8 above, include (without limitation):

   a. References to the "Clauses" means this Part 2 as it incorporates the Standard Contractual Clauses

   b. Clause 6 Description of the transfer(s) is replaced with:

      "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."
      c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
      d. References to Regulation (EU) 2018/1725 are removed.

e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"
f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;
g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".
h. Clause 18 is replaced to state:
"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."
i. The footnotes to the Clauses do not form part of this Part 2.

10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.

11. The Parties may amend this Part 2 provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Standard Contractual Clauses and making changes to them in accordance with Section 8 above.

12. The Parties may give force to this Part 2 (incorporating the Standard Contractual Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Contractual Clauses.

<u>PART 3 – Additional Safeguards</u>

1. In the event of an EEA Transfer or a UK Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:

    a. The Processor shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from the Controller to the Processor and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.

b. The Processor will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under GDPR or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Court ("**FISA**");

c. If the Processor becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:

   I. The Processor shall inform the relevant government authority that the Processor is a processor of the Personal Data and that the Controller has not authorized the Processor to disclose the Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Personal Data should therefore be notified to or served upon the Controller in writing;

   II. The Processor will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the Processor’s control. Notwithstanding the above, (a) the Controller acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Personal Data, the Processor has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (e)(II) shall not apply. In such event, the Processor shall notify the Controller, as soon as possible, following the access by the government authority, and provide the Controller with relevant details of the same, unless and to the extent legally prohibited to do so.

2. Once in every 12-month period, the Processor will inform the Controller, at the Controller’s written request, of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.