DATA PROCESSING AGREEMENT

hereinafter referred to as the **Agreement** is concluded by and between the following parties:

(1) **Association for Applied Research in IT**

company with registered seat at Branická 26/43, Braník, 147 00 Prague 4 Czech Republic, Business ID No. 10684271, registered with City Court in Prague under the registration No. L 74638, on behalf of which act(s) independently Jaromír Hanzal, Director, e-mail:

(**AAVIT** or the **Controller**)

And

(2) **National Coalition for Digital Skills and Jobs of the Slovak Republic**

interest association of legal persons with registered seat at Mlynské nivy 18890/5, 821 09 Bratislava – city district Ružinov, the Slovak Republic, ID No. 52 828 123, registered with Registry of interest associations of legal persons maintained by the District Office Bratislava with registration No. OU-BA-OVVS1-2019/140232, e-mail:

(**Digital Coalition** or the **Processor**)

concluded in particular under the provisions of

a) Article 28(3) of 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) (the **GDPR**)

b) and also in accordance with the provisions of other applicable legislation of the Slovak Republic and applicable legal acts of the European Union.

with the following content:

PREAMBLE

A. On 6 May 2024, AAVIT and the Digital Coalition concluded the Memorandum of Cooperation (the **Main Agreement**), the subject of which is cooperation on IT Fitness Test 2024. The performance of the Main Agreement relates to the implementation of the IT Fitness Test project to be implemented by the Digital Coalition (the **Project**).

B. In the performance of the Main Agreement, the Digital Coalition will process information relating to identified or identifiable natural persons (the **Data Subject**). This information constitutes personal data within the meaning of the GDPR (the **Personal Data**).

C. With regard to such a setup of relationships, AAVIT is the controller within the meaning of the GDPR and the Digital Coalition is the processor.

D. Pursuant to the provisions of Article 28(3) of the GDPR, the processing of personal data by the processor must be governed by an agreement which will bind the processor to the controller and which will set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data processed, the categories of data subjects and the obligations and rights of the controller.

Taking into account the above, the Controller and the Processor agree on the following terms and conditions.

ARTICLE 1: INTRODUCTORY PROVISIONS AND REPRESENTATIONS OF PARTIES

1.1. The processing of the Personal Data pursuant to the Agreement is governed primarily by the GDPR; in some specific cases, the processing may also be governed by the provisions of Act No. 18/2018 Coll. on the Protection of Personal Data and on Amendments and Additions to Certain Acts, as amended (the **Data Protection Act**; together with the GDPR, the **Data Protection Regulations**).

1.2. The Processor represents that it is authorised to conclude the Agreement and to perform the obligations set out in the Agreement. The Processor also represents and assures the Controller that to ensure the protection of the rights of the Data Subjects, it has taken sufficient technical and organisational measures and provides sufficient guarantees so that the processing of the Personal Data complies with the requirements of the Data Protection Regulations.

1.3. The Controller represents that it is entitled to enter into and perform the Agreement and to entrust the Processor with the processing of the personal data under the terms and conditions agreed in the Agreement.

ARTICLE 2: SUBJECT MATTER AND PURPOSE OF AGREEMENT

2.1. **[Subject-Matter of Agreement]** The subject-matter of the Agreement is **(i)** the mandate of the Processor granted by the Controller to process the Personal Data of the Data Subjects for the purposes specified in the Agreement, in the extent and under the conditions specified in the Agreement, and the acceptance of the mandate by the Processor.

2.2. **[Purpose of Agreement]** The purpose of the Agreement is to regulate the mutual rights and obligations of the Parties regarding the processing of the Personal Data of the Data Subjects by the Processor on behalf of the Controller so that the processing is carried out in accordance with the Data Protection Regulations and to ensure sufficient and effective protection of the Personal Data processed.

2.3. **[Mandate]** AAVIT, as a controller, hereby authorises Digital Coalition, as the processor, to process the Personal Data on behalf of AAVIT.

ARTICLE 3: PERSONAL DATA PROCESSED

3.1. **[Purpose of processing of Personal Data]** The processing of the Personal Data is solely for the purpose of the performance of the Main Agreement. The Processor shall not be entitled to process the Personal Data for any other purpose without the prior written consent of the Controller.

3.2. **[Place of processing of Personal Data]** The Parties agree that the place of processing of Personal Data shall be the registered office of the Processor or its premises. Processing of the Personal Data by the Processor at any other location is only possible with the prior written consent of Digital Coalition.

3.3. **[Type of Personal Data]** The Controller shall provide the following Personal Data to the Processor:

a) **identification data of** the Project participants (and, where applicable, their legal representatives), namely first and last name, date of birth;

b) **contact details of** the Project participants (and, where applicable, their legal representatives), namely -email address;

c) **data on the physical characteristics** of the Project participants, namely their gender, if they provide it;

d) **information on the target group of the Project participants**, specifically whether the participant is a pupil, student, teacher, employee or a person interested in improving his/her digital skills;

e) **data related to the inclusion of the Project participants in the target group**, for students and pupils information on their school, year and class/group, for educators information on their school and class/group, for employees and persons interested in improving their digital skills information on their country of origin, highest level of education attained, organisation and department/group (if relevant);

f) **other information** that Project participants provide about themselves.

3.4. **[Categories of Personal Data processed]** The Personal Data provided by Digital Coalition to the Processor is general personal data. The Processor does not have the right to process special categories of personal data within the meaning of Article 16 of the Data Protection Act and Article 9 of the GDPR.

3.5. **[Categories of Data Subjects]** The Data Subjects are the participants of the Project, i.e. in particular **(i)** pupils and students of primary, secondary and higher education institutions (including pupils and students from Ukraine), or their legal representatives, **(ii)** educators, (**iii)** employees and **(iv)** persons interested in improving their digital skills.

3.6. **[Period of processing of Personal Data]** The Processor is entitled to process the Personal Data on behalf of the Digital Coalition from the effective date of the Agreement until the termination of the Main Agreement, unless a shorter period of time results from the instructions of the Controller or from the law.

3.7. **[Nature of Processing of Personal Data]** Regarding the Personal data the Processor processes, the Processor shall have the right to:

a) obtain and record;

b) organise, store and archive;

c) to inspect, rectify, update;

d) process it by automated and non-automated means of processing; processing by automated means will be carried out by the Processor in the internal system of Digital Coalition;

e) process by other processing operations permitted by law;

f) erase and discard.

ARTICLE 4: CONDITIONS FOR PROCESSING PERSONAL DATA

4.1. **[Processed Data]** The Processor shall process Personal Data **(i)** provided to the Processor by the Controller in connection with and for the purpose of the Main Agreement, **(ii)** obtained by the Processor in the performance of the Main Agreement, or **(iii)** provided to the Processor directly or indirectly by the Data Subject, solely to the extent necessary for the fulfilment of the purpose of the processing pursuant to the Agreement.

4.2. **[Basic Processing Conditions]** The Processor undertakes to process Personal Data only on the basis of the Controller's instructions and according to the terms and conditions set out in the Agreement and undertakes to comply with the safeguards set out in the Agreement.

4.3. **[Controller's Instructions]** The Controller shall be liable for the instructions given to the Processor in relation to the processing of the Personal Data; this does not relieve the Processor of its obligation to inform the Controller if, in its opinion, a particular instruction breaches the Data Protection Regulations. In such a case, the Processor shall only carry out such operations with the Personal Data that cannot wait until the remedy is implemented. If the execution of the Controller's instructions requires the incurrence of additional costs on the part of the Processor in connection with the execution of such instructions, the Processor shall be entitled to claim reimbursement of the costs incurred, unless the acts in question are part of the remuneration under the Main Agreement.

4.4. **[Rights and obligations of Controller]** The Controller shall be:

a) obliged to process the Personal Data in accordance with the Data Protection Regulations;

b) entitled to give the Processor written instructions regarding the processing of the Personal Data;

c) obliged to regularly update the data on the Personal Data processed as set out in Article 3 of the Agreement.

4.5. **[Basic Obligations of Processor]** The Processor shall:

a) provide the Controller with any and all assistance to the extent necessary to fulfil the purpose of the Agreement and the Main Agreement and any information necessary to demonstrate compliance with the Processor's obligations under the Agreement and the Data Protection Regulations;

b) process the Personal Data in accordance with the applicable law, in particular the Data Protection Regulations, and only for the processing period specified under the Agreement;

c) notify (and make available to) its employees the Privacy Policy, the current version of which is available at https://itfitness.eu/cs/stranky/ochrana-osobnich-udaju/;

d) help the Processor to ensure compliance with its obligations under the GDPR, taking into account the nature of the processing and the information available to the Processor;

e) taking into account the nature of the processing, the Processor shall assist the Controller as much as possible by appropriate technical and organisational measures in fulfilling its obligation to respond to requests to exercise the data subject's rights under Chapter III of the GDPR.

4.6. **[Processing in accordance with Purpose]** The Processor shall not use or aggregate the Personal Data for purposes other than those specified in the Agreement or the Main Agreement, i.e. the Processor shall:

a) process the Personal Data solely for the purposes set out in the Agreement or the Main Agreement;

b) process only Personal Data that is adequate in scope and content for the intended purpose and necessary to achieve that purpose;

c) keep data collected for different purposes separate and ensure that Personal Data is processed only in a manner that is appropriate to the purpose for which it was collected;

d) to only process the Personal Data that is correct, complete and up-to-date in relation to the purpose for which it is being processed and deal with incorrect and incomplete data in accordance with the Data Protection Regulations;

e) process the Personal Data in such a way that the fundamental rights and freedoms of data subjects are not violated, in particular the right to preserve human dignity;

f) not obtain the Personal Data from the Data Subjects under the pretext of another purpose or other activity;

g) process the Personal Data in accordance with good morals and act in a manner that does not contravene the law.

4.7. **[Dealing with suggestions from Data Subjects]** If the Processor receives a request or suggestion from the Data Subject in relation to the processing of the Personal Data pursuant to the Agreement, the Processor shall promptly submit such request or suggestion to the Controller and shall provide the Controller with assistance in fulfilling its obligations in relation to the requests and suggestions of the Data Subjects.

4.8. **[Termination of Processing]** Upon termination of the processing of the Personal Data, the Processor shall delete or return all Personal Data to the Controller and delete all existing copies of the Personal Data, unless the retention of such data is required by law.

4.9. **[Demonstration of compliance and facilitation of audits]** The Processor shall provide the Controller with all information necessary to demonstrate compliance with its obligations under Article 28 of the GDPR and shall allow and contribute to audits or inspections carried out by the Controller or its authorised auditor; it shall also allow the Data Protection Authority to check compliance with the Data Protection Rules and compliance with the subject matter of the Agreement.

4.10. **[Exceptions to being governed by the Agreement and the Instructions]** The Processor shall only process Personal Data on the basis of the Main Agreement or documented written instructions from the Controller, including in respect of the transfer of Personal Data to a third country or an international organisation, except where required by European Union law or the law of a Member State to which the Processor is subject, in which case the Processor shall notify the Controller of this legal requirement prior to processing, unless the law in question prohibits such notification for compelling reasons of public interest.

4.11. **[Notification of breaches]** The Processor shall promptly notify the Controller in writing if, in its opinion, the Data Protection Regulations or other relevant legislation are being breached, even if the breach is by the Controller or if the Controller's instruction is in breach of the Data Protection Regulations pursuant to the provisions of paragraph 4.3 of the Agreement.

4.12. **[Public Authorities]** The Agreement does not prevent the Processor from processing Personal Data in a manner required by law, regulation or a competent court or supervisory authority. If a supervisory authority or a competent court issues a request relating to the processing of the Personal Data, including a request for restriction of processing, erasure, rectification of Personal Data, provision of information or any other measures, the Processor shall inform the Controller without undue delay of the receipt of any such request prior thereto, before responding to such request or taking any other action in relation to the Personal Data being processed, or as soon as can reasonably be expected if any law or regulation requires the Processor to respond promptly to a supervisory authority or competent court, except where such notification to the Controller is prohibited by law, regulation or decision or order.

4.13. **[Notification of inspection]** The Processor shall immediately notify the Controller of the initiation or conduct of an inspection or investigation by the Data Protection Authority or another supervisory authority and provide the Controller with detailed information on the progress of such inspection as well as on any subsequent administrative or judicial proceedings. If the Data Protection Authority or another supervisory authority initiates an inspection or investigation of the Controller, the Processor shall provide the Controller with all necessary cooperation in such inspection.

ARTICLE 5: ENSURING THE PROTECTION OF PERSONAL DATA

5.1. **[Technical and organizational measures]** The Processor is obliged to adopt and ensure compliance with the relevant technical and organizational measures pursuant to the provisions of Section 39 of the Data Protection Act and Article 32 of the GDPR that are appropriate to the data processed and, taking into account the type of processing and the information provided, will support the Controller in complying with the obligations set out in the provisions of Article 39, Article 40 and Article 41 of the Data Protection Act or the corresponding provisions of the GDPR. The Processor shall regularly test, assess and evaluate the effectiveness of its measures taken. The Processor undertakes to comply with the technical and organisational measures set out in **Annex 1** of the Agreement. Where necessary, the Processor shall take other appropriate measures to ensure an adequate and appropriate level of security of the Personal Data (taking into account the state of the technology, the costs, the nature, the scope, the context, the purposes and the risks of the processing carried out).

5.2. **[Focus of the measures]** The technical and organisational measures taken are aimed in particular at:

a) pseudonymisation and encryption of the Personal Data;

b) the ability to ensure the continued confidentiality, integrity, availability and resilience of service processing systems;

c) the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

5.3. **[Security of Personal Data]** The Processor is obliged to protect the Personal Data against damage, destruction, loss, alteration, unauthorised access and disclosure, disclosure or publication, as well as against any other impermissible means of processing; for this purpose, the Processor is obliged to take appropriate technical, organisational and personnel measures corresponding to the manner in which the Personal Data is processed for the individual purposes of processing, in the form and under the conditions set out in the Data Protection Regulations, taking into account in particular the technical means to be used, the confidentiality and importance of the Personal Data processed, as well as the extent of the possible risks that are capable of impairing the security or the functionality of the information system.

5.4. **[Security Breach]** In the event of a breach of the security of Personal Data pursuant to the provisions of the preceding paragraph, the Processor shall promptly take appropriate remedial measures as soon as practicable and shall provide the Controller with all relevant information requested by the Controller in this regard and the necessary cooperation in order to remedy the consequences of the breach of the security of the Personal Data.

5.5. **[Secrecy and Confidentiality]** The Processor is obliged to maintain the secrecy of all Personal Data with which it comes into contact. The Processor shall also oblige all its employees or other persons who come into contact with the Personal Data to the duty of confidentiality; they shall not use the Personal Data for their own purposes, nor shall they disclose or disclose them to anyone without the prior written consent of the Controller, except where the disclosure or disclosure of the Personal Data is necessary to ensure the processing of the Personal Data pursuant to this Agreement or where the obligation to disclose or disclose the Personal Data arises from specific legislation or from a decision of a public authority. The Processor shall maintain this confidentiality even after the termination of the assignment under the Agreement and shall keep a record of any disclosure or provision of Personal Data made pursuant to the preceding sentence for the entire duration of the Agreement.

ARTICLE 6: MANNER OF PROCESSING OF PERSONAL DATA

6.1. **[Processing in electronic form]** The Processor shall process the Personal Data in electronic form using information technology means.

6.2. **[Basic Security Principles]** In processing the Personal Data, the Processor shall adopt and comply with mainly the following Personal Data Security Principles:

a) electronic data containing Personal Data will be stored and further processed exclusively on media (e.g. portable or non-transitory data carriers, network data storage devices) that are in the possession or in the legitimate use of the Controller or the Processor;

b) the Personal data shall not be aggregated with personal data processed by the Processor for other purposes or for other controllers. Personal Data will not be aggregated with Personal Data processed for third parties without the prior written instruction of the Controller;

c) access to Personal Data is only granted to the relevant authorised persons using individual access data, to the extent appropriate to the authorisation of the relevant authorised person;

d) electronic records will be made of the processing of Personal Data, which will enable the determination of when, by whom and for what reason the Personal Data was processed;

e) the Personal Data carriers will be secured and protected from unauthorised access.

6.3. **[Documentation]** The Processor is obliged to document the technical and organizational measures taken to protect Personal Data, to update this documentation regularly and to submit it to the Controller for inspection upon request. The Processor shall also submit to the Controller any reports documenting security audits carried out by the Processor or an auditor appointed by the Processor. The Processor shall allow audits and inspections conducted by the Controller or other auditor to verify the security of Personal Data, upon prior notification by the Controller.

6.4. **[Processing only within the EU/EEA]** The Processor may process Personal Data on its information systems as well as on the information systems of third parties only within the EU/EEA. Should cross-border processing of Personal Data take place, the Processor is obliged to obtain the Controller's consent to the cross-border processing.

6.5. **[Approval of Transfer]** The Processor shall inform the Controller in advance of any transfer of the Personal Data not referred to in the preceding paragraph. Unless the Controller objects in writing to such transfer within 15 calendar

days after the Processor has informed it of the intended transfer, the Processor is entitled to carry out such transfer subject only to the provision of appropriate safeguards (European Commission standard contractual clauses, Data Privacy Framework, etc.). If the Controller objects to the transfer within the aforementioned time limit, the Processor shall make reasonable efforts to modify the data transfer or recommend a commercially reasonable modification to the performance of the Main Agreement in order for the Parties to avoid such transfer of the Personal Data. If the Processor fails to make such change or if the Controller refuses to make such change within 60 calendar days, the Controller may terminate the Agreement within another 60 calendar days from the notice (or, if the Processor fails to respond, from the expiration of the 60 days available for the Processor's notice). If the Controller does not terminate the Agreement within the specified period, this shall be deemed to be the Controller's consent to the transfer of the Personal Data.

6.6. **[Audit]** The Controller or a recognised independent auditor appointed by the Controller shall be entitled to carry out audits and inspections at any time during the term of the Agreement at the facilities of the Processor and its sub-processors -in accordance with the Agreement. Any audit of the Processor shall be limited to assessing compliance with the obligations under the Agreement and shall not cover access to any data of other Controllers or data relating to the use of the Processor's security measures. When carrying out an inspection or audit, the Processor shall create reasonable conditions and provide reasonable cooperation without delay. If the inspection or audit is carried out by the Controller or a person authorised by the Controller, the Controller shall notify the Processor in writing of the date of the inspection or audit at least two days in advance.

6.7. **[Security Incident]** The Processor is obliged to prevent a Personal Data breach. In the event of a breach of security measures leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Personal Data (the **Security Incident**), the Processor is obliged to inform the Controller of the Security Incident **without delay (within 48 hours at the latest)** of becoming aware of the Security Incident.

6.8. **[Security Incident Notification]** The Personal Data Breach Notification shall include at least **(i)** a description of the nature of the Security Incident, including the categories and approximate number of the Data Subject and the categories and approximate number of affected Personal Data Records, as well as **(ii)** a description of the likely consequences of the Personal Data Breach, and **(iii)** a description of the measures taken to address the Security Incident and to mitigate the potential negative effects of the Personal Data Breach. If, as a result of the Security Incident, there is also a threatened breach of the Agreement on the part of the Processor, the notification shall also include **(iv)** information about such breach. If it is not possible to provide all of this information at the same time, it may also be provided gradually without undue delay.

6.9. **[Security Incident Documentation]** The Processor is obliged to document all security incidents and to make this documentation available to the Controller upon request.

6.10. **[Security Incident Resolution]** Upon becoming aware of a Security Incident, the Processor is obliged to take the necessary and appropriate steps to ensure the protection of Personal Data and to limit any possible negative impact on Data Subjects. The Processor shall cooperate with the Controller in responding to identified Security Incidents.

6.11. **[Sub-processors]** The Processor shall be entitled to use the persons listed in **Annex 2** of the Agreement as sub-processors for the processing of the Personal Data of the Data Subjects under the Agreement. The Processor shall be entitled to use other persons only on the basis of the prior specific, written permission of the Controller. The Processor shall make available to the Controller an up-to-date list of sub-processors (in Annex 2 of the Agreement), which includes the names and locations of the sub-processors -as well as the scope of services provided to the Processor. The Controller agrees to use the listed sub-processors -for the above scope of services.

6.12. **[Setting up relationships with sub-processors]** The Processor is obliged to regularly monitor the activities of sub-processors -and is responsible for the processing of Personal Data by sub-processors -in the same way as if it were processing the data directly. The Processor shall also be obliged to -enter into a agreement -with the Sub-processors -imposing on them the same or stricter obligations to protect Personal Data as it has under the Agreement. The Processor shall be responsible for ensuring that **(i)** each sub-processor undertakes in writing to comply with the obligation of confidentiality or is subject to a legal obligation of confidentiality and **(ii)** each sub-processor properly fulfils its obligations in relation to the protection of Personal Data.

ARTICLE 7: LIABILITY OF THE PROCESSOR AND PENALTIES

7.1. **[Indemnification and Damages]** The Processor shall be liable for damages suffered by the Controller or the Data Subject if **(i)** it has failed to perform its obligations under the Agreement, **(ii)** it has failed to comply with the obligations specifically set out for the Processor by the Data Protection Regulations or other generally applicable law, or **(iii)** it has acted in excess of or in contravention of the Controller's instructions under the Agreement. In the event of harm or loss, the Processor undertakes to indemnify the Controller or the Data Subject for the damage or repair non-pecuniary injury by way of appropriate compensation, immediately upon the Controller's request, but no later than within 10 working days after receipt of the request.

7.2. **[Contractual Penalty]** If the Processor breaches any of its obligations under Article 4, Article 5, Article 6 and Article 8 of the Agreement, the Controller shall be entitled to a contractual penalty of EUR 5,000 for each individual breach of any of these obligations (separately). The Processor shall pay the contractual penalty within 3 days after receipt of the Controller's call for payment. The payment of the contractual penalty shall be without prejudice to the right of the Controller to claim from the Processor compensation for damages or non-pecuniary loss, even in an amount in excess of the agreed contractual penalty.

ARTICLE 8: CONFIDENTIALITY

8.1. The processing of the Personal Data is confidential. The Parties are obliged to maintain the confidentiality of all confidential information provided to them or otherwise obtained in connection with the Agreement or with which they have become acquainted during the performance of the Agreement, or which is related to the subject matter of the Agreement, even after the termination of the Agreement, except in the following cases:

a) where the provision of the information is required of the Party concerned by law;

b) if the information is publicly available for any reason other than a breach of the obligation of confidentiality by the party concerned;

c) if it is information that becomes public knowledge after the signature of the Agreement or that can be obtained from means of information generally available after that date;

d) where the information is provided by professional advisers to the Party concerned (including legal, accounting, tax and other advisers) who are either bound by a general professional duty of confidentiality or who have undertaken a duty of confidentiality to the Party concerned;

e) if the information is required for the purposes of any judicial, arbitration, administrative or other proceeding to which the Party concerned is a party;

f) if the information is provided with the consent of the other Party.

8.2. The Parties undertake not to use for themselves or for third parties, disclose to third parties or allow third parties access to confidential information without the prior written consent of the other Party. Third parties shall not be deemed to be members of the Parties' bodies, auditors or legal advisers of the Parties who are bound by a duty of confidentiality under generally applicable law in respect of the information disclosed to them.

ARTICLE 9: COMMUNICATION

9.1. **[Methods of Communication]** Unless otherwise specified in the Agreement, any notices, requests and other documents or information addressed to the other Party or required by the Agreement and any other communication between the Parties shall be in the Slovak language and shall be delivered to the other Party by one of the following methods

a) by email to the address of the other party set out in the Agreement (with a request for notification of delivery if possible);

b) by registered mail with acknowledgement of receipt;

c) by a courier service that allows delivery verification.

9.2. **[Delivery]** A message sent in the above manner shall be deemed to have been delivered to the other Party who is the recipient:

a) in the case of delivery by email, the date of receipt of confirmation of successful delivery of the email message (or equivalent proof) or, if the message was not sent with a request for notification of delivery, the day after the message was sent;

b) in the case of delivery by post, on the date of receipt of the message; if the addressee Party fails or refuses to accept the message or is otherwise unable to receive the message, the message shall be deemed to have been delivered on the expiry of the tenth working day following the date of dispatch of the message;

c) in the case of delivery by courier service, on the date of receipt of the message; if the addressee party fails or refuses to accept the message or is otherwise unable to receive the message, the message shall be deemed to have been delivered on the expiry of the tenth working day after the message has been handed over to the courier service.

ARTICLE 10: FINAL PROVISIONS

10.1. **[Validity and Effectiveness]** The Agreement shall enter into force and effect on the date of its signing by all Parties (or the last of them); if the legislation provides for mandatory publication of the Agreement, the Agreement shall be

effective on the day following the date of its publication in the Central Register of Contracts maintained by the Government Office of the Slovak Republic.

10.2. **[Duration of Agreement]** The Agreement shall be concluded for the period of processing of the Personal Data by the Processor pursuant to the provisions of Article 3, paragraph 3.6 of the Agreement and shall terminate upon fulfilment of the obligation of the Processor referred to in Article 4, paragraph 4.8 of the Agreement. The Controller shall terminate the Agreement under the condition stipulated in Article 6 paragraph 6.6 of the Agreement.

10.3. **[Annexes]** Annexes are an integral part of the Agreement:

Annex 1: Technical and organisational measures to ensure the protection of Personal Data;

Annex 2: Transfers and list of other intermediaries.

10.4. **[Waiver and Severability]** A waiver of a breach of any obligation under the Agreement by either Party shall not constitute or be construed as a waiver of a right arising from a subsequent breach of that obligation, nor a waiver of a right arising from a breach of any other obligation under the Agreement. Failure to exercise any right, and delay in exercising any right, shall not constitute a waiver of the right nor shall it be construed as such. If any provision of the Agreement is or hereafter becomes invalid, ineffective or unenforceable, the other provisions of the Agreement shall not be affected thereby and shall remain valid, effective and enforceable to the fullest extent of the law. The Parties hereby undertake to replace the invalid, ineffective or unenforceable provisions with new provisions which are as close in meaning as possible to the meaning of the provisions which have become invalid, ineffective or unenforceable.

10.5. **[Language and Counterparts]** The Agreement shall be drawn up and signed in the English language, in two (2) counterparts, with each Party retaining one (1) of the counterparts.

10.6. **[Amendment of the Agreement]** The Agreement may be amended or supplemented only by written amendments signed by both Parties.

10.7. **[Governing Law]** The Agreement and its interpretation shall be governed by the laws of the Slovak Republic and the applicable laws of the European Union and shall be interpreted in particular in accordance with the GDPR or the Data Protection Act. The same rules shall also apply to annexes and amendments to the Agreement and all non-contractual obligations related to or arising from the Agreement.

10.8. **[Dispute Resolution]** The Parties agree that any disputes arising out of the Agreement, including disputes concerning its validity, interpretation or termination, shall be resolved amicably and in good faith as a matter of priority. Disputes between the Parties that are not settled pursuant to the preceding sentence shall be finally resolved in a court of competent jurisdiction in the Slovak Republic.

10.9. **[Substitution of Prior Agreements]** The Agreement, with all of its provisions and attachments, constitutes the entire agreement of the Parties with respect to the subject matter of the Agreement and supersedes all prior negotiations and written or oral agreements between the Parties with respect to the subject matter of the Agreement.

10.10. **[Final Declarations]** The Parties jointly declare that they have all the necessary professional experience, expertise and resources to perform the Agreement and that their financial situation enables them to undertake in good faith the obligations set out in the Agreement. The Parties also jointly declare that they have read the text of the Agreement, that they have fully understood its contents, that it is sufficiently definite for them and expresses their free and serious will, free from any mistake, and that they do not enter into it under duress or on terms manifestly unfavourable to either of them, in witness whereof they attach their handwritten signature.

SIGNATURES OF PARTIES

In [·], on [·]

For the Controller

For the Processor

_____

Jaromír Hanzal, Director

_____

Ing. Mário Lelovský, President of the Bureau

ANNEX 1: TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE PROTECTION OF PERSONAL DATA

TECHNICAL MEASURES

Technical measures implemented by means of a physical nature		
Securing the building by means of mechanical barriers (e.g. lockable doors, windows, grilles) and, if necessary, by means of technical security devices (e.g. electrical security system of the building, electrical fire alarm system)	▣ Yes	□ No
Securing the protected area by separating it from other parts of the building (e.g. walls, barriers in the form of partitions, grilles or glazing)	▣ Yes	□ No
Location of the Information System in a protected area (protection of the Information System from physical access of unauthorised persons and adverse environmental influences)	▣ Yes	□ No
Secure storage of physical media of personal data (e.g. storage of paper documents in lockable cabinets or safes)	▣ Yes	□ No
Preventing accidental removal of personal data from Information System displays (e.g. appropriate placement of displays)	▣ Yes	□ No
Equipment for the destruction of physical media with personal data (e.g. document shredding equipment)	▣ Yes	□ No

Protection against unauthorised access		
Encryption protection of the contents of data media and encryption protection of data moved over computer networks	▣ Yes	□ No
Rules for third party access to the Information System, if any	▣ Yes	□ No

Access Control for Authorised Persons		
Identification, authentication and authorisation of Authorized Persons in the information system	▣ Yes	□ No
Recording of individual Authorised Persons' entries into the Information System	▣ Yes	□ No

Protection against malicious code		
Detecting the presence of malicious code in incoming electronic mail and other files received from a publicly accessible computer network or from data storage media	▣ Yes	□ No
Protection against unsolicited e-mail	▣ Yes	□ No
Use of legal and Controller-approved software	▣ Yes	□ No
Rules for downloading files from a publicly accessible computer network	▣ Yes	□ No

Network security		
Control, restrict or prevent the connection of the Information System in which the Personal Data is Processed to a publicly accessible computer network	▣ Yes	□ No

Records of all network interconnection points, including the publicly accessible computer network	▣ **Yes, partially** (basic network architecture is developed)	□ **No**
Protecting the external and internal environment with a network security tool (e.g. firewall)	▣ **Yes**	□ **No**
Rules on access to a publicly accessible computer network (e.g. preventing access to certain websites)	▣ **Yes**	□ **No**
Protection against other threats originating from a publicly accessible computer network (e.g. a hacker attack)	▣ **Yes**	□ **No**

Backup		
Backup data carrier functionality test	▣ **Yes (IT Consultant)**	□ **No**
Creating backups with a pre-selected periodicity	▣ **Yes (IT Consultant)**	□ **No**
Information system recovery test from backup	▣ **Yes (IT Consultant)**	□ **No**
Secure storage of backups	▣ **Yes**	□ **No**

Disposal of personal data and data carriers and updating of software		
Secure deletion of personal data from data carriers	▣ **Yes**	□ **No**
Equipment for the destruction of data carriers of personal data	▣ **Yes**	□ **No**
Updating the operating system and application software	▣ **Yes**	□ **No**

ORGANISATIONAL MEASURES

Personnel measures		
Written instructions to Authorised Persons before the first processing operation with personal data is carried out	▣ **Yes**	□ **No**
Instructions on the rights and obligations stipulated in the GDPR, internal policies and rules of the Controller	▣ **Yes**	□ **No**
Definition of the personal data to which a particular Authorised Person is to have access for the purpose of performing his or her duties or tasks	▣ **Yes**	□ **No**
Determination of the procedures that the Authorised Person is required to apply when Processing the Personal Data	▣ **Yes**	□ **No**
Definition of prohibited practices or operations with personal data	▣ **Yes**	□ **No**
Definition of liability for breaches of the GDPR and this GDPR Compliance Project or its binding parts for Authorised Persons (Internal Policies)	▣ **Yes**	□ **No**
Instructions to Authorised Persons on the procedures associated with automated means of processing and the related rights and obligations (on and off the controller's premises)	▣ **Yes**	□ **No**
Appointment of the Data Protection Officer (DPO) to an independent supervisory role within the Company's organisational structure	▣ **Yes**	□ **No**
Familiarisation of Authorised Persons with the adopted internal policies on the protection of personal data	▣ **Yes**	□ **No**
Training of Authorised Persons (e.g. legal, IT, cybersecurity, internal privacy policy)	▣ **Yes**	□ **No**
Procedure for termination of the employment or similar relationship of the Authorised Person (e.g. handing over	▣ **Yes**	□ **No**

the assigned assets, cancellation of access rights, instruction on the consequences of breach of the legal or contractual obligation of confidentiality)		
Maintaining and updating the list of assets	▣ **Yes**	□ **No**

Control of Access of Authorised Persons to Personal Data		
Control of access to the premises and the Controller's protected areas (e.g. through technical and personnel measures)	▣ **Yes**	□ **No**
Management of keys (individual key allocation, secure storage of spare keys)	▣ **Yes**	□ **No**
Assignment of access rights and access levels (roles) of Authorised Persons	▣ **Yes**	□ **No**
Password management	▣ **Yes**	□ **No**
Mutual representation of Authorised Persons (e.g. in the event of an accident, temporary incapacity for work, termination of employment or similar relationship)	▣ **Yes**	□ **No**

Organisation of Personal Data Processing		
Rules for Processing Personal Data in a Protected Area	▣ **Yes**	□ **No**
Continuous presence of an Authorised Person in the Protected Area if there are other than Authorised Persons in the Protected Area	▣ **Yes**	□ **No**
Maintenance and cleaning regime for protected areas	▣ **Yes**	□ **No**
Rules on Processing of Personal Data outside the protected Area, if such processing is foreseen	▣ **Yes**	□ **No**
Rules on handling physical media of personal data (e.g. documents, photographs) outside secure areas and definition of liability	▣ **Yes**	□ **No**
Rules on use of automated means of processing (e.g. laptops) outside protected areas and definition of responsibilities	▣ **Yes**	□ **No**
Rules on the use of portable data carriers outside protected premises and definition of liability	▣ **Yes**	□ **No**
Setting forth procedures for the disposal of personal data with the definition of the related responsibilities of individual Authorised Persons (secure deletion of personal data from data carriers, disposal of data carriers and physical carriers with personal data)	▣ **Yes**	□ **No**
Procedure for reporting security incidents and identified vulnerabilities of the Information System for the purpose of timely preventive or corrective action	▣ **Yes**	□ **No**
Recording Security Incidents and applied solutions	▣ **Yes**	□ **No**
Procedure for dealing with individual types of Security Incidents	▣ **Yes**	□ **No**
Identification, recording and remediation of Security Incidents	▣ **Yes**	□ **No**
Modification of the reporting of Security Incidents in relation to the Supervisory Authority and in relation to the data subjects	▣ **Yes**	□ **No**
Procedures for accidents, malfunctions, and other emergencies	▣ **Yes**	□ **No**
Procedure for the malfunction, maintenance or repair of automated means of processing (e.g. protection of	▣ **Yes**	□ **No**

personal data on the hard drive of the computer being repaired)		

Control activity		
Control activities of the controller aimed at compliance with the adopted security measures, specifying the manner, form and periodicity of its implementation (e.g. regular checks of access to the Information System)	▣ **Yes**	□ **No**
Informing Authorised Persons about the control mechanism, if implemented by the controller (scope of the control and methods of its implementation)	▣ **Yes**	□ **No**

ANNEX 2: LIST OF OTHER INTERMEDIARIES AND BENEFICIARIES

List of other intermediaries				
Name	Business ID No.	Registered seat	Services rendered	Country
Pragmatic Mates s.r.o.	46 706 291	Hodvábna 1291/1	Management of IT platform	Slovakia

At the time of signing of this Agreement, if the Processor doesn't use services of any other intermediaries, Annex 2 shall remain empty.