**Data Processing Supplemental Agreement**

*Agreement name*: [*insert, including references to any amendments*]

[*Agreement Number*: [*insert*]]

*Supplier*: [*insert full legal name*]

This Supplemental Agreement to the above referenced agreement ("**Agreement**") is made by and between **XX** (registered office: XX, registration court and court number: Municipal Court of Budapest, acting as Court of Registration XX) acting in the name and on behalf XX (registered office: XX, registration court and court number: Companies Registration Office, no. XX) an entity registered in XX (“**Customer**”) and the above referenced Supplier ("**Supplier**") (together, the “**Parties**”).

WHEREAS, Customer and Supplier have previously entered into the aforesaid Agreement;

WHEREAS, the purpose of this Supplemental Agreement is to set out data processing terms relating to the processing activities under the Agreement as indicated below;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Customer and Supplier hereby agree to supplement the Agreement as follows:

**Definitions**

Except where the context requires otherwise, references in this Supplemental Agreement to the Agreement are to the Agreement including this Addendum.

**Effective date**

The effective date of this Supplemental Agreement is [*insert*] ("**Supplemental Agreement Effective Date**").

**Data processor terms**

The Parties agree that the Appendix (Confidentiality, Personal Data and Information Security Terms) of this Supplemental Agreement (and any Annexes to that Appendix) ("**Supplemental Agreement Appendix**") applies to the Supplier’s processing of European Personal Data (as defined in the Supplemental Agreement Appendix) under the Agreement.

**General**

* 1. The provisions of this Supplemental Agreement that, by their nature and content, must survive the completion, rescission, termination or expiration of the Agreement and the Supplemental Agreement in order to achieve the fundamental hereof shall so survive and shall continue to bind the Parties.
  2. Other sections and paragraphs of the Agreement remain unchanged and valid.

**IN WITNESS WHEREOF,** the Parties hereto, through their duly authorised officers, have executed this Supplemental Agreement as of the Addendum Effective Date.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **[*Supplier entity*]:** | |  | ***XX*:** | |
| By: |  |  | By: |  |
| Name: |  |  | Name: |  |
| Title: |  |  | Title: |  |
| Date: |  |  | Date: |  |

Appendix

**APPENDIX**

**CONFIDENTIAL INFORMATION, PERSONAL DATA AND INFORMATION SECURITY TERMS**

1. **DEFINITIONS**

“**Acceptance Criteria**” means the criteria by which Deliverables and Services will be evaluated by Customer, which (for Software Deliverables) shall include criteria to determine compliance with the Specifications set forth in the applicable Documentation, together with such other test data, test conditions, descriptions and exception conditions as may be set out in any work order or statement of work or similar under the Agreement;

“**Affiliate**” means in relation to Customer (or Supplier) any entity that from time to time directly or indirectly Controls, is Controlled by, or is under common Control with Customer (or Supplier);

“**Applicable Law**” means country laws, state and federal laws, European directives, rules, regulations, executive orders, regulatory guidance, regulatory requirements (including standard contractual clauses) and any form of secondary legislation, resolution, policy guideline, concession or case law from time to time that apply to Customer, Customer’s Affiliates, Supplier or Supplier’s Affiliates (as a service provider to Customer or Customer’s Affiliates) or the Services, including (i) Data Protection Laws (ii) any bribery, fraud, kickback, or other similar anti-corruption law or regulation of any relevant country including the US Foreign Corrupt Practices Act 1977, (iii) laws or regulations addressing unfair, deceptive or abusive acts or practices, (iv) laws or regulations addressing money laundering and (v) laws or regulations related to economic sanctions;

“**Associated Person**” means in relation to any entity, a person who (by reference to all the relevant circumstances) performs services for and on behalf of that entity in any capacity; for example, employees, agents, subsidiaries, representatives and subcontractors.

“**XX Standards for Suppliers**” means an overview of Customer’s key policy requirements with which suppliers must comply, which is available via the link set out in Annex 2 of this Addendum Appendix;

“**Confidential Information**” of either Party means all data, information, and material relating to the business, customers, internal policies, systems or affairs of that Party, its representatives or its customers that is or has been: (i) disclosed by that Party to the other Party under or in connection with the Agreement, whether orally, electronically, in writing or otherwise, including copies of such information; or (ii) learnt, observed, acquired or generated by the other Party in connection with the Agreement.

The following shall be Customer’s Confidential Information: (a) the terms of the Agreement; (b) any Customer Personal Data acquired or generated by or on behalf of Supplier and/or any Supplier Affiliate; and (c) Work Products.

“**Control**” of an entity means the ownership of, or the power to vote, at least fifty per cent (50%) of the voting stock, shares or interests of such entity;

**“Customer Data”** means data relating to, or received by Customer or its Affiliates from, clients of Customer or its Affiliates that has been received or generated by Supplier, Supplier Affiliates or their subcontractors in connection with the provision of Services under or pursuant to this Agreement or any transactional document.

“**Customer Personal Data**” means Personal Data relating to Customer’s Personnel, customers or service providers (and other persons or entities connected with such persons or entities) which is received, acquired or generated by or on behalf of Supplier in the course of providing Services to the Customer under any work order or statement of work or similar under the Agreement;

“**Customer’s Systems**” means all computer or electronic processing equipment, all associated or interconnected network equipment, routers, semi-conductor chips, embedded software, and communication lines, all other equipment (including printers, copiers, scanners and telephones), and all software owned, licensed or operated by, or operated on behalf of, Customer or its Affiliates;

“**Data Controller**” means the person who alone or jointly with others determines the purposes and means of the processing of Personal Data;

“**Data Processor**” means a person which processes Personal Data on behalf of the Data Controller;

"**Data Protection Laws**" means the Data Protection Directive (95/46/EC) and the Directive on Privacy and Electronic Communications (2002/58/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including Regulation (EU) 2016/679, when applicable) and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by supervisory authorities;

“**Data Transfer Agreement**“ is an agreement in the form set out in the European Commission's Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under EU Directive 95/46/EC (as may amended by Customer in connection with transfers relating to Data Protection Laws in Switzerland), or any replacement or additional form approved by the European Commission or as applicable in the UK, Switzerland or Jersey from time to time

“**Data Subject**” means a natural person who is identified, or who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

“**Defect**” means a defect, failure, malfunction, or non-conformity of a Deliverable or Services that prevents the Deliverable or Services from operating in accordance with the applicable Acceptance Criteria or Specification;

“**Deliverables**” means any item to be developed, prepared or delivered by Supplier or a Supplier Affiliate, as identified in any work order or statement of work or similar under the Agreement or otherwise required for Supplier to comply with any work order or a statement of work or similar under the Agreement or the Agreement;

“**Documentation**” means: (i) all documents and materials (in any language, format or medium) that are normally supplied by Supplier to its customers to aid in the use and operation of the Software, including: (a) functional, technical, design and performance specifications; (b) installation, configuration, administration, operation and maintenance procedures and instructions; (c) training guides and user manuals; (ii) all additional documentation or materials describing the functional, technical, design or performance characteristics of the Software provided by Supplier to Customer; and (iii) all modifications to such documents or materials that are made by or on behalf of Supplier from time to time;

“**European Personal Data**” means Customer Personal Data where the relevant Customer or Customer Affiliates are located in Hungary or subject to (i) the European Commission Data Protection Directive (95/46/EC) or any implementing or related legislation of any member state in the European Economic Area; (ii) when applicable, the Regulation (EU) 2016/679 and any related legislation of any member state in the European Economic Area; or (iii) any Data Protection Laws in Switzerland or Jersey;

“**Open Source Code**” means open source code, free code, community source code or similar software, including any libraries or software licensed under the General Public License or any other license agreement or arrangement obliging Customer to make source or object code available to third parties;

"**Personal Data**" means any information that relates to a Data Subject, or (in jurisdictions where Data Protection Laws give legal entities the protections afforded to natural persons) a legal entity, or other information that constitutes “personal data” under such Data Protection Laws;

“**Personnel**” means a Party’s or its Affiliate’s directors, officers, employees, non-employee workers, agents, auditors and consultants. In addition, Personnel includes the directors, officers, employees, non-employee workers, agents and consultants or subcontractor used by Supplier or a Supplier Affiliate, directly or indirectly, to provide any Services;

“**Regulatory Bodies**” means those government departments and regulatory, statutory and other entities, committees and bodies, which whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate or influence any matter dealt with in this Agreement or any other affairs of Customer or its Affiliates;

“**Specification**” means the specifications for Deliverables and/or Services as set out in any work order or statement of work or similar under the Agreement, or where none is set out, the specifications for such Deliverables and/or Services published or made generally available by Supplier;

"**Services**" means any services, responsibilities, processes and/or functions to be provided by or on behalf of Supplier, Supplier Affiliates or sub-contractors under the Agreement;

“**Software**” means: (i) the computer programs licensed by Supplier or provided by a Supplier Affiliate to Customer and/or Customer Affiliate hereunder, including any customisations, enhancements, updates, upgrades, releases, replacement or successor products, Defect corrections, and other modifications thereto provided to Customer and/or Customer Affiliate by Supplier or a Supplier Affiliate; and (ii) any third-party software that is embedded into, or otherwise furnished by Supplier with, Supplier’s proprietary software (including Open Source Code), together with related Documentation; however, “Software” shall not include any modifications or enhancements made thereto by or on behalf of Customer;

“**Sub-processor**” means any party (including any Supplier Affiliate or subcontractors) appointed by or on behalf of Supplier to process European Personal Data on behalf of any Customer or Customer Affiliates in connection with the Agreement;

“**Work Product**” means each Deliverable, and all ideas, concepts, know-how, techniques, inventions, discoveries, improvements, specifications, designs, methods, devices, systems, reports, studies, computer software (in object or source code), programming and other documentation, flow charts, diagrams and all other information or tangible material of any nature (in any medium and in any stage of development or completion) relating to the subject matter of the Agreement or any work order or statement of work or similar under the Agreement, that are conceived, designed, practiced, prepared, produced or developed by Supplier, Supplier Affiliate or any of their Associated Persons (i) during the course of providing the Services; (ii) based upon knowledge or information learned or gained from Customer or a Customer Affiliate; or, (iii) resulting from the use of Customer’s or a Customer Affiliate’s facilities, Personnel, or materials.

1. **CONFIDENTIALITY**
   1. **Duty of Care and Use Restrictions.**
   2. The Party receiving Confidential Information (“**Receiving Party**”) of the other Party (“**Disclosing Party**”) (pursuant to the Agreement, any work order or statement of work or similar under the Agreement or in contemplation of entering into any work order or statement of work or similar under the Agreement) will:
      1. exercise at least the same degree of care with respect to Disclosing Party’s Confidential Information that Receiving Party exercises to protect its own Confidential Information and other customers’ confidential information of a similar nature, if any; and
      2. at a minimum, adopt, maintain and follow written and comprehensive security practices and procedures that are sufficient to safeguard Disclosing Party’s Confidential Information from any (a) unauthorised disclosure, access, use or modification; (b) misappropriation, theft, destruction, or loss; or (c) inability to account for such Confidential Information.
   3. Supplier represents that it has or will have security practices and procedures which contain administrative, technical, organisational and physical safeguards to ensure the security and confidentiality of any Personal Data. Such practices and procedures shall include (but not be limited to) the following security measures:
      1. encryption of all transmitted records and files containing Personal Data that are sent across wireless or communications networks;
      2. utilisation of appropriately set passwords, firewalls, malware and any other software to protect Personal Data stored on computer systems;
      3. appropriately restricted use of portable devices for storing Personal Data and encrypting such portable devices to the extent they must be used;
      4. encryption of all laptops where Personal Data may be stored; and
      5. disposal of Personal Data in such a way as to make it inaccessible or unreadable by anyone, whether through technical or other means.
   4. Without limiting the generality of the foregoing, Receiving Party will only use or reproduce Disclosing Party’s Confidential Information to the extent necessary to enable Receiving Party to fulfil its obligations under the Agreement or any work order or statement of work or similar under the Agreement and in Customer’s case, to exercise its rights as contemplated by the Agreement or any work order or statement of work or similar under the Agreement. In addition, Receiving Party will disclose Disclosing Party’s Confidential Information only to those of Receiving Party’s (or in the case of Customer, also to its Affiliates’) Personnel who have a “need to know” such Confidential Information (and only to the extent necessary) to fulfil the purposes contemplated herein.
   5. Supplier will ensure that (a) each of its Personnel and Associated Person who will be providing Services shall be bound to uphold the obligations of confidentiality set forth herein; and (b) it maintains and follows security practices and procedures that are sufficient to detect patterns, practices or specific forms of activity that indicate the possible existence of an actual or attempted theft or misappropriation of Personal Data. Supplier shall promptly report all such incidences or suspicious activities to Customer. Supplier represents that it will conduct regular risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of electronic, paper, and other records containing Personal Data and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting such risks.
   6. **Exclusions.** The obligations of confidentiality assumed hereunder shall not apply to the extent Receiving Party can demonstrate, by clear and convincing evidence, that such information:
      1. is or has become generally known by persons engaged in the technology or financial services industries, without any breach by Receiving Party of the provisions herein or any other agreement between the Parties;
      2. was rightfully in Receiving Party’s possession, without confidentiality restrictions, prior to such Party’s receipt pursuant hereto;
      3. was rightfully acquired by Receiving Party from a third party who was entitled to disclose such information, without confidentiality or proprietary restrictions;
      4. was independently developed by Receiving Party without use of or reference to Disclosing Party’s Confidential Information; or
      5. is subject to a written agreement pursuant to which the Disclosing Party authorised the Receiving Party to disclose the information in question.

The exclusions in paragraphs 2.7(i) to (iii) above shall not apply to Customer Personal Data.

* 1. **Accounting for Confidential Information.** Except as otherwise specified in the Agreement, upon the request of the Disclosing Party, the Receiving Party will return (or purge its systems and files of, and suitably account for) all Confidential Information supplied to, or otherwise obtained by, the Receiving Party in connection with the Agreement. The Receiving Party will certify in writing that it has fully complied with its obligations under this Addendum Appendix within seven days following the date it receives a request from the Disclosing Party for certification. For the avoidance of doubt, this **Section 2.9** will not be construed: (i) to require Customer to return to return any Software, any Documentation, any information or materials provided by Supplier or any of Supplier’s Confidential Information that was provided as part of, or in conjunction with, the Software or Services, or (ii) to limit either Party’s right to seek relief for damages that are caused by the other Party’s default.

1. **PERSONAL DATA AND INFORMATION SECURITY**
   1. Supplier agrees and ensures that its Personnel and any Associated Person agree to collect, store, process, disclose, allow access to, disseminate or use any Customer Personal Data (a) only as expressly instructed by Customer or the Customer Affiliate in writing (either within the provisions of the Agreement or otherwise), (b) for the sole purpose of its performance under the Agreement and managing its relationship with Customer, and only to the extent strictly necessary to do so, (c) in accordance with any Applicable Law, and (d) in accordance with the provisions of Customer’s and its Affiliates’ applicable policies that are made available to Supplier.
   2. Supplier must promptly notify Customer of any request by an individual or by any other person for Customer Personal Data to be released to that requestor, other than in accordance with instructions provided by Customer or a Customer Affiliate.
   3. **Supplier Personal Data.** Customer and its Affiliates may collect, store, process, disseminate or use information that relates to Supplier or is the Personal Data of Supplier Personnel or the Supplier’s beneficial owners and principals (collectively, “**Supplier Personal Data**”) to exercise their rights or fulfill their obligations under the Agreement or Applicable Law, or for their legitimate business purposes including supplier management, risk and control, and administration. Under Customer’s global operating model, Supplier Personal Data may be stored in, or accessed from, countries whose privacy laws may not be as protective as those in the country from which the Supplier Personal Data was provided. Supplier consents to the processing of Supplier information by Customer and its Affiliates as described in this **Section 3.3** and confirms that if Supplier discloses any Supplier Personal Data to Customer or its Affiliates in connection with the Agreement, Supplier has the authority to make such disclosure and that such disclosure will be made in compliance with applicable Data Protection Laws and that Supplier has made available to, or provided the relevant individuals with, a copy of any privacy statement provided by Customer or its Affiliates.
   4. **Data Processor.** Customer and Customer Affiliates, as relevant, will be the Data Controller and the Supplier will be the Data Processor when processing European Personal Data in the course of the Supplier providing Services to Customer under any work order or statement of work or similar under the Agreement. The Parties acknowledge that a description of the European Personal Data processed by the Supplier as a Data Processor under the Agreement in Annex 1 of this Addendum Appendix or may be set out in any work order or statement of work or similar under the Agreement, and contains the following information: (i) the subject-matter of the processing; (ii) the duration of the processing; (iii) the nature and purpose of the processing; (iv) the types of Personal Data processed; and (v) the categories of Data Subjects in relation to Personal Data processed.
   5. In this context, Supplier shall and shall procure that any Associated Person processing European Personal Data shall, at no additional cost:
      1. process the European Personal Data in accordance with the provisions of **Section 3.1**;
      2. promptly advise Customer of any notices, requests or queries from Data Subjects, any data protection supervisory authority or any law enforcement authority, for Customer to resolve;
      3. promptly provide such information and assistance to Customer as it may reasonably require to allow it to comply with:(a) the rights of Data Subjects under Data Protection Laws (including, taking into account the nature of the processing, appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to Data Subject requests to exercise such rights),(b) notices, requests or queries served or raised by any data protection supervisory authority or any law enforcement authority, (c) requirements to conduct data protection impact assessments and to consult with supervisory authorities in relation to data processing; and(d) to facilitate timely resolution of any matter arising hereunder or any investigation;
      4. implement (and update from time to time as needed) appropriate technical, organisational, and security measures (including any specific security measures notified by Customer) to protect Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, disclosure, or alteration, and provide Customer with a written detailed description of such measures promptly on request from time to time;
      5. without limiting the foregoing, follow best industry practice (including background checks and ongoing training) to ensure: (a) the reliability of Customer’s Associated Persons who may have access to Customer Personal Data; and (b) that such measures include the ability to retrieve promptly any Customer Personal Data in such format and on such media as Customer reasonably requests;
      6. maintain written records of all categories of European Personal Data processing activities carried out on behalf of Customer or Customer Affiliates containing the information prescribed in applicable Data Protection Laws;
      7. upon the expiry or termination of the Agreement and/or any work order or statement of work or similar under the Agreement under which European Personal Data will be processed, promptly arrange for the secure return or destruction of Customer Personal Data as notified by Customer in writing at the relevant time and delete existing copies of the European Personal Data, unless European Union or European Union member state law requires storage of the European Personal Data, in which case the Parties will work together to ensure that this requirement is met. Where the expiry or termination is in respect of any work order or statement of work or similar under the Agreement, this **Section 3.5(vii)** shall apply to the European Personal Data processed in connection with that work order or statement of work or similar under the Agreement;
      8. notify Customer immediately if, in Supplier's opinion, an instruction for the processing of Customer Personal Data infringes Applicable Law; and
   6. If Customer determines, in its sole discretion and acting reasonably, or a supervisory authority for data protection considers that amendment to the Agreement or any work order or statement of work or similar under the Agreement, or execution of further or additional agreements between the Parties, is required in order to comply with applicable Data Protection Laws, Supplier shall enter into such amendments or further or additional agreements.
   7. **Non EEA Access and Storage.** Supplier shall not, without Customer’s express prior written approval, send any European Personal Data to, store European Personal Data at, or provide access to European Personal Data from, any facility or data center outside the European Economic Area. If required by Customer, Supplier shall promptly execute, or shall procure that any relevant Sub-processor promptly executes a Data Transfer Agreement, populated as reasonably required by Customer, with Customer or any Customer Affiliate that requires this. Should the terms in this Appendix impose additional or more stringent obligations on Supplier than a Data Transfer Agreement entered into, then Supplier undertakes to comply with and ensure any Sub-processor complies with such additional or more stringent terms of this Appendix unless this would result in the invalidity of the Data Transfer Agreement under Data Protection Laws (in which case the relevant term of the Data Transfer Agreement shall prevail).
   8. **EU-US Privacy Shield**. In the event that the Supplier or any relevant Sub-processor is Supplier is EU-US Privacy Shield and/or Swiss-US Privacy Shield certified and such certification is relied upon to ensure that transfers of any European Personal Data to, or storage of European Personal Data at, or access to European Personal Data from, any facility or data center outside the European Economic Area are in accordance with data transfer rules under Data Protection Laws, Supplier represents and warrants in respect of itself and, where relevant, in respect of any relevant Sub-processor, that it (or the Sub-processor, if relevant) has self-certified its adherence to the EU-US Privacy Shield Framework and/or the Swiss-US Privacy Shield Framework (as relevant) to the US Department of Commerce and that any such certification is adequate and appropriate to cover the processing of European Personal Data in connection with the Agreement and all relevant work orders or statements of work or similar under the Agreement. In such cases, Supplier shall, and shall ensure that any relevant Sub-processor shall, comply with the relevant Privacy Shield Principles when processing any European Personal Data in connection with the Agreement or all relevant work orders or statements of work or similar under the Agreement. Supplier shall notify Customer as soon as possible if Supplier and/or any relevant Sub-processor stops adhering to the requirements of the EU-US Privacy Shield Framework and/or Swiss-US Privacy Shield Framework (as relevant) or the EU-US Privacy Shield and/or Swiss-US Privacy Shield (as relevant) ceases to exist.