APPENDIX #1 TO LIVESPACE TERMS OF SERVICE (DATA PROCESSING AGREEMENT)

PREAMBLE

This Data Processing Agreement ("DPA") constitutes an integral part of the Livespace Terms of Service ("Terms of Service") and provides the rules for processing personal data by the Service Provider on behalf of the Ordering Party, using the Livespace application (hereinafter jointly referred to as the "Parties" and individually as each "Party").
The terms used in the DPA such as "Users", "Registration Form" or "Application" are to be considered in accordance with their definitions provided within the Terms of Service.
The essential purpose of the DPA is to ensure a high level of protection for personal data in accordance with the current provisions of the law and to implement high standards of personal data protection regarding human, technical and organisational resources serving that purpose.

§ 1 DEFINITIONS

For the purpose of the DPA, including the Preamble, the following definitions have been compiled:

1. **"GDPR"** refers to the General Data Protection Regulation of the European Parliament and Council (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95 / 46 / EC (General Data Protection Regulation);
2. **"Data Controller"** refers to the Ordering Party or any entity related to it, which defines the purposes and means for processing Personal Data, individually or in cooperation with others;
3. **"Data Processor"** refers to the Service Provider, that is "Livespace" sp. z o.o. with its registered seat in Warsaw (02-516) in 17/12 Tadeusza Rejtana St., entered into the National Court Register maintained by the Regional Court for the Capital City of Warsaw in Warsaw, 8th Commercial Division of the National Court Register, under KRS#: 0000358766, with VAT#: 52133568709; REGON#: 142447001, with share capital of 6250.00 PLN;
4. **"Data Subject"** refers to any physical person, to whom the Personal Data is related to;
5. **"Agreement"** relates to the agreement for the provision of a service in the form of the Livespace application which is provided by the Data Processor to the Data Controller, concluded in writing between the Parties or through filling in and confirming of a Registration Form by the Data Controller and thus creating an account within the Application;
6. **"Personal Data"** refers to all information which relates to a physical person who is identified or may be identified (Data Subject), which is the subject matter of this Data Processing Agreement;
7. **"Sensitive Personal Data"** refers to particular types of Personal Data which indicate racial or ethnic origins, political views, participation in labour unions, genetic data, biometric data, medical history, gender or sexual preference, as well as any information regarding convictions or conflicts with the law;
8. **"Personal Data Breach"** refers to an event which takes place in the location of the Data Processor or Data Sub-Processor, which leads to accidental or unlawful destruction, loss, modification or unauthorised disclosure or unauthorised access to Personal Data held by the Data Controller;
9. **"Processing of Personal Data"** refers to an operation or a set of operations performed on Personal Data or collections of Personal Data in an automated or non-automated manner, such as gathering, recording, organizing, arranging, storing, adapting or modifying, downloading, reviewing, using, disclosing by transfer, distributing or any other way of sharing, matching or connecting, limiting, removing or destroying of the data;
10. **"Law on Protection of Personal Data"** refers to GDPR and other applicable acts and regulations of the European Union or a Member State;
11. **"Data Sub-Processor"** refers to a contractual partner of the Data Processor, who processes Personal Data which belongs to the Data Controller, admitted into the process by the Data Processor;
12. **"EEA"** refers to European Economic Area including European Union member states and Norway, Iceland and Liechtenstein;
13. **"Transferring Personal Data to Third Countries"** refers to processing data by a Data processor outside of the EEA, under the condition of fulfilling provisions of chapter 5 of GDPR.

§ 2 SUBJECT MATTER OF THIS AGREEMENT

1. The Parties are bound by an Agreement, the performance of which shall involve processing of Personal Data.
2. The Data Processor agrees to process Personal Data on the basis of the Data Processing Agreement and in compliance with GDPR.
3. In case of any inconsistencies between member state laws regarding data protection and GDPR following May 25, 2018, provisions of the GDPR shall prevail. Until May 25, 2018 member state regulations regarding data protection shall remain in force.
4. Terms used in the Data Processing Agreement, which have not been individually defined in its provisions shall be considered as defined within GDPR.

§ 3 PURPOSE, SCOPE AND MEANS OF PROCESSING PERSONAL DATA

1. The Data Controller entrusts the Data Processor with Personal Data in relation to the carrying out of the Agreement, with the purpose of providing access to the Application, using its functionalities and organisational and technical support related to the use of the application by the Data Controller.
2. The Data Processor shall process Personal Data related to the following category of persons: physical persons, whose Personal Data was entered into the Application by its users.
3. The Data Processor may process in particular the following Personal Data:
   first and last name, position, company name, telephone number, e-mail address, postal address and others. Considering the specificity of using the Application the exact scope of the Personal Data which is being entered into the Application and processed depends on the activities of Users and how they fill the Application with specific Personal Data.

   The Data Processor informs the Data Controller and Users that they are responsible for the Personal Data they enter into the Application, and they require a legal ground for processing the data and ways it may be processed. The Data Controller and Users should not send or in any other way disclose any Sensitive Data belonging to them or any other persons through the Application or otherwise.
4. The Data Processor shall process data in electronic form with the use of software, that is the Application and other tools required for carrying out of the provisions of the Agreement.

§ 4 SECURITY OF PERSONAL DATA

1. Considering the scope of technical knowledge, cost of implementation, and the character, scope, context and purposes of processing, as well as the risk of violation of the rights and freedoms of physical persons of different probabilities and seriousness levels, The Data Processor shall implement proper technical and organizational means to ensure that processing of Personal Data takes place in compliance with GDPR.
2. The list of technical and organisational means implemented by the Data Processor constitutes Appendix #1 to this Agreement.
3. The Data Processor shall perform recurring reviews and updates of the technical and organisational means employed to ensure they are compliant with GDPR at any given time. Changes to Appendix #1 shall not constitute changes to this Data Processing Agreement.

§ 5 RULES FOR PROCESSING DATA BY THE DATA PROCESSOR AND ITS COLLABORATORS

1. The Data processor shall process the Personal Data only on the basis of this Data Processing Agreement, and other documented orders of the Data Controller delivered under the provisions of § 11.4 and §11.5 of the Terms of Service.
2. The Data Processor is obliged to ensure that any persons authorised to process Personal Data on their behalf are formally required to maintain confidentiality, or are under a proper legal obligation to maintain confidentiality.

3. The Data Processor shall familiarise their employees, collaborators and other persons authorised to Process Personal Data on their behalf with the provisions of the law regarding personal data protection and the consequences of violating those laws.

§ 6 COOPERATION BETWEEN THE DATA CONTROLLER AND THE DATA PROCESSOR

1. The Data Processor shall assure the highest degree of professional care to assist the Data Controller in carrying out their duties resulting from GDPR, in particular by providing information required to:
    a. evaluate potential consequences for the protection of personal data or carry out audits, including inspections performed by the Data Controller,
    b. respond to requests submitted by Data Subjects within the scope of art. 15-22 of GDPR,
    c. notify the supervisory authority of any Personal Data Breach,
    d. communicate a Personal Data Breach to the data subject.
2. The Data Processor shall notify the Data Controller of a Personal Data Breach immediately via electronic mail to their email address, no later than within 36 hours from becoming aware of any case of suspicion of a breach of personal data protection or non-compliance with the Law on Personal Data Protection.
3. In case the Data Processor receives any complaint, notice or request, which relates to the processing of Personal Data of the Data Controller by the Data Processor or compliance with the Law on Personal Data Protection, within the scope allowed by the provisions of the law, the Data Processor shall immediately notify the Data Controller by sending a proper message to their email address, no later than within 3 working days from the moment of receiving of such complaint, notice or request and in the required scope they will cooperate and assist the Data Controller in providing a proper response.
4. In case when the Data Controller issues any instructions for the Data Processor which in the opinion of the Data Processor shall constitute a Personal Data Breach or a violation of other provisions of the Law on Personal Data Protection, the Data Processor shall immediately inform the Data Controller.

§ 7 AUDIT OF PERSONAL DATA PROCESSING

1. The Data Controller is entitled to audit the location of data processing or the premises of the Data Processor to obtain the required information or review the Personal Data which is being stored.
2. The Data Controller is obliged to inform the Data Processor of the date of the planned audit using electronic mail to the e-mail address of the Data Processor, at least 4 (four) weeks before the scheduled date of the inspection. The inspection shall be carried out within the working hours of the Data Processor's office on a regular workday, and it may not negatively influence the proper and timely conduct of daily operations of the Data Processor related to their current business activity.
3. Due to the necessity to ensure efficient functioning of the Data Processor the Audit conducted by the Data Controller may take up to 1 full workday.
4. Persons authorised to carry out the Audit on behalf of the Data Controller shall be obliged on the basis of a written agreement to maintain confidentiality of all information, documents, data, particularly of technical, commercial and financial character, regarding the Data Processor or other information obtained from the Data Processor, which they received or became aware of as result of conducting the audit.

§ 8 TERRITORIAL SCOPE OF PROCESSING PERSONAL DATA

1. The Data Processor is authorised to process Personal Data within the territory of EEA.
2. The Data Processor is authorised to process Personal Data by transferring it to Third Countries. This may only take place under the conditions defined in Chapter 5 of GDPR, particularly the Data Processor may transfer the data to a Third Country which the European Commission decided that it ensures an adequate level of protection, as per Art. 45 of GDPR.

§ 9 USING THE SERVICES OF SUB-PROCESSORS

1. The Data Controller agrees for the Data Processor to use services provided by Sub-Processors in the processing of the Personal Data, to carry out the provisions of the Agreement properly.
2. Information regarding Sub-Processors which are entrusted with the Personal Data constitutes appendix #2 herewith.
3. In case of a planned change of the Sub-Processors with whom the Data Processor cooperates to process Personal Data, by adding a new entity, the Data Processor shall inform the Data Controller, by means of electronic mail to the e-mail address of the Data Controller, no later than 14 days before providing Personal Data for processing by the Sub-Processor. Changes to the list of Sub-Processors do not constitute changes to this Data Processing Agreement. Within the content of such notice, the Data Processor shall indicate in what scope, provision of services by the Sub-Processor is required, to maintain access to the Application, part of the Application, or any additional feature it is regarding
4. The Data Controller can express their objections against any changes to the list mentioned above using electronic mail to the e-mail address of the Data Processor, within 7 days from the day of receiving notice of such change from the Data processor.
5. In case when provision of the service of access to the Application, part of the application or any additional feature is not possible without cooperation with the Sub-processor, to which the Data Controller submitted objections, the Parties agree that upon submission of these objections, their Agreement is terminated effective at the end of the month, following the month in which the Data Controller submitted their complaints, in accordance with the provisions of § 9.7 of the Terms of Service.
6. The Agreement between the Data Processor and the Sub-Processor includes an obligation for protecting Personal Data by the Sub-Processor, at least to the same scope as defined in this Data Processing Agreement. In particular, the Sub-Processor is obliged to ensure sufficient guarantees of implementing proper technical and organisational means, for the processing to meet the requirements of GDPR.

§ 10 DURATION OF PERSONAL DATA PROCESSING

1. Upon termination or dissolution of this Agreement, the Data Processor shall cease to process the Personal Data.
2. In accordance with the will of the Data Controller, the Data Processor shall remove or anonymise any Personal Data in an irreversible way, on every medium, where the Personal Data was stored, both on premises of the Data Processor and all Sub-Processors.
3. Removing or anonymisation to the Personal Data, shall take place no later than 70 days from the day of termination or dissolution of the Agreement, unless the Parties agree on another date for removal or anonymisation of the Personal Data.
4. In case any provisions of the law require, the Data Processor shall immediately inform the Data Controller of the requirement to store Personal Data for a particular period, following termination or dissolution of the Agreement. In such case the Data processor is authorised to process the Personal Data only within the scope and as required by the provisions of the law.

§ 11 RESPONSIBILITY OF THE DATA PROCESSOR TOWARDS THE DATA CONTROLLER

1. The Data Processor is responsible for any damages caused to the Data Controller, which resulted in relation to non-fulfilment or improper fulfillment of the provisions of this Data Processing Agreement, by the Data Processor, particularly any Personal Data processing noncompliant with this Agreement, within the scope of the actual loss incurred by the Data Controller, with the reservation that the Data Processor does not bear any responsibility for any damages which resulted from unintentional guilt.
2. In that same scope, the Data Processor bears responsibility for any actions of their employees, collaborators, and other persons assisting them in processing the entrusted Personal Data, including Sub-Processors.

§ 12 FINAL PROVISIONS

1. This Data Processing Agreement comes into force on the day of accepting the Terms of Service by the Data Controller.
2. This Data Processing Agreement shall become dissolved upon termination of the Agreement or in any other way as defined therein.
3. In the case when any provision of the Data Processing Agreement becomes void or unenforceable, the remaining provisions remain valid, unless the Data Processing Agreement becomes unenforceable without those particular provisions. In such case, the Parties shall immediately begin negotiations to agree on new provisions allowing for the Data Processing Agreement to remain in force.
4. The Data Processing Agreement constitutes the entire agreement and arrangements between the Parties regarding the subject matter of this Agreement, and it supersedes all previous contracts binding the Parties and referring to this matter.
5. This Data Processing Agreement shall be governed and interpreted under the provisions of the law of the Republic of Poland. Any disputes arising from the provisions of this Agreement shall be settled before a common court with jurisdiction over the seat of the Data Processor.
6. The Parties shall use their best efforts so that any disputes arising from this Agreement or related to it are settled amicably. In case of a lack of an amicable solution within one month from the moment a dispute arises, such dispute is to be presented for the final settlement before a common court with supervision over the seat of the Data Processor.
7. None of the Parties to this Agreement is authorised to transfer the rights and obligations resulting from this Agreement to any other third party without prior written consent of the other Party.
8. Appendixes to this agreement constitute its integral parts:
    - Appendix #1 - Technical and Organizational Means of Data Protection
    - Appendix #1 - List of Sub-Processors

APPENDIX #1 TO THE DATA PROCESSING AGREEMENT

TECHNICAL AND ORGANIZATIONAL MEANS OF SECURITY EMPLOYED BY THE DATA PROCESSOR

1. **Organizing security**
    a. Protection of Personal Data is carried out through physical safeguards, organisational procedures, software systems and the users of the Application themselves.
    b. In the objective scope, the safeguards described herein, are applied to Personal Data processed within information systems of the Data Processor, personal data stored on external information storage devices and within paper documentation of the Data Processor.
    c. All employees of the Data processor and other individuals having access to the Personal Data are obliged to use the safeguards defined herein, including collaborators and persons employed on the basis of civil-law contracts.

2. **Applied safeguards**
    a. Individual access accounts are used for the Personal Data processing systems, secured by authentication mechanisms.
    b. Encrypted connections (SSL) are used for providing access to Personal Data processing systems.
    c. Particular procedures are in place with the purpose of granting and revoking user access permissions.
    d. A strong password policy is in place, along with the requirement to change passwords and block accounts.
    e. Storage drives within all the computers used for processing Personal Data are encrypted.
    f. Access to the operating system of the computer used to process Personal Data is secured with an authentication process.
    g. A screensaver is used along with automatic access restriction in case of inactivity on the computer which is used for processing Personal Data.
    h. A backup policy is in place.
    i. Particular means are in place which make it impossible to create unauthorised Personal Data backups.
    j. Documents and printouts including any Personal Data are stored in physically secure rooms.
    k. Periodic courses are conducted within the scope of personal data protection and information security.

APPENDIX #2 TO THE DATA PROCESSING AGREEMENT

SUB-PROCESSORS OF PERSONAL DATA

No.	Name	Address	Processing location	Purpose of processing
1.	ATM S.A.	21a Grochowska St. 04-186 Warsaw, POLAND	Warsaw, Poland	Hosting
2.	Amazon Web Services, Inc.	410 Terry Ave North Seattle, WA 98109-5210 USA	EEA (Ireland)	Hosting
3.	Hostersi sp. z o.o.	26A PCK St. 44-200 Rybnik, POLAND	Rybnik, Poland	Hosting service administration
5.	Vercom S.A.	22 Rosevelta St, 60-829 Poznań, POLAND	Poznań, Poland	Sending e-mail messages