JOINT DATA CONTROLLERS AGREEMENT

This Joint Data Controllers Agreement ("**Agreement**") is concluded on 21 December 2022, hereinafter referred to as the "**Effective Date**", by and between

SHBPAcademy OÜ, a company duly incorporated and validly existing under the laws of Republic of Estonia, herein acting and represented by its Director Anatolii Bondarenko,
Address: Harju maakond, Tallinn, Kesklinna linnaosa, Tuukri tn 19-315, 10120
Email: info@shbpacademy.com
Phone: +380 984556095,

Anatolii Bondarenko, a private entrepreneur, citizen of Ukraine,
Address: Ukraine, 62331, Kharkiv region, Dergachivskiy district, village Velyki Prokhody, Prikordonna Street, building 6
Email: anatoliybon13@gmail.com
Phone: +3 8(095) 867-44-78, and

Lyudmila Kotsiura, a private entrepreneur, citizen of Ukraine,
Address: Ukraine, 61201, Kharkiv region, Kharkiv city, Peremohy ave., House 53-B, apartment *
Email: luda21071979@gmail.com
Phone: +3 8(066) 413 400 9,

hereinafter referred to individually as a "**Party**" or together as the "**Parties**".

Parties have agreed on the following:

1. Definitions

For the purposes of this Agreement:

"data controller" has the meaning given to it by Article 4 of the GDPR, which is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"data subject" has the meaning given to it by Article 4 of the GDPR, which is an identified or identifiable natural person.

"**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 by the Parties or their respective contractors.

"GDPR" shall mean 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).

"personal data", has the meaning given to it by Article 4 of the GDPR, which is any information relating to a data subject.

"processing", has the meaning given to it by Article 4 of the GDPR, which is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"technical and organisational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or

access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

"**SCC**" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010.

2. Subject Matter

2.1. The subject matter to this Agreement is the distribution of responsibilities among the Parties regarding to collection and processing of personal data of the data subjects at the websites

https://shbpacademy.com/

https://shbp.info/

https://shbpacademy.online/

with all of their pages and sub-domains (altogether - **"Site"**), including those data collected through the contact form and form for subscription to newsletter, as well as e-mail and communication via the chatbot ("**communication tools**").

2.2. This Agreement is limited to personal data jointly collected by the Parties directly from the data subjects through Site and communication tools. In this case, the Parties act as joint controllers (as set forth in Article 26 of the GDPR). This means the Parties jointly determine the purposes and means of personal data processing.

2.3. Parties jointly determined that purposes of the processing of the data subject's data are as follows:
- to respond to data subject's questions and request;
- to send to data subject newsletter with offers, promotions and other relevant information after he/she has subscribed;
- to ensure the smooth function of the Site and prevent any fraudulent actions or intervention of the malware.

3. Roles and Responsibilities

3.1. Parties determine jointly the purposes and means of processing personal data and therefore act as joint controllers. With this Agreement, the Parties wish to define their roles and responsibilities as joint controllers.

3.2. Each Party commits itself to provide assistance to the other Parties in complying with all applicable requirements of the GDPR insofar as they pertain to the Agreement. In particular, each Party shall:

a. consult with the other Parties about any notices given to data subjects in relation to the personal data.
b. promptly inform the other Parties about the receipt of any data subject requests that shall be fulfilled by other Parties.
c. provide the other Parties with reasonable assistance in complying with any data subject access request.
d. not disclose or release any personal data in response to a data subject request without prior consulting the other Parties where necessary.
e. assist the other Parties in responding to any request from a data subject and in ensuring compliance with its obligations under the GDPR with respect to security matters, breach notifications, impact assessments and consultations with supervisory authorities and regulators.
f. notify the other Parties without undue delay on becoming aware of any breach of the provisions of the GDPR.
g. inform the other Parties of the DPIA outcome (if any was conducted).
h. use compatible technology for the processing of personal data to ensure that there is no lack of accuracy resulting from personal data transfers.

i. provide the other Parties with contact details of at least one employee as responsible officer for all issues arising out of the joint controllership, including the joint training of relevant staff, the procedures to be followed in the event of a data security breach, and the regular review of the Parties' compliance with the GDPR.
j. be responsible for the creation and publication of their own privacy policy, additional policies and other internal information security policies.
k. ensure that their privacy policies are clear and provide sufficient information to data subjects in order for them to understand what of their personal data are being shared between the Parties, the circumstances in which they will be shared, the purposes for the data sharing and either the identity with whom the personal data are shared or a description of the type of organisation that will receive the personal data, as well as how data subjects can make a data subject request;
l. give full information to any data subject whose personal data may be processed under this Agreement of the nature of such processing. Nevertheless, such information shall be necessarily contained within the privacy policy of each Party.
m. process the personal data only for the purposes defined in their respective privacy policies;
n. ensure that it has appropriate technical and organisational measures in place to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. For these purposes, each Party shall adopt internal information security policies and familiarize the other Parties with information about their security practices.

3.3. Where the Parties may not clearly divide, as the case may be, the responsibilities under this Agreement, SHBPAcademy OÜ shall be responsible.

3.4. The Parties shall designate a single contact point through which the Parties can be contacted in respect of queries or complaints in relation to issues covered by this Agreement or any other data protection issues:

SHBPAcademy OÜ: info@shbpacademy.com

Anatolii Bondarenko: anatoliybon13@gmail.com / s.best.practices@gmail.com

Lyudmila Kotsyura: luda21071979@gmail.com

4. Ensuring Rights of the Data Subjects

4.1. Data subjects have a range of rights under the GDPR. The Parties have agreed the procedures specified hereinafter in Section 4 to facilitate data subjects exercise their rights. Data subjects are not obliged to follow these procedures and, therefore, data subjects may exercise their rights against each of the controllers as stated in Article 26.3 of the GDPR.

4.2. **Right of Accessing Personal Data.** The Parties will provide the data subject with a copy of personal data undergoing processing as required under Article 15 of the GDPR. The Party which receives such a request shall satisfy it and notify thereof the other Parties.

In the event when the Party which received a request does not have full information regarding the undergoing processing, it may ask the other Parties for lacking information.

In the event when the Party which received a request may not proceed on it, the request shall be transferred to the other Parties in accordance with the request and complaints procedure of each Party.

4.3. **Right of Rectification of Personal Data**. A data subject may request the rectification of any inaccurate personal data held by the Parties under article 16 of the GDPR. The Party which receives such a request shall satisfy it and notify thereof the other Parties.

In the event when the Party which received a request does not have full information to be rectified, it may ask the other Parties for lacking information.

In the event when the Party which received a request may not proceed on it, the request shall be transferred to the other Parties in accordance with the request and complaints procedure of each Party.

4.4. **Right of Erasure of Personal Data.** A data subject may request the erasure of personal data held by the Parties under article 17 of the GDPR. The Party which receives such a request shall delete the information in question and notify thereof the other Parties about obligation for data deletion.

In the event when the Party which received a request does not have full information to be erased, it may ask the other Parties for lacking information.

In the event when the Party which received a request may not proceed on it, the request shall be transferred to the other Parties in accordance with the request and complaints procedure of each Party.

Party shall not delete the personal data where that processing is necessary for one of the following reasons in compliance with their national laws and the conflict of law provisions thereof:

a. for exercising the right of freedom of expression and information;
b. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) of the GDPR;
d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e. for the establishment, exercise or defense of legal claims.

4.5. **Right of Restriction of Processing.** The Party which obtains a request to restrict processing under Article 18 of the GDPR shall do so and notify thereof the other Parties.

In the event when the Party which received a request does not have full information to be restricted, it may ask the other Parties for lacking information.

In the event when the Party which received a request may not proceed on it, the request shall be transferred to the other Parties in accordance with the request and complaints procedure of each Party.

4.6. **Right of Data Portability.** The Party which obtains any requests for data portability under Article 20 of the GDPR shall administer them and notify thereof the other Parties.

In the event when the Party which received a request does not have full information regarding the transfer in question, it may ask the other Parties for lacking information.

In the event when the Party which received a request may not proceed on it, the request shall be transferred to the other Parties in accordance with the request and complaints procedure of each Party.

4.7. **Provision of Information Regarding Processing.** Each Party shall provide the data subject with information required under articles 13 and 14 of the GDPR by means of privacy policy and other additional policies published on the Site.

4.8. **Provision of Information through Social Media.** The Party which obtains a request through their social media accounts shall satisfy it and notify thereof the other Parties. The Parties shall administer any request in accordance with particular social media's privacy policy and other additional policies.

In the event when the Party which received a request does not have full information regarding the transfer in question, it may ask the other Parties for lacking information.

In the event when the Party which received a request may not proceed on it, the request shall be transferred to the other Parties in accordance with the request and complaints procedure of each Party.

4.9. While processing the data subject's request regarding his/her exercising data protection rights, each Party shall maintain documented evidence of procedures and steps taken to satisfy the request. The documentation shall include the following:

a. date and time of the request;

b. type of request and request details;
c. personal data involved;
d. validity assessment;
e. actions taken to respond to the request.

5. Data Retention

5.1. The Parties shall not retain or process the personal data for longer than is necessary to carry out the purposes defined in their respective privacy policies.

5.2. Where possible the Parties shall publish details of their respective retention schedules in their respective privacy policies and other additional policies on the Site.

5.3. On termination or expiration of this Agreement, the Parties are to return, delete or anonymise any personal data unless they are required to keep the data by legislation or other written contracts.

6. International Transfer of Personal Data

6.1. The Parties agree that in order to fulfil the purposes defined in their respective privacy policies the Parties may share the personal data to third parties outside the EEA given that the appropriate safeguards applied. The Parties shall define the list of third parties the personal data is sent to in their respective privacy policies.

6.2. In case of international transfer of personal data, the Party shall adopt the data processing agreements with the third parties pursuant to the provisions of SCC.

6.3. Each Party shall notify the other Parties upon the conduct of any international transfer of personal data and provide the appropriate safeguards taken to that effect.

6.4. Each Party shall be solely responsible for the preservation of integrity and confidentiality of the personal data transferred outside the EEA.

7. Record of Personal Data

7.1. Each Party shall maintain and keep the record of the personal data collected, including:
a. the purposes of the processing;
b. a description of the categories of data subjects
c. a description of the categories of personal data;
d. the categories of the recipients to whom the personal data have been or will be disclosed;
e. transfers of personal data to a third country, including the identification of that third country or and, in the documentation of suitable safeguards;
f. the envisaged time limits for erasure of the different categories of data;
g. a general description of the technical and organisational security.

7.2. At the request of either Party the other Parties shall present the aforementioned information in writing and/or in electronic form.

8. Technical and Organisational Security Measures

8.1. The Parties agree, where possible, to establish, implement, and maintain an information security program that includes policies and procedures, to protect and keep secure personal data in accordance with good industry practice and as required by the GDPR. Among others, each Party undertakes to implement appropriate technical and organisational measures that comply with applicable laws and regulations designed to ensure and protect the security, integrity and confidentiality of the data subjects' personal data and protect data subjects' personal data against any unauthorized processing, loss, use, disclosure or acquisition of or access.

9. Breach Notifications

9.1. The Parties agree to accord assistance and necessary support in case of any data breach.

9.2. The Party who becomes aware of the data breach shall notify the other Parties as soon as possible, but no later than 24 hours from the indication of the data breach. Such Party provides other Parties with all of the details of the breach.

9.3. The Party who becomes aware of the data breach shall determine whether the supervisory authority needs to be notified. The Party who becomes aware of the data breach may involve other Parties to assist in the risk assessment process and jointly determine whether the supervisory authority needs to be notified, if it is necessary.

9.4. The notification of the data breach to the supervisory authority shall be made in accordance with the procedure established by the Article 33 of the GDPR and include the following, namely:

a. a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b. the name and contact details of the data protection officer and other contact point where more information can be obtained;
c. a description of the likely consequences of the personal data breach;
d. a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Such notification shall be submitted by the Party within 72 hours from the identification of the data breach.

9.5. In case where the Party may not provide the whole aforementioned information at once due to the carrying out the complicated investigation, it shall notify thereof the supervisory authority. This does not prevent the Party from providing further information, if it becomes aware of additional relevant details of the data breach in question.

9.6. The Party who becomes aware of the data breach shall determine whether the data subjects need to be notified. The Party who becomes aware of the data breach may involve other Parties to assist in the risk assessment process and jointly determine whether the data subjects need to be notified, if it is needed.

9.7. The Party who becomes aware of the data breach shall communicate without undue delay to the data subjects concerned. Such notification shall be made by the Party within 72 hours from the identification of the data breach. In the event when the Party who becomes aware is not capable to notify the data subjects concerned, the other Parties shall do so.

9.8. The notification to the data subjects concerned shall include at least the following information:

a. a description of the nature of the breach;
b. the name and contact details of the contact point;
c. a description of the likely consequences of the breach;
d. a description of the measures to be taken by the data subject to mitigate the possible adverse effects of the data breach.

10. Governing Law

10.1. This Agreement shall be governed by the law of the Republic of Estonia.

11. Miscellaneous

11.1 This Agreement is executed in duplicate, each of which being equally authoritative, one for each Party.

11.2. This Agreement constitutes the agreement between the Parties and sets out all the promises, warranties, representations, conditions, understandings and agreements between Parties concerning the subject matter of this Agreement.

SIGNATURES

SHBPAcademy OÜ	**Anatolii Bondarenko**	**Lyudmila Kotsyura**
Address: Harju maakond, Tallinn, Kesklinna linnaosa, Tuukri tn 19-315, 10120	Address: Ukraine, 62331, Kharkiv region, Dergachivskiy district, village Velyki Prokhody, STREET PRIKORDONNA, building 6	Address: Ukraine, 61201, Kharkiv region, Kharkiv city, Peremohy ave., House 53-B, apartment *
Registry code: 16228260	Date of the record of state registration: 12.06.2018 Number of the record of state registration: 24560000000008784	Date of the record of state registration: 12.05.2021 Number of the record of state registration: 2004800000000257899
_____ /Director A. Bondarenko/	**_____/PE A. Bondarenko/**	**_____/PE L. Kotsiura /**