DATA PROCESSING AGREEMENT

IMPULSE B2B SOLUTIONS

1. **Parties**

1.1 This agreement on the collection, storage and use of documents and information (hereinafter the "Sub Data Processing Agreement") has been signed by and between

IMPULSE B2B SOLUTIONS.
Company reg. no.
Address…..
Address…..
City and Country Name
(hereinafter referred to as the" Data Processor")

And co-signed

[Customer name]
CVR.no. [No]
[Address]
[Address]
(Herein after referred to as "Sub Data Processor")

(hereinafter jointly referred to as the "Parties" and individually as "Party")

2. **Definitions**

2.1 **"Affiliate"** means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a Party, where **"Control"** means the direct or indirect control of greater than 50% of the voting rights or equity interests of a Party or the power to direct or cause the direction of the management and/or business strategy of that Party.

2.2 "Applicable Data Protection Law" means any and all applicable data protection and privacy laws including, where applicable, Regulation (EU) 2016/679

regarding the Personal Data Protection ("GDPR"), any other applicable law which governs the agreements between the Parties in the field of data protection.

2.3 **"Data Subject"** shall mean the identified or identifiable natural person to whom Personal Data refers.

2.4 **"Cloud Services"** means, as applicable, the software, products or services provided by the Processor to the Controller in a hosted environment managed by the Processor, pursuant to the Main Agreement, pursuant to which there is a transfer of Personal Data from the Controller to the Processor through electronic or physical means of communication.

2.5 **"Company"** is the Controller signing this DPA and means either (i) a customer of PWF under a validly concluded license agreement, or (ii) a partner of PWF under a validly concluded partner agreement.

2.6 **"Incident"** means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Company Personal Data transmitted, stored, or otherwise processed by the Processor for the purpose of this DPA

2.7 **"Main Agreement"** means the agreement concluded between the Controller and the Processor which is underlying to the Personal Data Processing contemplated by this DPA.

2.8 **"Personal Data"** shall have the meaning given in GDPR and herein means the Personal Data transferred by the Controller to the Processor and processed by the Processor under this DPA.

2.9 **"Sales and Delivery Terms"** shall mean the agreement on the supply of IT services entered into by and between the Sub Data Processor and the Data Processor on the date:

2.10 "**SCCs**" means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council approved by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as available here (or successor website): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.

2.11 **"Sub-processor"** means any third-party subcontractor appointed by the Processor to perform Personal Data Processing on behalf of the Processor, as provided in the Sub-processors list available on the Trust Portal here (or successor website):

2.12 **"Third Country"** means any third country, the territory or one or more specified sectors from that third country, or an international organization, which is not a member of the European Union or of the European Economic Area

2.13 **"Transfer Safeguard"** means a solution, other than the SCCs, that enables the lawful transfer of Personal Data to a Third Country in accordance with the GDPR,

including, by way of example and without limitation, adequacy decisions, biding corporate rules, etc.

2.14 **"Trust Portal"** means the collection of documentation and policies made available and amended by IMPULSE B2b SOLUTIONS from time to time on IMPULSE B2b SOLUTIONS's website () and integrated by way of reference in this DPA.

3. Purpose & Governance

3.1 Purpose: The Controller and the Processor have concluded this DPA in accordance with the legal requirements concerning Personal Data protection and to establish their responsibilities regarding the protection of Personal Data which may be processed pursuant to the performance of the Main Agreement. The Parties agree that, under this DPA, the Company acts as a controller and IMPULSE B2b SOLUTIONS acts as a processor, unless the Company is a processor for some or all of the Personal Data, in which case IMPULSE B2b SOLUTIONS is a sub-processor. The Controller acknowledges that Personal Data is not a pre-requisite for the performance of the Main Agreement, or for the access to the Cloud Services, but considering the particularities of each Cloud Service, Personal Data may be transferred to the Processor. While IMPULSE B2b SOLUTIONS understands that the Controller might transfer some Personal Data to it via Cloud Services made available for general availability, there are some scenarios where such transfer is restricted, namely:

3.1.1 out of care for the Controller and the Data Subjects, IMPULSE B2b SOLUTIONS might contractually prohibit or limit the use of Personal Data with products or services offered by IMPULSE B2b SOLUTIONS for preview, early access or evaluation, as further indicated by IMPULSE B2b SOLUTIONS in the underlying terms of use of such products or services;

3.1.2 where legislations allow the transfer of Personal Data to a provider solely subject to certain formalities (such as data localization, certification, or registration with the appropriate regulatory bodies, etc.) and such formalities are not yet fulfilled, as indicated by IMPULSE B2b SOLUTIONS in the applicable documentation, use of Personal Data will not be allowed and the Controller must refrain from using and transferring Personal Data to IMPULSE B2b SOLUTIONS.

3.2 Governance: - This DPA is tailored and applies solely to the Processor's Cloud Services that are used by the Controller and solely to the extent that Personal Data is transferred from the Controller to the Processor, as agreed in the Main Agreement and under this DPA. The Controller has full control over the Personal Data sent for Processing and is responsible for complying with its applicable data protection laws and for assessing whether the use of the Cloud Services meets its compliance and contractual obligations. This DPA does not apply to:

3.2.1 Personal Data processed as a result of the Controller using third party cloud integrations, which are subject to their own terms and conditions and privacy policies;

3.2.2 any data received by IMPULSE B2b SOLUTIONS in connection to the provision of support services, which are subject to the Support Terms available on the Trust Portal;

3.2.3 Any data received by IMPULSE B2b SOLUTIONS in connection to the provision of professional services (such as implementation, trainings, etc.), unless the provision of professional services cannot be done in absence of Personal Data being transferred to IMPULSE B2b SOLUTIONS, and therefore the provisions of this DPA will apply;

3.2.4 Any products and services made available by IMPULSE B2b SOLUTIONS that are not hosted by IMPULSE B2b SOLUTIONS or its processors on behalf of IMPULSE B2b SOLUTIONS and where there is no transfer of Personal Data from the Company to IMPULSE B2b SOLUTIONS.

4. Object of the DPA

4.1 Controller to Processor. The Parties agree that, in accordance with the Applicable Data Protection Law, the Company is the Controller of the Personal Data transferred by the Company to the Processor by using the Cloud Services.

4.2 Scope. This DPA sets forth the general rights and obligations of the Parties, and the specific information and details regarding Personal Data Processing (i.e., purpose, duration, nature and purpose of each processing, type of Personal Data and Data Subjects), as detailed in Exhibit A (Details of the Processing) attached to this DPA. Any amendment to the processing details described in Exhibit A (Details of the Processing) may only be made based on a written instruction from the Controller

5. Processing in accordance with Controller's Instructions

5.1 Controller Instructions. The Processor is required to process the Personal Data only subject to, and within, the limits set forth in the instructions received in writing from the Controller, including with regards to transfers of Personal Data to a Third Country. The Processor will notify the Controller without delay if it considers that a Controller's instruction or any implementation of an instruction received from the Controller breaches or may breach the Applicable Data Protection Law.

5.2 Records of Processing. IMPULSE B2b SOLUTIONS shall maintain the records required under Article 30(2) of the GDPR for the Personal Data and, to the extent applicable to the processing of Personal Data on behalf of Controller, make them available to Controller upon request.

6. Confidentiality and Security

6.1 Confidentiality. The Processor will preserve the confidentiality of the Personal Data and the Processing activities. The Processor shall ensure that any person charged with the Processing of Personal Data by the Processor, either an

employee, a contractor, or a Sub-processor, undertakes to maintain the confidentiality of Personal Data.

6.2 Security of Processing. Having regard to the current state of technology and the varying degrees of risks and severity for the rights and freedoms of individuals, the Processor will implement technical and organizational practices to ensure an adequate level of security for the Personal Data Processing that it carries out, in line with ISO 27001 or similar industry information security standards, as reflected on the Trust Portal. The Processor reserves the right to modify or update its practices, to the extent this will not result in a lower level of security for the Processing activities. Notwithstanding the Processor's practices, the Controller is responsible to safeguard any Personal Data part of its credential information and/or any components under its control and assessing whether its privacy and security obligations are met when using the Cloud Services.

7. Obligations for the Processor

7.1 Access to Personal Data. Subject to, and within the limits provided under the Applicable Data Protection Law (including, by means of example and without limitation, Article 12 para. 5 of the GDPR), the Processor undertakes the obligations listed below with respect to the access to Personal Data.

7.1.1 The Processor shall promptly inform the Controller of requests received by the Processor from Data Subjects exercising their rights under the Applicable Data Protection Law

7.1.2 To the extent technically possible to it, the Processor shall assist the Controller with extracting, deleting or performing any other operations on the Personal Data, or, where possible, provide the Controller with the ability to perform any of the aforementioned actions on the Personal Data.

7.1.3 The Processor shall provide commercially reasonable and timely assistance to Controller, in accordance with the technical capabilities of each Cloud Service, to enable Controller to respond to (i) any request from a Data Subject exercising its rights under the Applicable Data Protection Law; and (ii) any other enquiry or complaint received from a Data Subject or a Supervisory Authority in connection with the Processing of the Personal Data.

7.2 Incidents. The Processor will inform the Controller, without undue delay from becoming aware that an Incident has occurred, and shall provide reasonable information and cooperation to Controller so that the Controller can fulfil the Personal Data Breach reporting obligations it has under the Applicable Data Protection Law. The notice shall be sent to an e-mail address provided by the Controller and available in the Processor's records. The Controller is responsible for providing appropriate and updated contact information. The Parties agree that, by the mere giving notice of an Incident, the Processor does not acknowledge any liability or fault thereof. The Controller acknowledges that it is responsible

for complying with its own legal obligations regarding Personal Data breach notifications. If the Controller suspects that an incident occurred, the Controller shall without undue delay notify the Processor at privacy@impulseb2b.com

7.3 Assistance. Upon written request from the Controller, the Processor shall give reasonable assistance to the Controller in carrying out any assessment of the consequences or impact of Processing of Personal Data and in any consultation with the Supervisory Authority. The Processor will notify the Controller without delay if a Supervision Authority contacts the Processor directly with respect to the processing activities that fall within the subject matter of this DPA.

8. Controller's Rights

8.1 Proofs of Compliance. Upon reasonable written request from the Controller and no more than once (1) a year, the Processor will provide the Controller, without undue delay, with (a) answers to a written security questionnaire provided by the Controller, or references to where information required under that questionnaire is available, (b) a description of the Processor's technical and organizational practices in respect of the Processing of Personal Data, as necessary to assess compliance with this DPA.

8.2 Audit. If the Controller believes, acting reasonably and in good faith, that an on-site or remote audit is necessary to verify compliance with this DPA, the Controller may request that it or a third party conducts an audit, which shall be subject to the conditions set out below.

8.2.1 an audit plan must be agreed by the Parties and, if applicable, the third-party auditor, with eight (8) weeks in advance of the proposed audit date; the audit plan will describe the scope, duration, third party auditor and start date of the audit and shall be limited as to ensure the Processor's confidentiality and security obligations towards its employees and counterparties.

8.2.2 if the audit scope described in the audit plan is addressed in an ISO, SOC or similar verification report performed by a qualified third party in the twelve (12) months prior to the Controller's audit request, the Controller agrees to accept and rely on these reports and Processor's confirmation that there were no material changes in the verified data protection/security measures, and therefore no audit will be performed.

8.2.3 audits may be performed no more than once (1) a year and must be conducted during the business hours, according to Processor's policies, and will not interfere with Processor's business activities.

8.2.4 audits may be performed only if a confidentiality agreement is concluded with the third-party auditor and the audit results will remain confidential and will not be shared with any third party unless agreed by an authorized representative of the Processor in writing.

8.2.5 unless prohibited by legislation binding on the Parties, the Controller must provide the Processor with a copy of the audit report free of charge

8.2.6 audits are performed at Controller's expense and Processor will give reasonable cooperation and assistance.

9. Sub-processors

9.1 Appointment and authorization. The Processor may use certain services provided by the Sub-processors listed in the Sub-processor list to provide the Cloud Services or parts thereof. Furthermore, the Processor may engage other third parties as Sub-processors, and Sub-processors may engage other third-party Sub-processors in connection with the provision of the Cloud Services. The Processor will keep its Sub-processors to the same confidentiality obligations and adequate guarantees for the security of Personal Data as those provided for the Processor in this DPA. The Controller hereby grants a general written authorization in accordance with Article 28 of the GDPR (i) for the appointment, engagement and use of the services of Sub-processors, and (ii) to Subprocessor to carry out the Personal Data Processing activities on the Processor's behalf.

9.2 **Changes of Sub-processors**. When the Processor intends to make any changes to the Sub-processors, it will send a written notice to the Controller, at the e-mail address provided by the Controller and available in the Processor's records. Subject to having a legitimate reason under Applicable Data Protection Law, the Controller will have 30 (thirty) days from the date it received the change notice from the Processor to object to the change and terminate the applicable Cloud Service, by sending a written notice to the Processor at privacy@impulseb2b.com, which will contain at least (i) the name of the Cloud Service to be terminated and (ii) the termination date, which will be no later than 30 (thirty) days from the date of Processor's notice to Controller. The Controller acknowledges its sole and exclusive remedy for objecting to any change in Sub-processors is the termination of the Main Agreement, but only limited to the Cloud Service for which the new Sub-processor is intended to be used. If the Processor does not receive a written notice of objection and termination in accordance with this section, it will deem in good faith that the Controller has accepted the change in Sub-processors. Within the 30 (thirty)-day period from the date of the Processor's notice, the Controller may request that the Parties discuss in good faith a resolution to the objection. Such discussions shall not extend the period for objection and do not affect the Processor's right to use the new Sub-processor(s) after the 30 (thirty)-day period.

9.3 **Mandatory Changes in Sub-processors**. Notwithstanding the foregoing rules setting out the procedure for changes in Sub-processors, the Processor may replace a Sub-processor without advance notice to the Controller where the reason for the change is outside of the Processor's reasonable control and prompt replacement is required for regulatory, security, system integrity, business

continuity purposes or other urgent reasons. The Processor will inform the Controller of the replacement Sub-processor as soon as possible following such change, and the procedure set out above will apply accordingly.

9.4 **Affiliates.** Notwithstanding the foregoing rules setting out the procedure for changes in Sub-processors, the Controller acknowledges, agrees, and hereby gives written authorization under Article 28 of the GDPR to the Processor to engage its Affiliates as Sub-processors. A list of the Processor's Affiliates will be maintained on the Trust Portal or successor website ().

9.5 **Hosting Location**. Personal Data uploaded by the Controller in the Cloud Services will be hosted in the region(s) evidenced in the Sub-processor list. Where technically implemented in a particular Cloud Service, the Controller may configure the hosting location of the Personal Data used therein, provided however that back-ups may have different configurations.

10. Cross-border Transfers of Personal Data

10.1 **Transfer Safeguards.** IMPULSE B2b SOLUTIONS will also process Personal Data, including by using Sub-processors, outside the country in which the Controller or its Affiliates using the Cloud Services are located, in accordance with this DPA and as permitted under Data Protection Law, and only by offering Transfer Safeguards and ensuring that all transfers are made in accordance with Transfer Safeguards.

10.2 **SCC.** Where IMPULSE B2b SOLUTIONS is not located in a Third Country and acts as a data exporter, IMPULSE B2b SOLUTIONS has entered into SCC with, or relies upon, Transfer Safeguards in connection to each Sub-processor located in a Third Country as the data importer. To the extent, Transfer Safeguards cannot be provided, as regulated by the Applicable Data Protection Laws, and where the Processor is located in a Third Country, the SCC is hereby incorporated into this DPA. By executing the DPA, the Parties hereby agree to the execution of the SCC by and between the Processor as "the data importer", and the Controller as "the data exporter" and the SCC will be deemed incorporated into, and considered part and parcel of, this DPA.

10.3 **Description of Processing.** The details required by the SCC, and by Annexes, I and II thereto, are specified in Exhibit B below.

10.4 **Amendments to the SCC.** Unless the Processor notifies the Controller to the contrary, if the European Commission amends the SCCs after the Effective Date, the amended SCCs will supersede and replace the SCCs executed between the Parties by virtue of this section. In addition, if and to the extent a court of competent jurisdiction or Supervisory Authority orders (for whatever reason) that the measures described in this DPA cannot be relied on for the purpose of lawfully transferring Personal Data to Third Countries, the Controller agrees that the Processor may implement any additional measures or safeguards that may be reasonably required to enable a lawful transfer.

11. Term and Termination

11.1 **Term.** This DPA is effective at the Effective Date and will be in force for as long as the Controller uses Cloud Services under the Main Agreement, without exceeding the duration of the Main Agreement. The Parties may agree to terminate this DPA in writing.

11.2 **Consequences of Termination.** Following termination of the Main Agreement and upon express written instructions from the Controller, the Processor will ensure that the Personal Data (including metadata) will be, as requested by the Controller, deleted, or returned to the Controller either manually or, if technically available, via direct export from the relevant Cloud Service. In the absence of any written instruction from the Controller given at the termination of the Main Agreement, the Parties agree that this section constitutes notice by Controller to Processor of the instruction to delete the Personal Data within a reasonable time following termination of the Main Agreement, in accordance with the Applicable Data Protection Law, unless and to the extent retention is required by applicable law, or the Personal Data has been archived on back-up systems due to the Cloud Service functionalities.

12. Liability

12.1 **Liability.** Each Party will be liable for its own actions and/or omissions under this DPA. The Processor will remain fully liable to the Controller for the performance of the obligations that its appointed Sub-processors fail to comply with.

12.2 **Limitation of Liability.** UNLESS OTHERWISE PROHIBITED BY APPLICABLE LAWS BINDING ON THE PARTIES, THE DAMAGES EXCLUSIONS SET OUT IN THE MAIN AGREEMENT APPLY TO ANY LIABILITY UNDER THIS DPA AND THE MAXIMUM AGGREGATE LIABILITY OF EACH PARTY AND/OR THEIR AFFILIATES, FOR ANY AND ALL BREACHES AND CLAIMS (INDIVIDUALLY AND TOGETHER) UNDER OR RELATING TO THIS DPA, AND FOR ALL DATA PROCESSING ACTIVITIES CONTEMPLATED BY THIS DPA, WILL NOT EXCEED THE LIABILITY CAP OR LIMITATION SET OUT IN THE MAIN AGREEMENT. THIS LIMITATION APPLIES WHETHER THE CLAIM ARISES FROM CONTRACT, NON-CONFORMITY OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY. UNLESS OTHERWISE PROHIBITED BY APPLICABLE LAWS BINDING ON THE PARTIES, NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR ANY SPECIAL, INDIRECT, MORAL, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, OR EXEMPLARY DAMAGES, LOSS OF PROFITS, REPUTATION, USE, OR REVENUE, OR INTERRUPTION OF BUSINESS, IRRESPECTIVE OF WHETHER THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. PROCESSOR WILL NOT BE LIABLE FOR ANY DAMAGE CAUSED BY FAILURE OF CONTROLLER TO COMPLY WITH THE DPA OR ANY APPLICABLE PRIVACY POLICIES, LAWS OR REGULATIONS.

13. Miscellaneous

13.1 **Main Agreement.** This DPA is without prejudice to the rights and obligations of the Parties under the Main Agreement, which will continue to have full force and effect. This DPA is incorporated into and made a part of the Main Agreement by this reference.

13.2 **Governing Law.** This DPA shall be interpreted and construed in accordance with the laws of Romania, unless otherwise expressly mandated by the Applicable Data Protection Laws. Any dispute arising in connection with this DPA, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the **courts of INDIA**

13.3 **Entire Agreement.** This DPA constitutes the entire agreement between the Parties with respect to the subject matter hereof and takes prevalence over any prior written or oral agreement between them with respect to such subject matter or in the event of conflicting provisions regarding any rights and obligations granted or incurred by the Parties for purposes of this DPA. Except as otherwise prescribed hereunder, any changes or amendments to the DPA or its Exhibits will be effective only if made in writing and agreed by both Parties.

Exhibit A

Details of the Processing

The Processor shall process the Personal Data received from the Controller in accordance with the details set out below.

Contact person(s) of the Processor	
Purpose (reason) of Processing	
Type of Processing	
Processing duration	
Categories of processed Personal Data	
Data Subjects (ex: employees, customers)	
Data storage/ server location	

Exhibit B
Details required by the Standard Contractual Clauses
and by Annexes I and II

Selection of Module		
Standard Contractual Clauses	Module Two (transfer controller to the processor) is selected as the application module for the entirety of the Standard Contractual Clauses.	
Selection of Options		
Clause 9(a)	Option 2 is selected (general written authorization), with a specified time period of 30 days.	
Clause 17	Option 1 is selected, with the specified Member State of Romania.	
Clause 18(b)	The specified Member State is Romania.	
Annex I		
List of Parties		
Data exporter(s)	*Identity:*	Company and its affiliates
	Contact person's name:	The data exporter's contact is identified in the Main Agreement.
	Activities relevant to data transferred under these Clauses:	The activities required to perform the Main Agreement: execution of instructions of Controller in accordance with the Main Agreement, continuous improvement of service features and functionalities, communication to authorized users, backup and restoration of Personal Data stored in the Cloud Service, security, monitoring etc.
	Role:	Controller
Data importer(s)	*Identity:*	IMPULSE B2b SOLUTIONS. (or one of its affiliates based in a Third Country) and its Sub-processors
	Contact person's name:	privacy@impulseb2b.com

	Activities relevant to data transferred *under these Clauses:*	The activities required to perform the Main Agreement: execution of instructions of Controller in accordance with the Main Agreement, continuous improvement of service features and functionalities, communication to authorized users, backup and restoration of Personal Data stored in the Cloud Service, security, monitoring etc.
	Role:	Processor
Description of Transfer		
Categories of data subjects whose personal data is transferred	Individuals whose Personal Data is provided by the Controller to the Processor by using the Cloud Services under the Main Agreement.	
Categories of personal data transferred	The controller determines the categories of data for each Cloud Service used under the Main Agreement.	
Sensitive data transferred	N/A, performance under the Main Agreement does not require the transfer of any sensitive data	
The frequency of the transfer	Personal Data is transferred continuously during the term of the Main Agreement.	
Nature of the processing	As necessary for the performance of the Main Agreement concluded between the Parties.	
Purpose(s) of the data transfer and further processing	Performing the Main Agreement concluded between the Parties.	
The period for which the personal data will be retained	Personal Data shall be retained for the duration of the Main Agreement and subject to Section 9.2 of the DPA	
Transfers to sub-processors	The list of Sub-processors and the processing activities performed by them is available here:	
Competent Supervisory Authority		
The supervisory authority with responsible for ensuring compliance by the data exporter	The applicable supervisory authority is the authority in the EU Member State where the data exporter is established or other supervisory authority with the right by operation of law to supervise compliance.	

Annex II
Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

Description of the technical and organizational measures implemented by the data importer(s)	The Processor will maintain at least the technical and organizational security measures set out in the DPA and on the Trust Portal ((or successor website))