

INTERMEDIARY AGREEMENT

concluded pursuant to Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, in conjunction with § 34 of Act No. 18/2018 Coll. on Personal Data

Protection (hereinafter referred to as the “**Agreement**”)

between:

Controller:

Business name:

Registered office:

BIN:

Represented by:

(hereinafter referred to as the “**Controller**”)

and

Intermediary:

Business name: **Emineo Partners – accounting services, s. r. o.**

Registered office: Hviezdoslavovo námestie 7, 811 02 Bratislava – mestská časť Staré mesto

BIN: 51 925 001

Zapísaná v Obchodnom registri Mestského súdu Bratislava III, Oddiel: Sro, Vložka č.: 132137/B

Represented by: **Ing. Marcel Muráni**, Managing Director

(hereinafter referred to as the “**Intermediary**”)

(Controller and Intermediary hereinafter collectively referred to as the “**Contracting Parties**”)

Article 1

Introductory Provisions

1.1 For the purposes of this Agreement, the terms capitalized herein shall have the following meanings:

Applicable personal data protection legislation includes:

- a) 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, repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter “GDPR”),
- b) Act No. 18/2018 Coll. on the Protection of Personal Data, as amended, and
- c) all laws and regulations establishing rules for the protection of data subjects in connection with the processing of personal data.

Standard Contractual Clauses are the standard contractual clauses pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.

EEA means the European Economic Area, including all member states of the European Union, Norway, Iceland, and Liechtenstein.

High Risk means a situation where processing, particularly using new technologies, considering the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

Third Country means any country outside the EEA which is presumed not to ensure an adequate level of protection of personal data under applicable law.

Personal Data means any information relating to an identified or identifiable natural person (hereinafter “Data Subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.

Processing means any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Sub-processor means any third party processing Personal Data on behalf of or under the instructions of the Intermediary.

Third Party means any entity other than the Contracting Parties.

Article 2 **Subject Matter of the Agreement**

- 2.1 The subject matter of this Agreement is to regulate the rights and obligations of the Contracting Parties regarding the processing of Personal Data by the Intermediary on behalf of the Controller. The processing of Personal Data is carried out pursuant to the **Agreement on the Provision of Accounting and Payroll Services** dated (hereinafter the “Service Agreement”).
- 2.2 The nature and purpose of the Processing, the duration of the Processing, the type of Personal Data, the categories of Data Subjects, and the instructions regarding the Processing of Personal Data are set out in **Annex No. 1** to this Agreement. The intention of the Contracting Parties in defining the conditions of Processing is to take into account the nature and content of the Service Agreement in a manner that ensures the lawfulness of the Processing of Personal Data while enabling proper performance of the Service Agreement. The Intermediary is obliged, in the course of Processing Personal Data, to comply with the restrictions arising from the agreed conditions of Processing and from other provisions of this Agreement.

- 2.3 The Intermediary shall process Personal Data solely for the purposes specified in **Annex No. 1** to this Agreement. The Intermediary shall not use Personal Data for any other purpose. For the avoidance of any doubt, the Intermediary expressly acknowledges that it is not entitled, in relation to Personal Data, to determine the purposes and/or means of their Processing and is not authorized to process Personal Data beyond the scope defined in this Agreement. The Intermediary expressly acknowledges that, in the event of a breach of this provision, it shall be considered a Controller of Personal Data with all attendant obligations, in particular those arising from the GDPR.
- 2.4 The date on which the Intermediary is entitled to process Personal Data on behalf of the Controller under the terms of this Agreement shall coincide with the effective date of the Service Agreement.

Article 3 Rights and Obligations of the Intermediary

- 3.1 The Intermediary shall process Personal Data only on the instructions of the Controller, including with respect to transfers of Personal Data to a third country or to an international organization.
- 3.2 The Intermediary shall ensure that appropriate documentation is maintained for the processing of Personal Data in accordance with applicable law.
- 3.3 The Intermediary shall ensure that persons handling Personal Data are adequately instructed. Furthermore, the Intermediary shall bind such persons in an appropriate manner, in connection with the performance of this Agreement, to maintain the confidentiality of information obtained and to keep secret any facts they become aware of.
- 3.4 The Intermediary shall implement technical measures to secure the Personal Data obtained, in order to prevent intentional or negligent misuse, theft, loss, or alteration of the Personal Data it processes.
- 3.5 Should the Intermediary identify any impropriety in the operations performed or instructions of the Controller regarding the processing of Personal Data, or any other breach of the GDPR or applicable personal data protection legislation, it shall immediately inform the Controller.
- 3.6 In the event of a Personal Data breach, the Intermediary shall immediately notify the Controller of the nature and scope of the breach.
- 3.7 Upon request of the Controller, the Intermediary shall provide the requested Personal Data processed under this Agreement.
- 3.8 The Intermediary shall comply with additional instructions of the Controller not explicitly set out in this Agreement but relating to the processing of Personal Data. This includes, for example, erasure of Personal Data following a request from a Data Subject, correction of Personal Data following a request from a Data Subject, or other forms of cooperation aimed at addressing a request, proposal, or notification from a Data Subject exercising any of their rights under the GDPR.
- 3.9 The Intermediary shall provide the Controller with information necessary to demonstrate compliance with its obligations and shall cooperate in audits of data protection and, upon request, in inspections conducted by the Controller.
- 3.10 In the course of processing Personal Data, the Intermediary shall comply with all applicable personal data protection legislation and other generally binding legal regulations.

- 3.11 Each Contracting Party shall address justified requests from the other Contracting Party for assistance to ensure compliance with applicable data protection legislation in the course of Processing.

Article 4 Security

- 4.1 The Intermediary declares that, taking into account the latest knowledge, the costs of implementing measures, and the nature, scope, context, and purposes of the Processing, as well as the risks that the Processing may pose to the rights of natural persons, it has implemented appropriate technical, personnel, organizational, and security measures to protect Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorized disclosure, access, storage, or transmission, and against all other forms of unlawful Processing, including unnecessary collection or further Processing of Personal Data. These measures shall ensure an appropriate level of protection of Personal Data. The Intermediary further undertakes to regularly test, assess, and evaluate these security measures.
- 4.2 The Intermediary declares that the security measures under clause 4.1 of this Agreement include measures in accordance with Article 32 of the GDPR.

Article 5 Confidentiality of Information and Duty of Secrecy

- 5.1 The Intermediary shall maintain confidentiality regarding Personal Data obtained from the Controller with which it comes into contact; it shall not use such data for its own purposes, nor disclose, provide, or make them available to any third party without the prior written consent of the Controller, except where disclosure or provision is necessary to ensure the Processing of Personal Data under this Agreement or where the obligation to provide and/or make Personal Data available arises from specific legal provisions or by decision of a public authority. This duty of confidentiality shall continue even after the termination of the mandate.
- 5.2 The Intermediary undertakes to allow access to Personal Data obtained from the Controller only to authorized persons (employees, representatives, or any other person working on behalf of or under the instructions or supervision of the Intermediary), and solely to the extent necessary to ensure the Processing of Personal Data. The Intermediary shall instruct authorized persons who have access to Personal Data regarding their rights and obligations under applicable data protection legislation, including the duty to maintain confidentiality and comply with data security rules.
- 5.3 In the event of lawful provision of Personal Data in accordance with clause 5.1 above, except where applicable data protection legislation provides otherwise, the Intermediary shall maintain a record of any such provision for the entire duration of this Agreement. Such a record shall include at a minimum the following information:
- a) name/title and address of the Third Party to whom the Personal Data were provided,
 - b) categories of Personal Data provided,
 - c) date and time of provision of the Personal Data, and
 - d) purpose of the provision.

Article 6
Sub-processors

- 6.1 The Intermediary is entitled, for the purpose of fulfilling this Agreement as well as the Service Agreement, to engage a Sub-processor, for which the Controller grants the Intermediary a general written authorization. In the event a Sub-processor is engaged in processing operations, the Intermediary declares that the Sub-processor meets the criteria under **Article 28(3) GDPR**, and has implemented all technical, personnel, and organizational measures necessary for the processing of Personal Data.
- 6.2 If the Intermediary engages a Sub-processor to perform specific processing activities on behalf of the Controller, the Intermediary shall impose on such Sub-processor the same data protection obligations as set out in this Agreement.
- 6.3 If such Sub-processor fails to fulfill its data protection obligations, the Intermediary remains fully liable to the Controller for the performance of the Sub-processor's obligations.

Article 7
Audit and Compliance Assurance

- 7.1 The Intermediary shall make its processing systems, facilities, and supporting documentation available for inspection or audit by the Controller or a Third Party (auditor) appointed by the Controller, and shall provide any assistance reasonably requested by the Controller for the purpose of conducting the audit. If the audit demonstrates that the Intermediary has breached any obligation under this Agreement, the Intermediary shall immediately remedy such breach and reimburse the Controller for all reasonable costs incurred in connection with the audit. If the audit does not demonstrate that the Intermediary has breached its obligations under this Agreement, the costs of the audit shall be borne by the Controller.
- 7.2 The Controller shall:
- a) provide the Intermediary with reasonable notice of the intended audit under clause 7.1 above,
 - b) ensure that its representatives and appointed persons performing the audit comply with reasonable confidentiality, security, and health regulations of the Intermediary as communicated to the Controller, and
 - c) ensure that its representatives and appointed persons performing the audit exercise reasonable efforts to minimize any disruption to the Intermediary's business resulting from the audit.

Article 8
Inspection or Audit by Public Authorities

- 8.1 The Intermediary shall submit its relevant processing systems, facilities, and supporting documentation to inspection or audit related to Processing conducted by a competent public authority, where required to fulfill the legal obligations of the Controller. In any such inspection or audit, each Contracting Party shall provide all reasonable assistance to the other Contracting Party in responding to such inspection or audit. If a competent public authority considers the Processing under this Agreement to be unlawful, the Contracting Parties shall immediately take measures to ensure future compliance with applicable data protection legislation and other relevant laws and regulations.

Article 9
Data Protection Impact Assessment

- 9.1 Where necessary, the Intermediary shall assist the Controller in carrying out a Data Protection Impact Assessment regarding the processing activities under the contractual documentation referred to in clause 2.1 of this Agreement. In addition, the Intermediary shall perform a review to assess whether the Processing is conducted in accordance with the Data Protection Impact Assessment, at least whenever there is a change in the risk posed by the processing activities.
- 9.2 If the results of the Data Protection Impact Assessment indicate that a processing activity would result in High Risk Processing or would trigger the Controller's obligation to consult the relevant supervisory authority, the Intermediary shall:
- a) provide the Controller with sufficient time to consult the relevant supervisory authority before carrying out such processing activities; or
 - b) suspend its processing activities for a sufficient period to allow consultation with the relevant supervisory authority before initiating or resuming the processing activities.

Article 10
Notifications of Provision and Personal Data Breaches

- 10.1 The Intermediary shall, without undue delay and no later than twenty-four (24) hours, notify the Controller if:
- a) it receives an order, summons, or request for inspection or audit from a competent public authority regarding Processing, except where such notification is prohibited by law;
 - b) it intends to provide Personal Data to any public authority; or
 - c) it becomes aware or reasonably suspects that a Personal Data Breach has occurred.
- 10.2 In the event of a Personal Data Breach, the Intermediary shall immediately take appropriate remedial measures. Furthermore, the Intermediary shall, without undue delay, provide the Controller with all relevant information concerning the Personal Data Breach requested by the Controller. The Intermediary shall fully cooperate with the Controller to promptly address the Personal Data Breach and, at the Controller's request, shall assist as necessary in appropriately notifying the Data Subjects.

Article 11
Complaints, Requests, Inquiries, and Data Subject Rights

- 11.1 The Intermediary shall, without undue delay, inform the Controller of any complaints, requests, or inquiries from Data Subjects, including the exercise of rights such as the right of access, the right to erasure, the right to restriction of Processing, the right to data portability, the right to object, and any other rights of the Data Subject under applicable data protection legislation.
- 11.2 The Intermediary shall not respond to any complaints, requests, or inquiries from Data Subjects without the prior written consent of the Controller, except where required by applicable law. Upon receiving a complaint, request, or inquiry from a Data Subject, the Intermediary shall, at its discretion, either make reasonable efforts to refer the Data Subject to the Controller or forward the complaint, request, or inquiry to the Controller within five (5) days of receipt.

Article 12
Return of Data to the Controller and Data Destruction

- 12.1 All Personal Data shall be returned to the Controller upon its first request. The Intermediary shall not retain Personal Data longer than necessary for the purposes of fulfilling its obligations under this Agreement.

- 12.2 Immediately upon termination of the contractual relationship by decision of the Controller, the Intermediary shall either:
- a) return to the Controller all documents containing Personal Data provided to the Intermediary, or
 - b) destroy such Personal Data and any copies thereof, except where this Agreement or applicable law provides otherwise.
- 12.3 The Controller may require the Intermediary to confirm, without undue delay and no later than twenty-four (24) hours, that all copies of Personal Data have been returned and/or destroyed. Upon the Controller's request, the Intermediary shall allow its processing facilities to be audited to verify compliance with the obligations under this Article 12.

Article 13 Indemnification

- 13.1 The Intermediary shall indemnify the Controller for any damage demonstrably suffered in connection with claims, proceedings, or lawsuits brought by public authorities or Data Subjects against the Processing of Personal Data by the Intermediary and/or any Sub-processors, or in connection with such Processing, as well as for any claims, proceedings, or lawsuits initiated against the Controller arising from any breach of data protection obligations by the Intermediary and/or any Sub-processors, provided that such breach does not result from the Intermediary having followed the instructions of the Controller.

Article 14 Transfer of Personal Data to a Third Country

- 14.1 The Intermediary shall not transfer Personal Data to a Third Country nor make any Personal Data accessible from such a country (e.g., for support services) without the prior written consent of the Controller.
- 14.2 Any transfer of Personal Data outside the EEA by the Intermediary or any Sub-processor to a Third Country shall be governed by the terms of the **Standard Contractual Clauses**. The Intermediary shall demonstrate compliance with the conditions for the transfer of Personal Data outside the EEA under applicable law to the Controller, i.e., by submitting the Standard Contractual Clauses together with a request for consent to such transfer.
- 14.3 Should the Court of Justice of the European Union invalidate the Standard Contractual Clauses or the European Commission replace the Clauses with a new protective or subsequent set of Standard Contractual Clauses during the term of this Agreement, the Controller and the Intermediary shall, without undue delay, enter into good faith negotiations upon the Controller's written request to implement such Standard Contractual Clauses or introduce an alternative data transfer mechanism in accordance with applicable data protection legislation.

Article 15 Cooperation

- 15.1 The Intermediary shall provide the Controller with cooperation to ensure compliance with applicable data protection legislation, taking into account the nature of the Processing and the information available to the Intermediary.
- 15.2 The Intermediary shall immediately notify the Controller if, in its opinion, any instruction or instructions from the Controller result in a breach of applicable data protection legislation or other generally binding legal regulations.

15.3 All notices, confirmations, and other statements exchanged by the Contracting Parties in connection with this Agreement shall be in writing and sent by email to **office@emineopartners.sk**, or delivered in hard copy to the Controller's registered office, addressed to the Data Protection Officer of the Controller.

Article 16 Term of the Agreement

16.1 This Agreement is concluded for a fixed term, corresponding to the duration of the contractual relationship between the Controller and the Intermediary under clause 2.1, Article 2 of this Agreement.

Article 17 Final Provisions

17.1 The Controller shall, annually or as circumstances require, review the Processing of Personal Data under this Agreement. The Intermediary shall provide the Controller with cooperation in amending this Agreement to ensure compliance with applicable data protection legislation.

17.2 This Agreement shall enter into force and become effective on the date of its signature by both Contracting Parties.

17.3 This Agreement constitutes the entire agreement between the Contracting Parties in relation to its subject matter (data protection).

17.4 If any provision of this Agreement is found to be invalid or unenforceable for any reason, such invalid or unenforceable provisions shall be deemed severable from the remaining provisions, which shall remain in full force and effect between the Contracting Parties.

17.5 This Agreement may only be amended in writing and upon agreement of both Contracting Parties by written addenda to this Agreement. Any changes made in another form shall be invalid and non-binding on the Contracting Parties.

17.6 Rights and obligations not expressly governed by this Agreement shall be governed by the provisions of applicable data protection legislation, Act No. 513/1991 Coll., Commercial Code, as amended, and subsidiarily by the provisions of Act No. 40/1964 Coll., Civil Code, as amended, as well as other laws applicable in the Slovak Republic.

17.7 This Agreement is executed in two originals, with each Contracting Party receiving one original.

17.8 The Contracting Parties declare that they have read this Agreement thoroughly, that it was not concluded under duress or on otherwise unilaterally disadvantageous terms. In witness whereof, the Parties execute this Agreement by their signatures.

In Bratislava, on

For the Intermediary:

For the Controller:

Emineo Partners – accounting services s. r. o.
Ing. Marcel Muráni
Managing Director

Annex 1**Conditions for the Processing of Personal Data**

Nature and Purpose of Processing:	Performance of the Agreement on the provision of services.
Duration of Processing:	For the duration of the validity of the Agreement on the provision of services dated, but not longer than is strictly necessary to achieve the purpose of processing.
Types of Personal Data:	Name, surname, title, maiden name, permanent residence address and correspondence address – street, postal code, city, email, telephone contact, personal identification number, date and place of birth, type and number of identity document, nationality, citizenship, marital status, information about the employee’s children, bank account number, information contained in the employee’s payslip or payroll, including details of employment and individual wage components, and information about health status.
Categories of Data Subjects:	Employees and former employees of the Controller.
Instructions regarding Processing:	None were issued.