DATA PROCESSING AGREEMENT

Concluded on ……. in Babimost

by and between:

…….., with its registered office at: ……, entered into the register of entrepreneurs of the National Court Register kept by the District Court ……, under the KRS (National Court Register) number: ……., NIP (Tax Identification Number): ……., REGON (National Business Registry Number): …….,

represented by ……,

hereinafter referred to as **the Entrusting Entity**,

and

Testportal spółka z ograniczoną odpowiedzialnością, with its registered office in Babimost, Poland, European Union, at the following address: ul. Szewska 9, postal code: 66 – 110, Poland, EU, entered into the register of entrepreneurs of the National Court Register kept by the District Court in Zielona Góra, VIII Commercial Division, under the number: 0000512302, NIP (Tax Identification Number): 9731017273, REGON (National Business Registry Number): 081208720,

represented by Krystian Dabrowski – President of the Management Board,

hereinafter referred to as **the Processor**,

hereinafter collectively referred to as **the Parties,** or separately referred to as **the Party**.

Keeping in mind that the Parties, on the basis of the Terms and Conditions available on the www.testportal.net website, or on any related websites, have concluded an Agreement for the provision of services by electronic means, hereinafter referred to as **the Service Agreement**. The Parties have agreed as follows:

1. The Subject of the Agreement

The Parties agree that, in order to fulfill the obligations arising from the provisions of the law, and in particular, the provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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), hereinafter referred to as **the GDPR**, and the Act on the Protection of Personal Data, hereinafter referred to as **the Act**, as well as for the purpose of the proper implementation of the Service Agreement, the Entrusting Entity entrusts the Processor with personal data for processing, referred to in § 2 below, in order for the Processor to provide services specified in the Service Agreement that are within the scope of the Service Agreement, on the terms and conditions specified in this Agreement, and in compliance with the provisions of the Service Agreement.

2. The Scope of the Entrusted Data

1. The Entrusting Entity entrusts the Processor with the following personal data for processing:
    a) The surnames and names of the account and sub-account users, as well as of the authors of the online Tests entered by the User, hereinafter referred to as **the Tests**,
    b) The e-mail addresses of the users of the accounts and sub-accounts,
    c) The personal data of the Respondents (i.e., the persons answering the questions contained in the Tests which have been made available to them), within the scope referred to in par. 3.
2. The personal data referred to in par. 1 is obtained from the User.
3. The data obtained from the Respondents is as follows:
    a) Surnames and names,
    b) E-mail addresses,
    c) Other:
    ……
4. The Entrusting Entity is the only Party responsible for providing the correct, full, and current information in the scope of entrustment referred to in par. 1.
5. The Entrusting Entity obliges to entrust the personal data to the Processor only within the scope indicated in par. 1 and par. 3 (not a wider scope), as well as to verify if the scope of the entrusted personal data is consistent with the disclosed state.
6. The Entrusting Entity may, at any time, change (extend or limit) the scope of entrustment specified in par. 3.
7. The Entrusting Entity declares that it will not entrust any special category data to the Processor for processing, as per the provisions of Art. 9 of the GDPR.

3. The Declarations of the Parties

1. As the Personal Data Controller, the Entrusting Entity declares that the personal data entrusted to the Processor for processing has been collected in accordance with the applicable law.
2. The Processor declares that they oblige to use the personal data only within the scope necessary for the performance of the Service Agreement and for the purpose specified therein.

4. The Obligations of the Parties

1. The Processor obliges to process data entrusted by the Entrusting Entity solely upon receiving documented instruction from the Entrusting Entity, wherein specified services referred to in the Service Agreement, as well as any particular services outlined by the Entrusting Entity, are considered such an instruction.
2. The Processor is obliged to provide technical and organizational means of protection of processed data when processing it. In particular, the Processor should secure said data against access by unauthorized persons, loss, damage, and destruction. The fulfillment of the terms referred to in Art. 28, par. 1 of the GDPR has been documented in Annex NO. 2 of this agreement, which contains the “Questionnaire - Verification of the Processor.”
3. To fulfill the obligation mentioned in the previous paragraph, the Processor is obliged to maintain documentation describing the method of data processing, and in particular, a register of the categories of personal data processing.
4. The Processor commits to assisting the Entrusting Entity in fulfilling the duties referred to in Art. 32-36 of the GDPR, taking into consideration the character of processing and available information.
5. The Processor is not authorized to transfer personal data to any third party, excluding employees and collaborators working for or operating on behalf of the Processor. To avoid ambiguity, Parties concur that only persons authorized in writing by the Processor can process entrusted data. The Processor is obliged to record every authorization or revocation of authorization in the "Records of Persons Authorized to Process Personal Data.”
6. The Processor is obliged to collect from its employees and collaborators, who will implement the subject of this Agreement as well as the Agreement for the provision of Services by electronic means, declarations on the indefinite obligation to keep the entrusted personal data confidential. The Processor commits to producing the declarations referred to in the preceding sentence within seven working days of any justified request by the Entrusting Entity.
7. The Processor is obliged to train its employees and collaborators on the methods of securing the processed data referred to in this Agreement.
8. The Processor will make available, upon the request of the Entrusting Entity, all information necessary to demonstrate the fulfilment of obligations arising from the GDPR and this Agreement. The Processor obliges to enable the Entrusting Entity or an auditor authorized by them to conduct audits, including inspections, and actively participate in them. The Entrusting Entity will inform the Processor at least two weeks in advance about the time and form of the inspection or audit by a means accepted by the Parties as a form of contact. The audit or inspection will take place during the Processor's working days and hours.
9. In the event of a breach of the protection of the entrusted personal data, the Processor is obliged to immediately, no later than 24 hours from the reception of such information, report it to the Entrusting Entity, taking into account the provisions of Art. 33 of the GDPR.

5. The Further Entrusting of the Processing of Personal Data

1. The Processor can entrust the personal data covered by this Agreement for further processing to subcontractors only for the purpose of the fulfilment of the contract and only in the absence of a written objection by the Entrusting Entity within seven days from the date of receipt of information from the Processor about the intention to further entrust it, taking into account par. 2 of this section. Information about the intention to further entrust data will be sent electronically to the e-mail address assigned to the User's account (account of the Entrusting Entity). This also applies to the transfer of data to a third country or an international organization. The consent of the Entrusting Entity is not required if the obligation to transfer the data by the Processor results from Polish or European Union law. In this case, prior to the commencement of processing, the Processor will inform the Entrusting Entity about this obligation, unless the law prohibits the provision of such information due to important public interest.
2. The Entrusting Entity agrees to further entrust the processing to subcontractors with whom the Processor cooperates at the time of signing this contract and who are indicated in Annex 1 of this contract. The Processor states that cooperation with these subcontractors is necessary for the proper implementation of the Agreement for the provision of Services by electronic means and this Agreement. Further, entrusting the data to Ably Realtime Ltd (indicated in Annex 1) may involve storing data on servers located in Great Britain. In the above case, the data is transferred to a country that ensures an adequate level of protection, in accordance with the decision of the European Commission of June 28, 2021 (C (2021) 4800 final).
3. The entity to which the processing of personal data will be entrusted under subcontract should meet the same requirements as are to be met by the Processor, as well as provide a guarantee of the proper performance of obligations of personal data protection. The Processor is fully liable to the Entrusting Entity if a subcontractor fails to comply with the obligations to protect the personal data of the Entrusting Entity.
4. In the event of an objection filed by the Entrusting Entity, referred to in par. 1 of this section, the Processor will be entitled to terminate this Agreement and the Agreement for the provision of Services by electronic means with immediate effect if further entrusting the processing to a particular subcontractor was necessary for the proper fulfilment of this Agreement and the Agreement for the provision of Services by electronic means.

6. The Cooperation of the Parties

1. During the term of this Agreement, the Parties oblige to cooperate closely — including via the Data Protection Officers, if they have been appointed by any of the Parties — and inform each other about any circumstances having, or which may have, an influence on the implementation of this Agreement.

2. The Processor is obliged to assist the Entrusting Entity as the Personal Data Controller in fulfilling the obligation of responding to the requests of the persons whom the data regards, within the scope of the personal data entrusted for processing.

7. Liability

1. Each Party is responsible for damages caused to the other Party and third parties in connection with the fulfilment of this Agreement, in accordance with the provisions of the GDPR, the Act, other applicable laws, and the provisions of this Agreement.
2. When assessing the legal liability of the Processor, Art. 82, par. 2 of the GDPR applies, according to which the Processor is liable for damages caused to a third party only when he has failed to fulfill the obligations imposed on him by the GDPR, or when he acted outside or against the lawful directives of the Entrusting Entity.
3. If the Entrusting Entity has compensated the third party in full for damage caused by processing in which the Processor participated, the Entrusting Entity has the right to request that the Processor reimburse part of the compensation, in accordance with the conditions set out in the previous paragraph.
4. In the event of damage caused unintentionally by the Processor, the recourse liability of the Processor towards the Entrusting Entity will be limited.
    a. If the total duration of the Agreement for the provision of Services by electronic means exceeds six months, the amount will be limited to the amount received in payments from the Entrusting Entity in the last six months in connection with the fulfilment of the Agreement for the provision of Services by electronic means,
    b. If the total duration of the Agreement does not exceed 6 months, the amount will be limited to the amount received in payments from the Entrusting Entity in connection with the fulfilment of the Agreement for the provision of Services by electronic means.
5. In the event of claims filed against the Entrusting Entity by persons whose data has been entrusted for processing, the Entrusting Entity shall immediately inform the Processer of this fact. In cases where the Processor is liable for the claims referred to in the preceding sentence (in accordance with Art. 82, par. 2 of the GDPR), the Processor is obliged to release the Entrusting Entity from liability and reimburse the costs incurred in this respect (including legal costs) and to satisfy the claims of such persons in the manner prescribed by law.
6. To avoid ambiguity, the Processor is responsible for the actions or omissions of its employees and other persons with the help of whom it processes the entrusted personal data, as well as for its own actions or omissions.

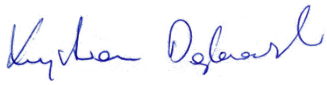
8. The Duration and Termination of the Agreement

1. This Agreement is valid for the duration of the Service Agreement.

2. Each Party is entitled to terminate this Agreement with one month's notice, subject to par. 3 and par. 4 of this section.
3. The Entrusting Entity is entitled to terminate this Agreement without notice and with immediate effect:
    a. In case of a gross breach by the Processor of the purpose and scope of the processing of the entrusted personal data specified in this Agreement,
    b. If, as a result of an inspection carried out by the President of the Personal Data Protection Office, it is proven that the Processor has not implemented appropriate technical and organizational means referred to in the GDPR, the Act, and any other relevant provisions of the law.
4. In the event of termination of this Agreement, the Entrusting Entity may, within seven days from submitting the request to delete the account, download the entrusted data via this account. To secure the functioning of the system, the data may be stored by the Processor in the form of backup copies for seven subsequent days after the expiration of the period indicated in the preceding sentence, from which they can no longer be restored at the User's request. After this deadline, the Processor will irretrievably delete the data from the system and all backups.

9. Final Provisions

1. The Agreement shall enter into force on the day of its signing by both Parties.
2. The Processor cannot transfer the rights or obligations under the Agreement without the prior written consent of the Entrusting Entity.
3. In matters not covered by this Agreement, the relevant provisions of the law, in particular the provisions of the GDPR, the Act, and the Civil Code, shall apply.
4. The court competent to settle disputes arising in connection with the performance of this Agreement is the court competent for the seat of the Processor.
5. This Agreement has been drawn up in two identical copies, one for each of the Parties.

	Krystian Dabrowski
……	……
Name and surname	Name and surname
	
……	……
Signature	Signature
Entrusting Entity	**Processor**

ANNEX NO. 1 - List of Current Sub-processors:

1) Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland, VAT number IE8256796U
2) Ably Realtime Ltd Labs Triangle, Chalk Farm Rd, London, NW1 8AB, United Kingdom, Company Number 6946246, VAT number GB974747564
3) Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxembourg R.C.S. Luxembourg: B186284

Annex NO. 2 - Questionnaire – Verification of the Processor:

Area of verification	**No.**	**Question**	**Answer: YES/NO**	**Additional notes**
GENERAL INFORMATION	1.	Does the Processor have experience in providing services connected with entrusting data processing? If yes, then for how long?	YES	Because of the scale and character of business operations, the Processor is a processor in most business relations and has been acting as such since June 2014.
	2.	Did the Processor designate a Data Protection Officer?	YES	Konrad Cioczek dpo@testportal.net
	3.	Does the Processor have references from other entities for which it provided data processing services on their request?	NO	
	4.	Has there been a final court or supervising authority ruling stating a breach of data protection by the Processor?	NO	
PERSONNEL	5.	Does the Processor ensure that access to the entrusted data is granted only to authorized persons who have also been obliged to keep the data confidential (including after termination of their employment / cooperation)? The Processor keeps a register of authorized persons.	YES	
	6.	Have the persons dedicated to the data control service on the part of the Processor been trained in the principles of safe personal data processing and	YES	

		familiarized with the relevant regulations in force?		
	7.	Does the Processor take steps to constantly increase the awareness of and knowledge about the personal data protection and information security of persons who process personal data as part of their official duties?	YES	
ACCESS CONTOL	8.	Is private equipment used in remote work to process entrusted personal data?	NO	Remote work is done on the equipment provided by the Processor.
	9.	Do devices used to process the entrusted personal data by the Processor have access control configured?	YES	
	10.	Do the Processor's employees participating in the processing of entrusted personal data receive an individual ID for their ICT systems?	YES	
	11.	Are the ICT system passwords used by the Processor changed periodically or if the need arises?	YES	
IMPLEMENTED RULES AND POLICIES, CONTROL PROCEDURES.	12.	Does the Processor have a developed, approved, and implemented Personal Data Protection Policy or other relevant document regulating the rules of personal data processing in the organization?	YES	The Processor has implemented the Personal Data Protection Policy.
	13.	Does the Processor implement a clear desk and clear screen policy?	YES	

	14.	Does the Processor keep a Categories of Processing Activities Register, an Authorized Persons Register and a Register of Incidents - in accordance with the provisions of the GDPR?	YES	
	15.	Does the Processor implement an approved code of conduct or certification mechanism pursuant to Art. 40-42 of the GDPR?	NO	So far, no codes of conduct have been approved by the supervising authority.
	16.	Does the Processor ensure the upholding of the rights of persons to whom the processed data relate, as per Chapter III of the GDPR?	YES	
	17.	Has the Processor carried out an ICT security audit in the last two years?	YES	
	18.	Has the Processor submitted to an external audit by independent auditors with regard to the rules on the protection of personal data in its organization in the last two years?	YES	
	19.	Does the Processor carry out regular audits and inspections in regards to compliance with the provisions related to personal data protection in the organization?	YES	
	20.	Does the Processor hold periodical reviews of the risks associated with the personal data processing?	YES	
	21.	In the event of a risk-level change, does the	YES	

		Processor introduce new, appropriate technical and organizational data protection measures, according to the results of analyses?		
	22.	Does the Processor implement the principles of privacy by design when introducing new solutions?	YES	
	23.	Does the Processor process data in accordance with the principles of privacy by default?	YES	
	24.	Has the Processor implemented a personal data breach procedure?	YES	
	25.	Is the Processor able to demonstrate the proper implementation of the principles of personal data protection in the organization?	YES	
TECHNICAL AND PHYSICAL SECURITY MEASURES	26.	Is the software used by the Processor regularly updated?	YES	
	27.	Does the Processor implement technical measures to protect the ICT system against unauthorized access? If so, what are they?	YES	Anti-virus software, firewall, file backups, individual logins, and passwords for the users of electronic devices (including the minimum password requirements policy).
	28.	Is the Processor able to restore personal data availability in the event of a physical or technical incident?	YES	
	29.	Does the Processor apply physical protection measures designated to secure the processed data against unauthorized	YES	External and internal monitoring, locked doors.

		access? If so, what are they?		
	30.	In the case of data transmission via ICT systems or external storage, is the data encrypted?	YES	
SUB-PROCESSORS	31.	Does the Processor use cloud solutions in the entrusted personal data processing? If so, indicate suppliers.	YES	AWS Cloud - Public cloud MS Azure - Public cloud
	32.	Does the Processor use subcontractors to whom it transfers the entrusted data? If so, please indicate entities.	YES	Entities mentioned in Annex NO. 1.
	33.	Have the subcontractors indicated in Point 31 signed a Data Entrustment Agreement?	YES	
	34.	Have the subcontractors mentioned in Point 31 been verified in terms of the implementation of appropriate personal data protection measures?	YES	
	35.	Will the entrusted personal data be processed outside the EEA? If so, provide details.	YES	In connection with the sub-processing of data by Ably Realtime Ltd Labs Triangle, personal data may be processed in the United Kingdom. As per the decision of the European Commission on June 28, 2021, Great Britain is recognized as a country meeting an adequate level of personal data protection, compliant with the GDPR.